

BESTEMMELSER FOR DEN MILITÆRE SIKKERHEDSTJENESTE

Version 2.57.02
Januar 2024



FORSVARSKOMMANDOEN

AUTORISATION

Nærværende "*Bestemmelse for Den Militære Sikkerhedstjeneste*" autoriseres hermed.

Bestemmelsen er gældende for alle institutioner og myndigheder inden for Forsvarsministeriets koncernområde.

KNUD BARTELS

Postadresse
Postboks 2153
1016 København K

Besøgsadresse
Danneskjold-
Samsøes Allé 1
1434 København K

Telefon 45 67 45 67
Gennemvalg: 45 67 + lok.nr

Telefax
45 89 07 48

Internet
fko@mil.dk
Forsvaret .dk

OVERSIGT OVER VÆSENTLIGSTE ÆNDRINGER VED RETTELSE NR. 57

Kapitel 9

Konsekvensændringer som følge af nedlæggelsen af Koncern Informationssikkerheds Udvalget (KIU) i 2020.

En generel sproglig gennemgang og opdatering

Konsekvensændringer som følge af at risikovurdering og -håndtering inden for informationssikkerhed behandles i FMNBST 358-2

Konsekvensændringer som følge af opdatering af informationssikkerhedsforanstaltningerne i kap. 6 i FKOBST 358-1, navnlig hvad angår informationssikkerhedsinstrukser

Konsekvensændringer som følge af at egenkontrol (intern kontrol), og tilsyn inden for informationssikkerhed er reguleret i FMNBST 358-1

Kapitel 10

Præcisering vedrørende rapportering om bortkommen ammunition og eksplosivstoffer. Ændringen præciserer, hvilken rapportering der skal gennemføres afhængigt af, om hændelsen udgør et brud på de fysiske sikkerhedsforanstaltninger, udgør en sikkerhedsmæssig risiko eller ikke udgør en sikkerhedsmæssig risiko.

Begge kapitler er ændret for så vidt angår sidenummerering ligesom de indledes med en indholdsfortegnelse. De øvrige 8 kapitler vil inden længe blive ændret på samme vis.

OVERSIGT OVER VÆSENTLIGSTE ÆNDRINGER VED RETTELSE NR. 57.01

Ikke noget af betydning

OVERSIGT OVER VÆSENTLIGSTE ÆNDRINGER VED RETTELSE NR. 57.02

Kapitel 2

Punkt 7. BESKYTTELSE AF PERSONEL

Punktet er blevet tilføjet at man skal aftage sit ID-kort eller adgangskort, når man færdes i det offentlige rum

INTRODUKTION TIL DEN MILITÆRE SIKKERHEDSTJENESTE

Nærværende "Bestemmelser for Den militære Sikkerhedstjeneste" træder i kraft ved modtagelsen.

Rettelser udgives normalt en til to gange om året.

FKO 358-1 understøttes af Forsikring & Pensions (F&P) sikringskataloger vedrørende Tyverisikring og Automatiske Indbrudsalarmanlæg (AIA), (se introduktion side II og III). F&P sikringskataloger er tilgængelig på Internettet.

FKOBST 358-1 findes på [FIIN](#) og [Internettet](#).

Der er i bestemmelsen indlagt en række links til relevante hjemmesider. Opmærksomheden henledes på, at links til hjemmesider på Internettet selvsagt ikke fungerer, når bestemmelsen åbnes via forswarets interne net (KFI/FFI), ligesom links til myndigheder og dokumenter på KFI/FFI ikke virker, når bestemmelsen åbnes via Internettet.

Links til skabeloner, skemaer mv. tilgår siderne med skrivbare skabeloner, hvorefter brugere skal finde den relevante skabelon i oversigten.

Ansvarlig for bestemmelsens udarbejdelse:

Forsvarets Efterretningstjeneste

Afdelingen for Militær Sikkerhed

Kontaktperson: Tlf. 33 32 55 66, lokal 3303, postadresse [FIIN](#).

INTRODUKTION TIL FORSIKRING & PENSION SIKRINGSKATALOGER

1. FORSIKRING & PENSION SIKRINGSKATALOGER

Forsikring & Pension (F&P), der er forsikringsselskabernes og de tværgående pensionskassers erhvervsorganisation i Danmark, udgiver en række vejledninger, pjecer samt kataloger og oversigter over bl.a. installatører og sikringsprodukter, der er registreret hos F&P.

Sikringskatalogerne er udarbejdet i en form, der gør dem anvendelige for en stor brugergruppe. Målgruppen er alle, der arbejder med indbrudssikring på praktisk eller projekterende plan.

Da udarbejdelsen er foretaget af F&P, er indholdet præget af forsikringsselskabernes interesse i skadeforebyggende arbejde. Det er værd at bemærke, at en lang række af F&P samarbejdspartnere – herunder forsvaret – på tyverisikringsområdet har været med til at give sikringskatalogerne et indhold, der rækker ud over forsikringserhvervets interesse.

F&P sikringskataloger findes på Internetadressen: www.fpsikring.dk/tyveri. Sikringskatalogerne kan også købes ved Dansk Brand- og sikringsteknisk Institut (DBI), dbi@dbi-net.dk.

1.1 Sikringskatalog.

Sikringskataloget er inddelt i 14 "klikbare" underpunkter, der indeholder en række råd og vejledninger, primært vedrørende mekanisk tyverisikring og TV-overvågning.

1.2 AIA-katalog.

Kataloget er inddelt i 23 "klikbare" underpunkter og gengiver de forskrifter, som F&P anvender for henholdsvis prøvning, projektering og installation af AIA-anlæg.

1.3 Sikringsprodukter.

Her findes en samlet oversigt over de mekaniske- og AIA-produkter, som er registreret (prøvet og godkendt) hos F&P.

1.4 Installatørkatalog.

I kataloget er listet de installatørfirmaer, som er registreret hos F&P inden for områderne alarmanlæg, mekanisk tyverisikring og ITV-anlæg. Fra medio 2007 vil registreringen inden for alarmanlæg kun omfatte installatører, der er certificeret iht. de kravspecifikationer, der er udarbejdet af Sikkerhedsbranchen, Tekniq, F&P m.fl.

At et firma står opført i installatørkataloget betyder alene, at firmaet er godkendt af F&P. Det er således ikke en garanti for, at firmaet er godkendt til at udføre klassificeret arbejde for Forsvaret. Vedrørende sikkerhedsgodkendelse af firmaer, se kapitel 8.

2. FKOBST 358-1.

F&P definitioner og terminologi er indarbejdet i relevante kapitler i nærværende bestemmelse. Uddrag af sikringskatalogerne er overført som bilag og underbilag til kapitel 7. I denne overførsel kan der være foretaget mindre korrektioner og/eller udeladelser. Såfremt der ved projektering og udførelse af sikringsløsninger måtte opstå tvivl om bestemmelsesgrundlaget, er FKOBST 358-1 gældende inden for forsvarsministeriets concern-område.

KAPITEL 1

MILITÆR SIKKERHEDSTJENESTE

Bilag:

1. Oversigt over chefer med ansvar lokal koordination af den militære sikkerhedstjeneste
2. Sikkerhedsofficeren – opgaver og uddannelse
3. Retningslinjer for udarbejdelse af uddannelsesprogram for militær sikkerhed
4. NATO, EU og nationale klassifikationsgrader
5. Praktisk klassifikationsvejledning
6. Klassifikationsmærkning
7. Kontorsikkerhed
8. Tilintetgørelse af informationsbærende materiale

1. FORMÅL

Formålet med denne bestemmelse er at fastsætte regler og procedurer for den militære sikkerhedstjeneste samt at give anvisninger om dens praktiske udførelse.

Den militære sikkerhedstjeneste skal beskytte Forsvarsministeriets (FMN) koncernområde såvel nationalt som internationalt mod de trusler, der rettes mod personel, materiel, informationer, informations- og kommunikationssystemer, operationer og etableringer. Den militære sikkerhedstjeneste skal desuden beskytte civile virksomheder, der udfører klassificeret arbejde for koncernen.

Hvor der i bestemmelsen anvendes "koncernen" eller "koncernområdet" menes alle styrelser, myndigheder og institutioner inden for FMN myndighedsområde.

2. GRUNDLAG

Bestemmelsen er udarbejdet på baggrund af statsministeriets cirkulære vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU mm., NATO sikkerhedsbestemmelser (C-M (2002)49), ISO/IEC 27001 (standard for informationssikkerhedsledelse), Forsvarsministeriets [Direktiv for Den Militære Sikkerhedstjeneste indenfor Forsvarsministeriets område](#) samt [FMNBST 358-1 om informationssikkerhedsledelse](#) og [FMNBST 358-2 om risikostyring inden for informationssikkerhed](#).

3. DEN MILITÆRE SIKKERHEDSTJENESTE

Den militære sikkerhedstjeneste identificerer truslerne mod koncernens virksomhed og infrastruktur såvel nationalt som internationalt. Karakteren og omfanget af truslerne analyseres løbende. Gennem risikovurderinger udvikles afbalancerede beskyttelsesforanstaltninger, og der anvises veje til deres implementering (risikostyring). Den indsats, der er forbundet hermed, og de organisatoriske elementer, der indsættes i opgavens løsning, betegnes den militære sikkerhedstjeneste.

4. AFGRÆNSNING

Der foreligger en grænsedragning mellem den civile sikkerhedstjeneste og den militære sikkerhedstjeneste, som er gældende under alle beredskabsforhold.

Det er Rigspolitichefens ansvar at indhente informationer, analysere og vurdere den sikkerhedsmæssige trussel i Danmark som helhed samt indsætte modforanstaltninger, mens det

er Forsvarschefens (FC) ansvar at udøve de samme opgaver inden for FMN koncernområdet.

Det er FC ansvar at udøve de samme opgaver uden for Danmark, hvor danske styrker er indsat eller kan forventes indsat.

Den militære sikkerhedstjeneste, som beskrevet i denne bestemmelse, udgør grundlaget for iværksættelse af sikkerhedsberedskabsforanstaltninger jf. [Forsvarets Beredskabsplan \(FKOBST O.120-1\)](#).

5. SIKKERHEDSUDVALG

5.1 Forsvarsministeriets Sikkerhedsudvalg

Forsvarsministeriets Sikkerhedsudvalg (FMN SIKU) er nedsat iht. Forsvarsministeriets [Direktiv for Den Militære Sikkerhedstjeneste indenfor Forsvarsministeriets område](#). Udvalget behandler, koordinerer og vurderer Forsvarets Efterretningstjenestes (FE) forslag til direktiver, bestemmelser og vejledninger for den militære sikkerhedstjeneste, undtagen på informationssikkerhedsområdet.

I udvalget deltager repræsentanter for koncernens myndigheder jf. direktivet og kommissoriet. FE varetager formandskabet i udvalget.

Forsvarsministeriets CISO (Chief Information Security Officer) deltager i eller lader sig repræsentere på møderne i udvalget med henblik på koordination med informationssikkerhedsområdet.

5.2 CISO Forum

På informationssikkerhedsområdet sker den overordnede koordination i koncernen i CISO Forum. Forummet sætter strategisk retning for informationssikkerhedsindsatsen og behandler forslag til direktiver, bestemmelser og vejledninger samt blandt andet awareness tiltag inden for informationssikkerhed. I forummet deltager Forsvarsministeriets CISO, CISO'erne ved styrelserne, andre ledelsesrepræsentanter fra Koncern Cyber- og Informationssikkerhed (CID, se pkt. 7.3 nedenfor), samt repræsentanter for myndigheder på styrelsesniveauet uden CISO'er. CISO Forum ledes af Forsvarsministeriets CISO. Væsentlige sager koordineres desuden i koncernstyringskredsen.

6. SIKKERHEDSTJENESTENS BESTANDDELE

Den militære sikkerhedstjeneste er opdelt i to hovedområder:

- Sikkerhedsefterretningstjeneste
- Forebyggende sikkerhedstjeneste

6.1 Sikkerhedsefterretningstjeneste

Den sikkerhedsmæssige trussel omfatter aktiviteter, der har til formål at tilvejebringe klassificerede og sensitive oplysninger om koncernens organisation, kapaciteter, virksomhed og hensigter. Truslen omfatter tillige aktiviteter, der kan hindre eller vanskeliggøre løsningen af koncernens opgaver.

Sikkerhedsefterretningstjeneste (SIK-E) omfatter informationsindhentning, analyse og vurdering af de trusselsskabende aktiviteter, der kan rettes mod koncernen på såvel kortere som længere sigt. Resultaterne heraf rapporteres til relevante myndigheder inden for koncernen, hvor de er forudsætningsskabende for gennemførelse af risikovurderinger.

SIK-E indgår som en del af grundlaget for den forebyggende sikkerhedstjeneste (SIK-F).

SIK-E analyserer og vurderer trusselsskabende aktiviteter i relation til følgende områder:

- **Terrorisme** omfatter ulovlig brug af eller trusler om brug af magt eller vold imod individer eller ejendom i forsøg på at tvinge eller skræmme regeringer eller samfund til at opnå politiske, religiøse eller ideologiske mål (jf. AAP 6).
- **Spionage** omfatter skjult indhentning af alle slags oplysninger vedrørende landets sikkerhed og koncernens evne til at forsvare nationens integritet. Endvidere omfatter spionage indhentning mod danske udsendte enheder og personel med henblik på at indsamle viden om planer, muligheder og kapaciteter.
- **Sabotage** omfatter bevidst ødelæggelse eller ubrugeliggørelse, eller forsøg herpå, af enhver form for udstyr, materiel eller faciliteter i den hensigt at vanskeliggøre eller hindre løsning af opgaver.
- **Undergravende virksomhed** omfatter bevidst påvirkning af koncernens personel i den hensigt at undergrave dets moral, loyalitet og forsvarsvilje (fx ved chikane). Området omfatter tillige aktivitet, der har til formål bevidst at skade koncernens omdømme i befolkningen.
- **Kriminalitet** omfatter enhver form for kriminelle handlinger rettet mod koncernen og dens ansatte. Området omfatter således organiseret kriminalitet, banderelateret kriminalitet samt almindeligt forekommende kriminelle handlinger som hærværk, indbrud, tyveri, vold mm.
- **Civile uroligheder** omfatter ulovlige demonstrationer, opløb og lign. rettet mod koncernen og dens etableringer.
- **Cyberangreb** omfatter hændelser, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til koncernens data, systemer, digitale netværk eller digitale tjenester.

6.2 Forebyggende sikkerhedstjeneste

SIK-F omfatter en risikobaseret udvikling og implementering af normalt længerevarende beskyttelsesforanstaltninger (risikobegrænsning) inden for følgende delområder:

- **Generel sikkerhed** omfatter krav til sikkerhedstjenestens organisering og styring, herunder ansvarsfordeling, uddannelse og kontrolvirksomhed samt sikkerhedsofficerernes opgaver. Desuden omfatter området en beskrivelse af de militære klassifikationsgrader samt forhold vedr. offentliggørelse og aktindsigt. Delområdet skaber forudsætninger for, at virksomheden inden for øvrige delområder kan gennemføres.
- **Personelsikkerhed** omfatter foranstaltninger til beskyttelse af forswarets personel mod spionage, undergravende virksomhed og kriminalitet. Desuden omfatter personelsikkerhed foranstaltninger, der har til formål at vurdere personellet's sikkerhedsmæssige kvalifikationer m.h.p. meddelelse af relevant sikkerhedsgodkendelse.
- **Materielsikkerhed** omfatter foranstaltninger til beskyttelse af materiel, herunder især kryptoudstyr, våben, ammunition og eksplosivstoffer mod spionage, sabotage og anden kriminalitet.
- **Dokumentsikkerhed** omfatter foranstaltninger til beskyttelse af informationsbærende materialer (dokumenter, kort, videobånd, lydbånd, og andre informationsbærende lagremedier) mod spionage, kompromittering, hærværk, tyveri og tab.
- **Operationssikkerhed** omfatter foranstaltninger til beskyttelse af informationer om operationer, øvelser og anden hertil knyttet aktivitet mod spionage. Operationssikkerhed er en operativ opgave og et operativt ansvar.
- **Informationssikkerhed** omfatter i denne bestemmelse foranstaltninger til beskyttelse af koncernens systemer under behandling, lagring og transmission af informationer. Systemerne skal navnlig beskyttes mod spionage, sabotage, anden kriminalitet og kompromittering, og under opretholdelse af fortrolighed, integritet, og tilgængelighed. Det

gælder såvel informationsbærende som ikke informationsbærende systemer, som understøtter vigtige forretningsprocesser.

- **Fysisk sikkerhed** omfatter foranstaltninger i form af mekanisk sikring, elektronisk overvågning og bevogtning til beskyttelse af etableringer og deployerbare kapaciteter, herunder materiel, dokumenter og informations- og kommunikationssystemer mod navnlig spionage, sabotage, anden kriminalitet og kompromittering.
- **Industrisikkerhed** omfatter foranstaltninger til beskyttelse af virksomheder, der udfører klassificeret arbejde for koncernen eller for udenlandske myndigheder, mod spionage, sabotage, undergravende virksomhed, terrorisme, anden kriminalitet og it-angreb mv.

7. ANSVAR OG ORGANISATION

7.1 Forsvarschefen

FC har ansvaret for den militære sikkerhedstjeneste inden for FMN koncernområde, undtagen på informationssikkerhedsområdet hvor ansvaret påhviler Forsvarsministeriet.

7.2 Forsvarets Efterretningstjeneste

FE leder og kontrollerer på FC's vegne den militære sikkerhedstjeneste inden for FMN koncernområde.

FE analyserer og vurderer de trusler, der kan rettes mod koncernen.

FE udarbejder forslag til de bestemmelser, direktiver og vejledninger, der er nødvendige for styring af den militære sikkerhedstjeneste (koncernens basissikkerhed). FE foranlediger forslagene behandlet i FMN SIKU og forelægger de endelige forslag for FC til godkendelse. FE yder rådgivning i forbindelse med den militære sikkerhedstjeneste, godkender sikkerhedsmæssige foranstaltninger, varetager sagsbehandling af sikkerhedsspørgsmål, behandler sikkerhedsgodkendelse af personel og systemer samt gennemfører uddannelse inden for sikkerhedsområdet.

7.3 Forsvarsministeriet, Koncern Cyber- og Informationssikkerhed

Det overordnede ansvar for informationssikkerheden i koncernen er forankret ved Forsvarsministeriet, som udsteder direktiver og bestemmelser på området, yder rådgivning og vejledning samt fører tilsyn med informationssikkerheden i koncernen. Forsvarsministeriets CISO udøver ansvaret gennem sikkerhedsorganisationen Koncern Cyber- og informationssikkerhed (CID). CID er nærmere beskrevet i den koncernfælles cyber- og informationssikkerhedspolitik.

7.4 Forsvarskommandoen

Forsvarskommandoen (FKO) deltager gennem FMN SIKU i behandling af direktiver, bestemmelser og vejledninger for den militære sikkerhedstjeneste. FKO udgiver de af FC godkendte direktiver, bestemmelser og vejledninger.

7.5 Styrelser, Hjemmeværnskommandoen, værnskommandoer og øvrige institutioner

Styrelserne, Hjemmeværnskommandoen (HJK), værnskommandoerne og øvrige institutioner deltager gennem FMN SIKU, jf. Forsvarsministeriets [Direktiv for Den Militære Sikkerhedstjeneste indenfor Forsvarsministeriets område](#), i behandling af direktiver, bestemmelser og vejledninger for den militære sikkerhedstjeneste.

Myndighederne kan inden for eget ansvarsområde udgive supplerende bestemmelser inden for den militære sikkerhedstjeneste, herunder om informationssikkerhed.

Myndighederne er ansvarlige for, at der ved underlagte myndigheder og enheder gennemføres den fornødne risikostyring jf. kapitel 9 samt kapitel 6 og FMNBST 358-2 om risikostyring inden for informationssikkerhed.

7.6 Garnisonskommandanter

På etablissementer, hvor der er flere myndigheder og enheder samlet, udpeger de lokale chefer for de på etablisementet repræsenterede myndigheder i samråd en repræsentant fra chefgruppen (eksempelvis en stabschef), der pålægges ansvaret for, som garnisonskommandant, at koordinere den samlede militære sikkerhedstjeneste. Der bør, hvis forholdene taler herfor, nedsættes et "Koordinationsudvalg vedrørende militær sikkerhed" (KUV-MILSIK), der skal tilgodese behovet for at koordinere den militære sikkerhedstjeneste. Dette gælder navnlig den fysiske sikkerhed. De udpegede garnisonskommandanter fremgår af bilag 1.

Eksempel på forretningsorden for KUV-MILSIK og områder inden for hvilke, der skal foretages koordination, fremgår af bilag 3 til kapitel 9.

8. DETAILANSVAR

8.1 Chefen

Chefen (myndighedschefen, direktøren, lederen m.fl.) er ansvarlig for at lede den militære sikkerhedstjeneste, herunder for gennemførelse af risikostyring inden for eget ansvarsområde (se pkt. 9). Chefen skal således have indsigt i og acceptere de sikkerhedsmæssige risici, der er forbundet med løsning af myndighedens eller enhedens opgaver. Chefen bliver dermed risikoejer jf. principperne om risikostyring.

Chefen skal sikre, at der udarbejdes risikovurderinger, og at der på baggrund heraf udgives relevante sikkerhedsinstrukser og sikringsplan(er), der beskriver, hvordan det lokale sikkerhedsmiljø etableres og drives.

Det er chefens ansvar, at alle medarbejdere har den fornødne sikkerhedsforståelse. Dette opnås gennem en målrettet uddannelse omfattende såvel basale som specifikke krav til og procedurer for den militære sikkerhed.

8.2 Projektorganisation

Chefen (lederen eller formanden) for et projekt, der gennemføres uden for basisorganisationen (projektgruppe, arbejdsgruppe, midlertidig oprettede stabe mv.), er ansvarlig for den militære sikkerhedstjeneste i forbindelse med projektet, herunder at der gennemføres den fornødne risikostyring. I tilknytning hertil udarbejdes nødvendige og evt. midlertidige sikkerhedsinstrukser.

8.3 Overordnet sikkerhedsofficer

Ved større myndigheder kan chefen udpege en overordnet sikkerhedsofficer, der er ansvarlig over for chefen og er dennes rådgiver vedrørende udøvelse af den militære sikkerhedstjeneste, undtagen på informationssikkerhedsområdet (se bilag 2).

8.4 Sikkerhedsofficer

Ved alle institutioner, myndigheder og enheder, herunder deployerbare kapaciteter, skal chefen udpege en sikkerhedsofficer (SIKOF), der refererer direkte til chefen eller til den overordnede SIKOF, hvor en sådan er udpeget. SIKOF's opgaver relaterer sig til myndighedens eller enhedens opgaveportefølje. SIKOF's væsentligste opgave er den praktiske gennemførelse af risikostyring. I alle tilfælde danner nærværende bestemmelse grundlag for sikkerhedsofficerernes løbende styring af den militære sikkerhedstjeneste. SIKOF kan i den forbindelse rette direkte henvendelse til Den Militære Sikkerhedsafdeling ved FE. En oversigt over SIKOF generelle opgaver fremgår af bilag 2.

8.5 Assisterende sikkerhedsofficer

Chefen kan udpege assisterende SIKOF, evt. for specifikke delområder, fx fysisk sikkerhed eller et geografisk område. Behovet vil normalt afhænge af organisationens størrelse og kompleksitet. For en assisterende SIKOF er det væsentligt, at opgave, ansvarsområde, kommandoforhold og meldevej er veldefineret. En assisterende SIKOF bør således referere til en SIKOF ved samme myndighed eller institution og kunne virke som stedfortræder i SIKOF fravær.

8.6 Informationssikkerhedsofficerer

Ved koncernens styrelser og øvrige myndigheder på styrelsesniveauet skal styrelseschefen efter behov udpege informationssikkerhedsofficerer (ISOF) som supplement til de roller, der varetager driften af styrelsernes ledelsessystemer for informationssikkerhed. Disse roller er beskrevet i FMNBST 358-1 om informationssikkerhedsledelse. Ved de til styrelserne direkte underliggende myndigheder (stabe, kommandoer og øvrige myndigheder), skal cheferne udpege en ISOF for hver af disse til koordination og varetagelse af informations-sikkerhedsopgaver. ISOF kan her ikke samtidig fungere som SIKOF.

Ved øvrige underliggende myndigheder og enheder skal chefen udpege de nødvendige ISOF'er og/eller informationssikkerhedsmedarbejdere efter behov. Opgaverne kan her eventuelt varetages af en udpeget SIKOF. Det er chefens ansvar at sikre, at medarbejderne kan varetage informationssikkerhedsopgaver som foreskrevet i bestemmelsesgrundlaget, herunder i koordination med ISOF ved foresatte myndighed.

Myndigheder og enheder kan vælge at udpege en eller flere Terminal Area Security Officers (TASO'er) til støtte for ISOF'ernes opgavevaretagelse. TASO'er kan varetage visse informationssikkerhedsforanstaltninger for systemerne, brugerstyring samt rådgivning af brugerne.

Alle myndigheder skal sikre, at ansvars- og referenceforhold mellem ISOF og andre roller i sikkerhedsorganisationen er fastlagt, tydeligt beskrevet og kommunikeret.

ISOF's generelle opgaver er beskrevet i bilag 2.

8.7 Kryptosikkerhedsofficer

Ved alle koncernens myndigheder og enheder, herunder deployerbare kapaciteter, hvor der anvendes kommunikationssystemer med kryptoudstyr og nøglematerialer, skal chefen udpege en kryptosikkerhedsofficer (KRYSO). KRYSO's opgaver er beskrevet i kapitel 6, bilag 3.

8.8 Personligt ansvar

Enhver, der er ansat eller beskæftiget inden for koncernen, skal kende de sikkerhedsmæssige forpligtigelser, som tjenesten medfører. Overholdelse af gældende sikkerhedsbestemmelser påhviler således den enkelte såvel i som uden for tjenesten. Det påhviler endvidere alt personel at rapportere til nærmeste foresatte, SIKOF eller direkte til chefen om observationer, uregelmæssigheder eller hændelser, der kan have sikkerhedsmæssig betydning og dermed udgøre en risiko for enheden. Se kapitel 10 om rapportering af sikkerhedsbrud.

9. RISIKOSTYRING

Den militære sikkerhedstjeneste styres ud fra principperne om risikostyring.

Risikostyring er en optimeringsproces, der kontinuerligt tilpasser sikkerhedsmiljøet til myndighedens aktiver i forhold til truslerne således, at chefen netop kan acceptere risikoen.

Sikkerhedsmiljøet betegner det samlede sæt af beskyttelsesforanstaltninger og deres samvirke i forhold til aktiverne, fx dokumentssikkerhed, informationssikkerhed og personssikkerhed. Ved aktiver forstås materiel, personel, informationer, infrastruktur mv. Risikostyringsprocessen skal ske i samspil med udvikling, drift og økonomi således, at der opnås helhedsløsninger.

Principperne om risikostyring medfører i øvrigt:

- At der træffes ledelsesbeslutninger på alle niveauer
- At beskyttelse skal være "cost-effective". Dvs., at den ikke skal etableres for enhver pris
- At styringen skal gennemføres systematisk og struktureret under anvendelse af standardiserede processer og terminologi
- At ekspertviden og sund fornuft indgår i processen
- At risikostyringsprocesserne skal dokumenteres
- At der er klare sammenhænge mellem årsager og virkninger
- At der skabes samklang mellem sikkerhed og brugerkrav gennem fælles forståelse af sikkerhedsbehov og -muligheder.

Vejledning i risikostyring, herunder udarbejdelse af risikovurdering, fremgår af kapitel 9.

Koncernens risikostyring i forhold til informationssikkerheden, jf. kapitel 6, skal ske på baggrund af den overordnede ramme og kriterierne i Koncern Cyber- og Informationssikkerhedspolitikken samt krav og vejledning i FMNBST 358-2 om risikostyring inden for informationssikkerhed.

10. SIKKERHEDSUDDANNELSE

Kravene til militær sikkerhed er mangeartede og på nogle områder komplekse. Det er derfor nødvendigt, at der på alle niveauer inden for koncernen tilrettelægges og gennemføres en differentieret sikkerhedsuddannelse af alt personel. Uddannelsen skal ikke blot meddele konkrete sikkerhedsregler og procedurer, men også medvirke til at opbygge og vedligeholde personellet's sikkerhedsforståelse og opmærksomhed.

10.1 Sikkerhedsforståelse

Personellet's sikkerhedsforståelse og opmærksomhed er en grundlæggende forudsætning for, at en afbalanceret militær sikkerhed kan opretholdes.

Sikkerhedsforståelse defineres som personellet's evne og vilje til at anvende de militære sikkerhedsregler, metoder og procedurer, der er knyttet til ansættelsen og funktionen. Det er således væsentligt, at personellet kan se, at militær sikkerhed giver mening.

10.2 Uddannelsesprogram

Ved alle myndigheder og enheder skal der gennemføres et uddannelsesprogram, der har til formål at opbygge og vedligeholde personellet's sikkerhedsforståelse. Uddannelsesprogrammet skal som minimum omfatte militær sikkerhed i forhold til:

- ansættelsen
- tiltrædelse i ny funktion
- afgang fra funktion eller ansættelsesforhold.

Desuden skal uddannelsesprogrammet omfatte løbende vedligeholdelse af sikkerhedsforståelsen. Uddannelsesprogrammet skal fremgå af sikkerhedsinstruksen.

Retningslinjer for udarbejdelse af et uddannelsesprogram for militær sikkerhed fremgår af bilag 3.

11. KONTORSIKKERHED

Kontorsikkerhed omfatter de foranstaltninger, der skal træffes på det enkelte kontor/arbejdsplads til imødegåelse af kompromittering af klassificeret materiale, mens det behandles og opbevares i kontorer, mødelokaler, arkiver m.v.

Alt tjenstgørende personel er ansvarlige for, at uvedkommende ikke får adgang til eller indsigt i klassificeret materiale.

11.1 Kontorer mv.

Klassificeret materiale må ikke efterlades i kontorer mv., hvor kravene til opbevaring af klassificeret materiale ikke er opfyldt. Materialet skal enten medtages eller overdrages til en bemyndiget person.

Når kontorer mv. forlades ved tjenestetids ophør, skal personalet sikre sig, at klassificeret materiale er opbevaret i godkendte opbevaringsmidler, og at intet klassificeret udstyr er tilgængeligt for uvedkommende.

11.2 Mødelokaler

Personel, der er ansvarlig for planlægning, tilrettelæggelse og afvikling af møder, hvor klassificeret materiale behandles, skal sikre sig, at mødelokalet opfylder minimumskravene til sikringsforanstaltninger, for så vidt angår mulighed for sikker aflåsning, opbevaring af klassificeret materiale, eventuel bevogtning samt etablering af adgangs- og udgangskontrol.

Tekniske sikkerhedseftersyn rekvireres i henhold til kapitel 6.

Ved mødets afslutning skal det sikres, at alt klassificeret materiale er fjernet fra lokalet.

11.3 Kontorudstyr

Bestemmelser for opstilling af elektronisk kontorudstyr (fx It-udstyr, telefon og telefax mv.) fremgår af kapitel 6.

11.3.1 Tilintetgørelse af informationsbærende materiale (makulering).

11.3.1.1 Tilintetgørelseskrav

Materiale, der er klassificeret FORTROLIGT (FTR) og højere, skal tilintetgøres på en sådan måde, at informationerne efter tilintetgørelsen ikke kan rekonstrueres.

Tilintetgørelse af materiale klassificeret FTR og højere skal finde sted ved institutionen, myndigheden eller tjenestestedet - henset til ansvar og kvitteringsprocedure.

Materiale, der er klassificeret TILTJENESTEBRUG (TTJ) skal tilintetgøres på en sådan måde, at materialets indhold ikke umiddelbart kan læses af uvedkommende.

Såfremt tilintetgørelse af materiale klassificeret TTJ og FTR finder sted ved offentlige eller private destruktionsfirmaer (genbrugsfirmaer/forbrændingsanlæg), der er godkendt af FE, skal dette ske under konstant kontrol af en sikkerhedsgodkendt person fra tjenestestedet.

Materialet må ikke afleveres til destruktionsfirmaet.

Makulaturen efter tilintetgørelsesprocessen betegnes som værende afklassificeret.

11.3.1.2 Tilintetgørelsesmetoder.

Tilintetgørelse af klassificeret materiale gennemføres ved anvendelse af makuleringsmaskiner. Brænding af store mængder klassificeret materiale uden forudgående makulering kan i særlige tilfælde gennemføres ved offentlige eller private forbrændingsanlæg. FE skal ind-

drages i hvert enkelt tilfælde. I nødsituationer og under feltmæssige forhold kan der foretages brænding af klassificeret materiale, evt. i en improviseret forbrændingsovn. Ved brænding skal det kontrolleres, at forbrændingen er fuldstændig, og at asken findeles, således at intet klassificeret materiale efterlades uden at være tilintetgjort

Beskrivelse af kontorsikkerhed fremgår af bilag 7.

12. KLASSIFIKATION

12.1 System

Den militære sikkerhedstjeneste tilrettelægges og udføres på grundlag af følgende klassifikationssystem, hvis klassifikationsgrader er bestemmende for den grad af beskyttelse, der skal ydes materialet.

12.2 Klassifikationsgrader.

12.2.1 National/NATO/EU.

NATIONAL	NATO	EU
YDERST HEMMELIGT (YHM)	COSMIC TOP SECRET (CTS)	TRÈS SECRET UE
HEMMELIGT (HEM)	NATO SECRET (NS)	SECRET UE
FORTROLIGT (FTR)	NATO CONFIDENTIAL (NC)	CONFIDENTIEL UE
TIL TJENESTEBRUG (TTJ)	NATO RESTRICTED (NR)	RESTREINT UE

Andre nationers nationale klassifikationsgrader fremgår af bilag 4.

12.2.2 Internationale (bilaterale).

Ved bilateral udveksling af klassificeret materiale anvendes klassifikationsgraderne:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED

(Mærkningerne COSMIC, NATO og UE kan ikke anvendes ved bilateral udveksling af klassificeret materiale, selv om denne finder sted til parter inden for NATO eller EU.

12.3 Principper for klassifikation og sikkerhedsbeskyttelse.

12.3.1 Klassifikation.

En klassifikationsgrad fastsættes, ændres og ophæves under hensyntagen til den skade, som bortkomst, kompromittering eller ødelæggelse vurderes at kunne medføre for statens, allierede staters, koncernens samt enkeltpersoners sikkerhed.

Ved fastsættelse af klassifikationsgrad anvendes efternævnte principper:

- YDERST HEMMELIGT (COSMIC TOP SECRET, TRÈS SECRET UE, FOCAL TOP SECRET)
Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse vil kunne forvolde Danmark eller landene i NATO eller EU overordentlig alvorlig skade.

- **HEMMELIGT (NATO SECRET, SECRET UE SECRET)**
Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse vil kunne forvolde Danmark eller landene i NATO eller EU alvorlig skade.
- **FORTROLIGT (NATO CONFIDENTIAL, CONFIDENTIEL UE CONFIDENTIAL)**
Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse vil kunne forvolde Danmark eller landene i NATO eller EU skade.
- **TIL TJENESTEBRUG (NATO RESTRICTED, RESTREINT UE/EU RESTRICTED)**
Denne klassifikationsgrad anvendes om informationer, der ikke må offentliggøres eller komme til uvedkommendes kendskab.

Når materiale klassificeres, skal udstederen være opmærksom på ovennævnte bestemmelser og bremse enhver tendens til at anvende for høj eller for lav klassifikationsgrad. Selv om en høj klassifikationsgrad umiddelbart kunne tænkes at sikre en information større beskyttelse, kan rutinemæssig anvendelse af en for høj klassifikationsgrad nedsætte tilliden til klassifikationsordningen.

På den anden side må informationen ikke klassificeres for lavt blot for at undgå de begrænsninger, de enkelte klassifikationsgrader medfører.

En praktisk klassifikationsvejledning med krav til mærkning og beskyttelse fremgår af bilag 5.

Opmærksomheden skal henledes på, at materiale, der ikke kræver nogen form for sikkerhedsbeskyttelse, ikke skal påføres hverken militær sikkerhedsklassifikation eller særlig mærkning.

Når der i det efterfølgende og øvrige kapitler nævnes TTJ, FTR, HEM eller YHM menes tillige de tilsvarende NATO og EU klassifikationsgrader jf. pkt. 12.2.1.

I de tilfælde hvor NATO eller EU sikkerhedskrav til håndteringen er højere eller markant anderledes end de tilsvarende nationale, vil det fremgå af teksten.

12.4 Sanering.

Udstederen bør jævnligt gennemgå de tidligere udfærdigede klassificerede informationer med henblik på at nedklassificere eller afklassificere disse, i det omfang de hensyn, der betingede klassifikationsgraden, ikke længere er til stede. Ned- og afklassificering meddeles til dem, der har modtaget informationerne.

13. MÆRKNINGER OG BETEGNELSER

13.1 COSMIC

Mærkningen tilkendegiver, at materialet er NATO-ejendom, der ikke må overdrages til myndigheder uden for organisationen uden særlig tilladelse.

Mærkningen COSMIC kan alene påføres materiale med klassifikationsgraden TOP SECRET. Materialet beskyttes på særlig måde og behandles udelukkende af dertil bemyndiget personel.

13.2 ATOMAL

Mærkningen tilkendegiver, at materialet indeholder ATOMAL informationer og samtidig er NATO-ejendom, der ikke må overdrages til myndigheder uden for organisationen.

Materiale med mærkningen ATOMAL er altid klassificeret som minimum NATO CONFIDENTIAL.

Materialet beskyttes på særlig måde og behandles udelukkende af dertil bemyndiget personel, som anført i kap. 4. pkt. 12.2.

13.3 NATO

Mærkningen tilkendegiver, at materialet er NATO-ejendom, der ikke må overdrages til myndigheder uden for organisationen uden særlig (udsteders) tilladelse.

Mærkningen NATO kan påføres materiale med klassifikationsgraderne SECRET, CONFIDENTIAL og RESTRICTED eller med betegnelsen, UNCLASSIFIED.

13.4 EU

Mærkningen tilkendegiver, at materialet er EU-ejendom, der ikke må overdrages til myndigheder uden for organisationen uden særlig (udsteders) tilladelse.

Mærkningen UE kan påføres materiale med klassifikationsgraderne TRÈS SECRET, SECRET, CONFIDENTIEL og RESTREINT.

13.5 ESDP/PESD

Betegnelsen "ESDP/PESD" (European Security and Defence Policy)/PESD (Politique Européenne de Sécurité et de Défence) kan anføres på dokumenter, som vedrører EU eller en eller flere af dets medlemsstaters sikkerhed eller forsvar, eller som vedrører militær eller ikke-militær krisestyring.

13.6 PfP

Skriftlig information, der udveksles under PfP programmerne, skal identificeres med mærkningen PfP.

Alle udvekslede dokumenter, hvad enten disse stammer fra NATO eller Partnere, skal desuden være påført korrekt mærkning/klassifikation (UNCLASSIFIED, RESTRICTED, CONFIDENTIAL eller SECRET) i overensstemmelse med den af udfærdigeren fastsatte sensitivitet, og i tilfælde af eksisterende NATO dokumenter, svarende til deres NATO klassifikation. Såfremt en udfærdiger beslutter, at fordeling af et bestemt dokument også skal begrænses til bestemte nationale modtagere, skal dette anføres ved at indsætte:

"Navn(e) på det/de pågældende modtagerland(e)... ONLY" på en separat linie umiddelbart under identifikations- og klassifikationsmærkningen, fx således:

NATO/PfP RESTRICTED
ALBANIA ONLY

13.7 UNCLASSIFIED (UNCLAS).¹

Betegnelsen angiver, at omhandlede materiale ikke kræver sikkerhedsbeskyttelse, som angivet i pkt. 12.

13.8 KLASSEFIKATIONSMEARKNING.

Klassifikationsmærkningens udformning og placering på dokumenter mv. fremgår af bilag 6.

- For klassificerede informationer i dokumentform placeres klassifikationsgraden som tydelig mærkning på alle dokumentets sider midtstillet for oven og for neden. Blanke sider klassifikationsmærkes ikke.
- Klassifikationsgraden skrives, trykkes eller stemples med VERSALER, der har mindst samme størrelse som dokumentets øvrige anvendte skrifttyper.

¹ Den nationale betegnelse UKLASSIFICERET (UKL) er udgået 1. juni 2005.

- Bøger, hæfter mfl. klassifikationsmærkes på samtlige sider, inkl. omslagets for- og bagside samt ryg, hvis muligt.
- Består et dokument af flere ark, skal arkene være forsvarligt sammenhæftede, og siderne skal sidenummereres.
- Informationsbærende materiale, der ikke kræver sikkerhedsbeskyttelse, skal jf. kap. 1, ikke påføres klassifikation eller særlig mærkning.
- Kryptonøglemateriale o.l. kan - af hensyn til bestemmelserne for mærkning af sådant materiale - afvige fra de anførte retningslinjer for klassifikationsmærkning.
- Film, videobånd og andre tilsvarende medier, samt emballage hertil, klassifikationsmærkes på et iøjnefaldende sted. Klassifikationen skal som minimum fremgå af billedet ved forevisningens indledning og afslutning.
- Ved lydoptagelser indtales klassifikationen i indledningen og afslutningen.
- Transparenter klassifikationsmærkes i hvert enkelt tilfælde på iøjnefaldende vis.
- Klassifikationsmærkning af elektroniske lagermedier, som fx USB-nøgler, CD, DVD o. lign. skal så vidt muligt være i overensstemmelse med ovenstående. Se også kapitel 6, afsnit IV.
- Ved enkeltafsnit og punkter, hvor klassifikationen er lavere end dokumentets generelle klassifikation, kan dette anføres umiddelbart efter afsnittets/punktets nummer. Eksempel "7. (FTR) Tekst..." I tilfælde hvor et afsnit ikke er klassificeret, markeres det således. Eksempel "8. (IKL) Tekst"
- For mærkninger gælder tilsvarende bestemmelser, som anført ovenfor.

13.9 SÆRLIG MÆRKNING.

13.9.1 Need-to-know.

Efter "need-to-know" princippet kan sager mærkes for at fastsætte yderligere begrænsninger i deres håndtering, fx med henblik på at præcisere den personkreds, som sagerne må overdrages til.

Sådanne "need-to-know" mærkninger kan eksempelvis være Personoplysning, fortrolig (POF), FORTROLIGT-KOMMERCIELT (FTR-K), TIL INTERN BRUG, TIL SNÆVERT BRUG, KUN TIL NATIONALT BRUG, KUN FOR STABENS ØJNE o. lign.

Klassifikationen på sager, der er mærket efter "need-to-know" princippet, er bestemmende for hvorledes de skal opbevares og håndteres.

"Need-to-know" mærkningen angiver yderligere begrænsninger i sagernes håndtering.

Bestemmelser for håndtering af POF fremgår af FMNBST 400-1, "Bestemmelse om mærkning og håndtering af personoplysninger, der skal mærkes "PERSONOPLYSNING, FORTROLIG" – POF".

Bestemmelser for håndtering af FTR-K fremgår af FMIVEJL 358-01, "Vejledning for håndtering af materiale mærket FORTROLIGT-KOMMERCIELT".

14. NED- OG AFKLASSIFICERING

Alene udstedende myndighed kan ændre klassifikationen på informationsbærende materialer. Myndigheden er i så fald ansvarlig for, at alle modtagere underrettes.

Nedenstående regler for ned- og afklassificering er kun gældende for nationale sager. Ved ned- og afklassificering skal den oprindelige klassifikationsgrad overstreges og en eventuelt ny påføres.

14.1 Nedklassificering

Ved nedklassificering forstås henføring til en lavere klassifikationsgrad. Nedklassificeringen af TTJ klassificeret materiale indebærer afklassificering, og materialet skal mærkes AF-KLASSIFICERET.

14.2 Afklassificering

Ved afklassificering forstås ophævelse af enhver form for klassificering. TTJ klassificeret materiale er automatisk afklassificeret, når det er 20 år gammelt. For materiale klassificeret FTR eller højere gælder en fristforlængelse til 60 år. Materialet mærkes således:

Afklassificeret ÅÅÅÅ-MM-DD

15. ANSVAR FOR KLASSIFICERING OG MÆRKNING

15.1 Klassifikation

Udfærdigende eller iværksættende myndighed er - inden for eget ansvarsområde - ansvarlig for, at dokumenter, materiel, projekter og operationsplaner mv. er klassificeret eller mærket i overensstemmelse med de principper, der er anført oven for.

15.2 Varighedsmærkning

Ved oprettelse af et dokument/materiale klassificeret TTJ, skal udfærdigende myndighed, så vidt det er muligt, anføre en dato eller frist, efter hvilken dokumentet/materialet kan afklassificeres, fx således:

TIL TJENESTEBRUG

Afklassificeret ÅÅÅÅ-MM-DD.

I tilfælde hvor et dokument/materiale påføres en "need-to-know" mærkning, kan udstederen tilsvarende fastsætte en dato for, hvornår mærkningen ophører, fx således:

TIL INTERNT BRUG

MÆRKNINGEN OPHØRER ÅÅÅÅ-MM-DD

Med henblik på aflevering til Statens Arkiver ophører sikkerhedsbeskyttelsen af "need-to-know" mærket materiale automatisk, når det er 20 år gammelt.

16. OFFENTLIGGØRELSE

16.1 Offentliggørelse.

Materiale, der er klassificeret eller påført "need-to-know" mærkning, må ikke offentliggøres. Offentliggørelse forudsætter, at den udstedende myndighed afklassificerer materialet eller meddeler sin tilladelse til at mærkningen fjernes.

Materiale, der er mærket AFKLASSIFICERET, eller ikke er påført nogen klassifikation eller særlig mærkning, kan offentliggøres af enhver myndighed, der har materialet i hænde. Dette gælder dog ikke, hvis en offentliggørelse af materialet vil være i strid med de hensyn, der efter lovgivningen kan begrunde nægtelse af aktindsigt og registerindsigt, jf. pkt. 18. Ved tvivl skal den udstedende myndighed normalt høres.

På grund af tidligere gældende regler for offentliggørelse må dokumenter udstedt før JUN 2005 kun offentliggøres med udstederens tilladelse. Materialet mærkes:

"MÅ OFFENTLIGGØRES".

16.2 Aflevering af arkivalier

I forbindelse med screening (klargøring af arkivalier til aflevering til Statens Arkiver) kan udstedende myndighed vælge at udsende årgangsvise oversigter over dokumenter, der fortsat er klassificerede (fristforlængede) således, at de ikke nævnte dokumenter for den anførte årgang anses som afklassificeret.

17. FRIGIVELSE

Regler og betingelser for frigivelse til andre nationer m.fl. af NATO -, EU - og nationalt klassificerede informationer fremgår af Kapitel 4.

18. AKTINDSIGT

Begæring om aktindsigt og indsigt i personoplysninger skal behandles og afgøres efter de herfor gældende regler, jf. bl.a. forvaltningsloven, offentlighedsloven samt lovgivning om persondatabeskyttelse. For nærmere orientering herom henvises til [FKOVEJL 300-1](#). Adgangen til at give aktindsigt i dokumenter og andet materiale kan være begrænset ved traktater og andre internationale aftaler. Der kan fx ikke umiddelbart gives aktindsigt i materiale, der er sikkerhedsbeskyttet i henhold til en fælles interesse for landene i NATO og EU, dvs. materiale påført en NATO eller EU klassifikation/-mærkning. Der skal dog i alle tilfælde foretages en konkret vurdering, idet det forvaltningsretlige udgangspunkt er, at myndighederne i videst mulig udstrækning skal imødekomme begæringer om aktindsigt. I den forbindelse skal det også overvejes, om der eventuelt kan ske en afklassificering af de pågældende materialer.

Det skal nøje påses, at der ikke ved meddelelse af aktindsigt sker krænkelse af væsentlige hensyn til statens sikkerhed, rigets forsvar eller rigets udenrigspolitiske interesser. Den ved Militær Straffelovs § 32, stk.1, særligt fastsatte tavshedspligt vedrørende militære hemmeligheder skal overholdes.

Opmærksomheden henledes på, at aktindsigt normalt ikke kan gives på vilkår vedrørende anvendelse af materialet, herunder at ansøgeren helt eller delvist skal undlade at offentliggøre materialet. Meddelelse af aktindsigt vil normalt indebære, at senere ansøgninger om adgang til det samme materiale skal imødekommes. Ved aktindsigt efter reglerne i arkivloven er der dog mulighed for at stille vilkår i forbindelse med adgang til arkivmaterialer.

19. ANSVAR OG PROCEDURER FOR OPBEVARING AF INFORMATIONSBÆRENDE MATERIALE (FTR OG HEM) PÅ PRIVAT BOPÆL.

Er der som følge af tjenesten undtagelsesvis behov for, at en styrelseschef, direktør, særlige medarbejdere eller tilsvarende inden for Forsvarsministeriets koncernområde skal opbevare klassificerede informationsbærende materiale (dokumenter eller elektroniske lagermedier) på bopælen, skal følgende retningslinjer efterleves.

Det er jf. kapitel 4 tilladt at medtage TTJ, FTR og HEM dokumenter på bopælen (folkeregisteradresse). For at opbevare informationsbærende materiale (TTJ, FTR og HEM) på bopælen (folkeregisteradresse), stilles der en række krav til boligens sikringsmæssige forhold.

Hvis der etableres mulighed for opbevaring af klassificerede informationsbærende materiale (FTR og HEM), skal FE i hvert tilfælde orienteres skriftligt af den pågældende myndighed.

Det er ikke tilladt at medtage og opbevare YHM materiale på bopælen, ligesom der ikke uden FE's skriftlige godkendelse må opbevares FTR og HEM klassificerede dokumenter mv. hos medarbejdere eller chefer, der er bosat uden for Rigsfællesskabet.

19.1 Procedurer

Inden klassificerede informationsbærende materiale opbevares på privat bopæl skal nedenstående punkter sikres gennemført:

1. Der skal af myndighedens SIKOF foretages en risikovurdering jf. kapitel 9. med fokus på bopælen. Den skal bl.a. beskrive mængden af dokumenter, typen af opbevaringsmedie og til hvilken klassifikationsgrad, der er behov for at opbevare, samt hvor længe opbevaringsbehovet forventes at være gældende. Risikovurderingen skal beskrive truslen for indbrud i nærområdet, sikkerhedsmiljøets styrke mv. Risikovurderingen skal jf. kapitel 9. løbende vedligeholdes bl.a. på baggrund af ændret trusselsvurdering.

2. Respektive myndighedschef (styrelseschef, direktør eller tilsvarende) skal i hvert enkelt tilfælde foretage en skriftlig godkendelse på baggrund af et konkret og dokumenteret behov, såfremt der skal opbevares klassificerede informationsbærende materiale (FTR eller HEM) på privat bopæl (folkeregisteradresse), idet risikovurderingen skal indgå som grundlag for godkendelsen.

3. SIKOF ved den pågældende myndighed skal herefter, evt. i samarbejde med FES, foretage en projektering og påse, at der etableres og installeres de nødvendige sikkerhedsmæssige tiltag iht. kapitel 4 og bilag 3 til kapitel 7. Det indskræpes, at alarmer skal terminere ved en godkendt alarmcentral.

4. Myndighedens SIKOF skal udarbejde en sikkerhedsinstruks, der dækker det sikrede og bopælen, og skal i forbindelse med den interne kontrol jævnligt, og mindst en gang om året, gennemgå SIKINST, sikkerhedsdokumentationen og sikkerhedsinstallationer for at sikre, at kravene i denne bestemmelse efterleves. Ligeledes skal regler i bestemmelsen vedr. opbevaring, medtagning, optælling mv. efterleves.

5. Inden ibrugtagning skal SIKOF gennemføre en funktionskontrol, hvor den mekaniske sikring og elektroniske overvågning gennemgås og afprøves.

6. FE kan efter anmodning fra myndigheden komme med yderligere rådgivning og evt. foretage funktionskontrol, ligesom myndigheder i forbindelse med generelle militære sikkerhedseftersyn, foretaget af FE, kan forvente kontrol af om opbevaringen på privat bopæl (folkeregisteradresse) er i henhold til gældende bestemmelser.

7. Ved sikkerhedsbrud og -hændelser rapporteres der iht. kapitel 10.

20. MILITÆRE SIKKERHEDSAFTALER

Sikkerhedsaftaler har til formål at fastlægge gensidigt forpligtende regler for beskyttelse af klassificerede oplysninger, der udveksles med andre lande og internationale organisationer.

Der er indgået sikkerhedsaftaler med følgende lande og internationale organisationer (aftaler der kun dækker militære oplysninger er markeret med M):

Australien (M), Bulgarien (M), Canada (M), Estland (M), Finland, Island, Polen (M), Letland (M), Litauen (M), Frankrig, Norge, Schweiz (M), Singapore (M), Slovakiet (M), Storbritannien (M), Sverige, Sydkorea (M), Tyskland, England (M), USA, EU-Rådet og NATO.

Kopi af aftalerne kan rekvireres ved henvendelse til FE.

OVERSIGT OVER CHEFER MED ANSVAR FOR LOKAL KOORDINATION AF DEN MILITÆRE SIKKERHEDSTJENESTE

Følgende chefer er af styrelserne pålagt som garnisonskommandanter at koordinere den militære sikkerhed på det anførte etablissement og de der til knyttede eksterne lokaliteter:

1. FORSVARSKOMMANDOEN, HÆRKOMMANDOENS OMRÅDE.

- CH/JDR Holstebro Kaserne
- CH/GHR Antvorskov Kaserne
- CH/EFR Varde Kaserne
- CH/IGR Skive Kaserne samt faciliteter på Aflandshage
- CH/TGR Ryes Kaserne
- CH/TRR Aalborg Kaserne
- CH/DAR Oksbøl Kaserne
- CH/DBH Almegaardens Kaserne
- CH/LG Høvelte Kaserne, Høveltegård, Gothersgade Kaserne og Brødeskov Kaserne
- CH SLFR Haderslev Kaserne

2. FORSVARSKOMMANDOEN, SØVÆRNSKOMMANDOENS OMRÅDE.

- CH/FLS FRH Flådestation Frederikshavn
- CH/FLS KOR Flådestation Korsør
- CH/CST Marinestation Nyholm
- CH/VBC Sjællands Odde

3. FORSVARSKOMMANDOEN, FLYVERKOMMANDOENS OMRÅDE.

- CH/ATW AAL Flyvestation Aalborg
- CH/OSW KAR Flyvestation Karup
- CH/FW SKP Flyvestation Skrydstrup

4. HJEMMEVÆRNSKOMMANDOENS OMRÅDE.

- CH/HJK Vordingborg Kaserne
- CH/TRFS Odense Kaserne
- CH/HVS Nymindegablejren
- CH/HDSSJ Søgårdlejren
- CH/HDSLIF Stensved Kaserne
- CH/HVS Slipshavn

5. FORSVARSAKADEMIETS OMRÅDE.

- CH/FAK Svanemøllen Kaserne
- CH/HO Frederiksberg Slot

6. FORSVARSMINISTERIETS EJENDOMSSTYRELSES OMRÅDE.

- CH/LSE KAS Kastellet
- CH/KS Hjørring Kaserne
- CH/KCDK ¹ Skydelejr/skydeterræner: Borris, Jægerspris, Hevringlejren

¹ Har ansvaret for koordineringen med besøgende enheder fsva. vagt og bevogtning

7. FORSVARETS SANITETSKOMMANDOS OMRÅDE.

- CH/FSK Sødalsparken, Aarhus
- CH/UDA/FSK Flyvestation Skalstrup

8. FORSVARSMINISTERIETS PERSONALESTYRELSES OMRÅDE.

- CH/FPS FPS domicil Ballerup

9. FORSVARSMINISTERIETS MATERIEL OG INDKØBSSTYRELSE.

- CH/FMI FMI domicil Ballerup

10. FORSVARETS KONCERNFÆLLES INFORMATIKTJENESTES OMRÅDE.

- CH/KAKI KAKI domicil Hvidovre

11. SPECIALOPERATIONSKOMMANDOENS OMRÅDE.

- CH/FKP Kongsøre og Sjællands Odde

12. ARKTISK KOMMANDOS OMRÅDE.

- CH/AKO AKO domicil Nuuk

SIKKERHEDSOFFICERERNE, OPGAVER OG UDDANNELSE**1. OPGAVER****1.1 Generelt**

Sikkerhedsofficerens (SIKOF), informationssikkerhedsofficerens (ISOF) og kryptosikkerhedsofficerens (KRYSOFF) opgaver tager først og fremmest udgangspunkt i myndigheds/enhedens opgaveportefølje, men også i omfanget og arten af informationer, systemer og materiel mm., der i forhold til en konkret risikovurdering skal beskyttes.

SIKOF og ISOF samt KRYSOFF skal være kendt af alt personel ved myndigheden/enheden, således at enhver kan henvende sig direkte til disse vedrørende forhold af betydning for den militære sikkerhedstjeneste og informationssikkerheden.

SIKOF, ISOF og KRYSOFF kan på chefens vegne henvende sig direkte til Forsvarets Efterretningstjeneste (FE) vedrørende sikkerhedsmæssige forhold, og er samtidig myndigheds/enhedens kontakt ved henvendelser fra FE. Ved styrelserne vil FE, hvad angår forhold vedrørende informationssikkerheden, dog typisk skulle etablere kontakt gennem den informationssikkerhedsansvarlige chef eller styrelses Chief Information Security Officeren (CISO).

1.2 Varetagelse af sikkerhedstjenesten

SIKOF og ISOF løser deres opgaver i overensstemmelse med kapitlerne i denne bestemmelse samt evt. sikkerhedsbestemmelser udgivet af foresatte myndigheder. Opgaverne, som beskrevet i det følgende, skal betragtes som eksempler på de mest forekommende opgaver. For enheder udsendt i internationale operationer tilpasses opgaverne de lokale forhold på stedet, herunder de operative vilkår.

1.2.1 Overordnet sikkerhedsofficer

- Er chefens rådgiver i alle spørgsmål vedr. den militære sikkerhed undtagen på informationssikkerhedsområdet.
- Samordner SIKOF virke ved egen stab og underlagte myndigheder/enheder.
- Kan på chefens vegne godkende sikkerhedsinstrukser og give bemyndigelser, undtagen på informationssikkerhedsområdet.

1.2.2 Sikkerhedsofficeren

- Forestår risikostyring.
- Udarbejder risikovurdering, sikkerhedsinstruks og sikringsplan.
- Tilrettelægger og gennemfører sikkerhedsuddannelse.
- Behandler sager vedrørende den militære sikkerhedstjeneste.
- Rådgiver chefen i spørgsmål og sager vedrørende den militære sikkerhedstjeneste.
- Orienterer nytiltrådte chefer om status vedr. den militære sikkerhed ved MYN/ENH, herunder navnlig risikovurderinger og sikringsplaner.
- Tilrettelægger og gennemfører på chefens foranledning intern kontrol af den militære sikkerhed ved myndigheden/enheden. Fører dokumentation for gennemført kontrolvirksomhed, herunder føring af en risikolog. Der skal herunder lægges vægt på kontrol med højt klassificerede informationer, systemer, materiel, samt våben, ammunition og eksplosivstoffer.
- Initierer i samarbejde med bl.a. centralregistraturer eller lign. mønstring af HEM klassificerede sager og materiel og udfærdiger en årlig mønstringsrapport samt foranlediger denne forelagt for chefen til godkendelse.
- Følger løbende udgivelse af rettelser til bestemmelserne for den militære sikkerhedstjeneste med henblik på justering af den lokale sikkerhedsinstruks herunder instruktion af relevant personel, fx vagtpersonel.

- Holder myndigheden, der er pålagt koordinerende opgaver, orienteret om forhold og sager af betydning for den militære sikkerhedstjeneste. Dette gælder navnlig forhold indeholdt i risikovurderingen og sikringsplanen.
- Samarbejder med og koordinerer relevante dele af sikkerhedstjenesten med ISOF og KRYSOFF samt eventuelle TASO'er.
- Rapporterer om brud på den militære sikkerhed og andre sikkerhedsmæssige hændelser.

1.2.3 Assisterende sikkerhedsofficer

Er SIKOF assistent og kan på SIKOF vegne varetage et eller flere delområder af den militære sikkerhedstjeneste afhængig af behov. Assisterende SIKOF er SIKOF stedfortræder i dennes fravær.

1.2.4 Informationssikkerhedsofficeren

ISOF'er ved styrelserne supplerer de roller, der varetager drift af ledelsessystemerne for informationssikkerhed, jf. FMNBST 358-1 om informationssikkerhedsledelse. De kan fx være tillagt opgaver vedrørende akkreditering eller udarbejdelse af lokale sikkerhedsinstrukser.

Ved underliggende myndigheder vil ISOF'erne typisk skulle varetage følgende opgaver:

- Overblik over myndighedens informationsaktiver og understøttende aktiver hertil
- Indsigt i trusselsbilledet og i sårbarheder i forhold til myndighedens aktiver
- Koordinere indsats med egenkontrol ved egen myndighed og deltage i tilsyn
- Risikostyring efter direktiv fra styrelse
- Udarbejde og opdatere lokale informationssikkerhedsinstrukser, herunder på baggrund af koncernfælles direktiver og bestemmelser m.v.
- Dialog med FE i forhold til at relevante akkrediteringer er eller kommer på plads
- Bidrage til intern uddannelses- og awareness aktivitet, f.eks. on-boarding briefinger
- Håndtering og rapportering af hændelser
- Rådgivning af myndighedschefen om informationssikkerhed
- Koordination af aktiviteter med andre sikkerhedsroller ved myndigheden
- Koordination med styrelse der driver ledelsessystemet for informationssikkerheden.

Styrelserne fastlægger rammer for og udgiver i relevant omfang instrukser om ISOF'ernes opgavevaretagelse samt støtter med rådgivning og vejledning.

Ved myndigheder, der driver IT, kan der være krav om udpegning af systemsikkerhedsofficerer (SYSOF), se kapitel 6.

1.2.5. Kryptosikkerhedsofficeren

KRYSOFF opgaver relaterer sig til krypto- og TEMPEST området. Detaljeret beskrivelse af KRYSOFF opgaver fremgår af bilag 3 til kapitel 6.

2. UDDANNELSE

Al sikkerhedspersonel inden for militær sikkerhed og informationssikkerhed skal besidde de nødvendige kompetencer i forhold til deres rolle med afsæt i den rette uddannelse og træning.

Omfanget og karakteren af sikkerhedsopgaver, der skal løses ved myndigheden/enheden, er styrende for, i hvilket omfang den udpegede SIKOF og ISOF skal gennemgå egentlig militær sikkerhedsuddannelse og uddannelse inden for informationssikkerhed.

SIKOF eller assisterende SIKOF samt ISOF/informationssikkerhedsmedarbejdere ved myndigheder/enheder uden sensitive informationer og systemer klassificeret højere end TTJ eller våben sprængstoffer og ammunition o. lign. kan eventuelt uddannes/instrueres lokalt af en uddannet SIKOF eller ISOF.

Sikkerhedsuddannelserne inden for militær sikkerhed kan findes på FE's sikkerhedsportal. På informationssikkerhedsområdet foranstalter CID uddannelsesaktiviteter, herunder i samarbejde med FKO og FE.

3. STØTTEVÆRKTØJ

Til brug for internationale operationer er der udarbejdet et støtteværktøj (kapitel 5 bilag 2 pkt. 5), der kan hjælpe sikkerhedsofficeren i overvejelser vedrørende sikkerhedsorganisationen. Værktøjets del 1 kan støtte og inspirere sikkerhedsofficeren i såvel planlægnings- som etableringsfasen.

BILAG 3, RETNINGSLINIER FOR UDARBEJDELSE AF UDDANNELSESPROGRAM FOR MILITÆR SIKKERHED

1. GENERELT

Forsvaret er i besiddelse af og anvender i stort omfang klassificerede eller på anden måde vitale og sensitive informationer, informationssystemer og materielgenstande. Dette stiller krav om sikkerhedsbeskyttelse, og om målrettet uddannelse af personalet.

Alt personel, der ansættes i koncernen, skal gennemgå en grundlæggende militær sikkerhedsuddannelse hurtigst muligt efter ansættelsen. Der ud over skal der for personel, der skal beskæftige sig med højt klassificerede informationer, systemer og vitalt- og sensitivt materiel og processer, gennemføres en lokal og mere specifik sikkerhedsuddannelse. I den forbindelse skal det understreges, at intet personel må beskæftige sig med klassificerede informationer og systemer før de er blevet sikkerhedsgodkendt.

Den grundlæggende og den lokale sikkerhedsuddannelse skal vedligeholdes gennem regelmæssige repetitioner, men mindst en gang årligt.

Omfanget af den samlede sikkerhedsuddannelse afhænger i høj grad af:

- Om medarbejderen skal beskæftige sig med oplysninger og materiel klassificeret højere end TTJ.
- Om tjenestestedet er beliggende i sikrede, kontrollerede eller overvågede områder.
- Om medarbejderen skal have adgang til vitalt og eller sensitivt materiel, våben, ammunition og eksplosivstoffer o. lign.

2. FORMÅL

Det er den militære sikkerhedsuddannelses formål at bibringe personalet viden, færdigheder og holdninger, der gør dem i stand til at anvende de sikkerhedsregler, metoder og procedurer, der er knyttet til ansættelse i forsvaret og varetagelsen af lokale og specifikke funktioner.

3. GRUNDLÆGGENDE UDDANNELSE

Den grundlæggende militære sikkerhedsuddannelse har til formål at give den nyansatte viden om de basale sikkerhedskrav, der er knyttet til ansættelsen i koncernen.

Uddannelsen gennemføres som et "lær selv program" via Forsvarets Elektroniske Skole (FELS). Link til FELS findes på FE Sikkerhedsportal på såvel KFI som Internettet. Efter bestået slutttest meddeles den nyansatte et Q i DEMARS.

Den grundlæggende sikkerhedsuddannelse bør finde sted i forbindelse med den øvrige ansættelsesprocedure eller snarest muligt efter mødet på tjenestestedet.

Følgende mål indgår i den grundlæggende sikkerhedsuddannelse:

- Have kendskab til Den Militære Sikkerhedstjenestes formål
- Have kendskab til Den Militære Sikkerhedstjenestes hoved og delområder
- Have kendskab til generelle trusler og risici
- Kunne anvende tavshedspligten
- Kunne anvende "Need to know" princippet
- Have forståelse af de militære klassifikationsgrader
- Kunne anvende oplysningspligten i forhold til konflikter med lovgivningen
- Kunne anvende "kontorsikkerhed"

- Have forståelse af opmærksomhed over for mistænkelige forhold i tjenesten (se pkt. 7)
- Have kendskab til strafferetslige forhold ved sikkerhedsbrud
- Have forståelse af rapportering af sikkerhedsbrud eller tilløb til sådanne
- Have kendskab til typiske eksempler på sikkerhedsbrud og konsekvenserne heraf.

4. LOKAL SIKKERHEDSUDDANNELSE

Den lokale sikkerhedsuddannelse har til formål at orientere nytildgået personel om myndighedens/enhedens sikkerhedsinstruks, idet myndigheden heri allerede har klarlagt hvilke regler og procedurer, der er gældende i forhold til den militære sikkerhed.

Følgende mål skal, afhængig af lokale forhold, indgå i uddannelsen:

- Have forståelse af den lokale militære sikkerhedsorganisation
- Have forståelse af generelle krav til opbevaring af klassificerede medier og materiel
- Have forståelse af de basale krav til informationssikkerhed, herunder navnlig anvendelse af bærbare lagermedier
- Kunne deltage i opholdskontrol
- Kunne betjene lokale adgangskontrolsystemer og elektroniske overvågningssystemer
- Kunne anvende militære sikkerhedsforskrifter for specifikke systemer og arbejdsgange
- Have kendskab til gennemførelse af intern kontrol af den militære sikkerhed
- Være orienteret om de 5 mest stillede spørgsmål vedr. den lokale militære sikkerhed og de hyppigst forekommende sikkerhedsbrud.

I den lokale sikkerhedsuddannelse skal der lægges vægt på den militære sikkerhed i forhold til våben, ammunition, eksplosivstoffer samt klassificeret eller på anden måde sensitivt materiel eller informationer. Her til kommer specifikke sikkerhedskrav til omgang med kryptomateriel og kryptomaterialer.

Personel, der bestrider vagtfunktioner i relation til den militære sikkerhedstjeneste, skal være nøje instrueret i udførelsen af denne tjeneste.

5. VEDLIGEHOOLDENDE SIKKERHEDSUDDANNELSE

Efter behov gennemføres repetition af relevante emner fra den grundlæggende og den lokale sikkerhedsuddannelse. Den vedligeholdende sikkerhedsuddannelse gennemføres mindst en gang om året og som opfølgning på sikkerhedsbrud.

Ud over repetition efter behov jf., pkt. 3 og 4 bør følgende mål indgå:

- Have kendskab til evt. ændringer i trussels- og risikobilledet.
- Have kendskab til ændringer i den lokale sikkerhedsinstruks.
- Være orienteret om resultaterne af intern kontrol.
- Have kendskab til konstaterede sikkerhedsbrud og deres konsekvenser
- Have kendskab til forsvarets generelle sikkerhedstilstand og de emner forsvarets øverste ledelse eller myndigheds- eller enhedschefen ønsker, at der sættes fokus på.

Den vedligeholdende sikkerhedsuddannelse bør gennemføres som "tilstedeværelse", men kan ved myndigheder og enheder, der ikke er i besiddelse af højere klassificerede informationer, systemer, våben, ammunition og eksplosivstoffer, gives i form af præsentationer på elektroniske informationssystemer.

6. SIKKERHEDSINSTRUKTION VED AFGANG FRA TJENESTE

- Have viden om tavshedspligten (indskærpelse).
- Have viden om muligheder og bestemmelser for fortsat adgang til forsvarets etableringer.

7. OPMÆRKSOMHEDSUDDANNELSE

Opmærksomhed overfor mistænkelige forhold i tjenesten indgår i såvel den grundlæggende som den vedligeholdende sikkerhedsuddannelse.

Mange sikkerhedsbrud eller tilløb til disse vil kunne undgås, hvis der i tjenesten udvises opmærksomhed over for såvel eksterne som interne trusler. Eksterne trusler er fx spionage, terrorhandlinger og ulovlig indtrængen, mens interne trusler oftest kan henføres til koncernens eget personel, fx, at en medarbejder har kontakt til kriminelle miljøer eller udviser manglende sikkerhedsforståelse. Der ses til stadighed eksempler på, at koncernens ansatte overgiver informationer til uvedkommende, der efterfølgende vil kunne anvende disse til fx ulovlig adgang til klassificerede områder, depotfaciliteter o. lign.

Som ansat i en koncern, der arbejder med højt klassificerede informationer, våben, ammunition og eksplosivstoffer, har man derfor et særligt ansvar for, at disse forbliver i koncernens varetægt. Dette stiller krav om omhyggelighed og en høj grad af opmærksomhed i tjenesten.

Følgende emner kan indgå i opmærksomhedsuddannelsen:

- Trusler generelt, såvel interne som eksterne
- Fokus på sårbare områder og processer
- Mistænkelige køretøjer
- Mistænkelige pakker og breve
- Mistænkelige personer
- Pludselige ændringer i adfærd blandt kollegaer
- Isolation fra kollegaer/gruppen
- Stigende fravær
- Kontakt til kriminelle eller ekstremistiske miljøer
- Observationer på it-netværk, herunder Internettet (BLOGS, FACEBOOK mv.)
- Svind og tab fra lagre, depoter o. lign.
- Rod på arbejdspladsen
- Kollegaers ligegyldighed i omgang med materiel og informationer
- Områder og situationer, hvor der skal udvises særlig opmærksomhed
- Ansvar i forbindelse med opholdskontrol og dens praktiske gennemførelse
- Rapportering/meldeveje.

ANDRE LANDES OG INTERNATIONALE ORGANISATIONERS KLASSIFIKATIONSGRADER

Danmark		YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
NATO		COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
EU	engelsk	EU TOP SECRET	EU SECRET	EU CONFIDENTIAL	EU RESTRICTED
	fransk	TRÈS SECRET UE	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
FN		INGEN	STRICTLY CONFIDENTIAL	CONFIDENTIAL	INGEN
Albanien		TEPËR SEKRET	SEKRET	KONFIDENCIAL	I KUFIZUAR
Australien		TOP SECRET	SECRET	INGEN ¹	OFFICIAL
Belgien	flamsk	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERKTE VERSPREIDING
	fransk	TRÈS SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTE
Bulgarien		СТОГО СЕКРЕТНО	СЕКРЕТНО	ПОВЕРЛИТНО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
Canada	engelsk	TOP SECRET	SECRET	CONFIDENTIAL	INGEN
	fransk	TRÈS SECRET	SECRET	CONFIDENTIEL	INGEN
Cypern		ΑΚΡΟΣ ΑΠΟΡΗΤΟ	ΑΠΟΡΗΤΟ	ΕΜΠΙΣΤΕΥΤΙΚΟ	ΠΕΡΙΩΡΙΣ ΜΕΝΗΣ ΧΡΗΣΕΩΣ
Estland		TÄIESTI SALAJANE	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland		ERITTÄIN SALAINEN ²	SALAINEN	LUOTTAMUKSELLINEN ³	KÄYTTÖ RAJOITETTU
Frankrig		TRÈS SECRET ⁴	SECRET	INGEN ⁵	DIFFUSION RESTREINTE
Grækenland	græsk	ΑΚΡΟΣ ΑΠΟΡΡΗΤΟ	ΑΠΟΡΡΗΤΟ	ΕΜΠΙΣΤΕΥΤΙΚΟ	ΠΕΡΙΩΡΙΣΜΕΝΗΣ ΧΡΗΣΕΩΣ
	latin	AKROS APORRITO	APORRITO	EMPISTEYTIKO	PERIORISMENIS CHRISIS
Holland		Staatsgeheim ZEER GEHEIM	GEHEIM	Statsgeheim CONFIDENTIEEL	Departementaal VERTROUWELIJK
Irland		TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Italien		SECRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Island		ALGJÖRT LEYNDARMÁL	LEYNDARMÁL	TRÚNAÐARMÁL	TAKMARKAÐUR AÐGANGUR
Kroatien		VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Letland		SEVIŠKI SLEPENI I	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
Litauen		VISIŠKAI SLAPTAI	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
Luxemburg		TRES SECRET LUX	SECRET LUX	CONFIDENTIEL LUX	RESTREINTE LUX
Malta		L-GHOLA SEGRETEZZA	SIGRIET	KUNFIDENZJALI	RISTRETT
Montenegro		STROGO TAJNO	TAJNO	POVJERLJIVO	INTERNO
Norge		STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
Polen		ŚCIŚLE TAJNE	TAJNE	POUFNE	ZASTRZEŻONE
Portugal		MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Rumænien		STRICT SECRET DE IM-PORTANTĂ DEOSEBITĂ	STRICT SECRET	SECRET	SECRET DE SERVICIU
Schweiz		INGEN	GEHEIM	VERTRAULICH	INTERN
Singapore ⁶			SECRET	CONFIDENTIAL	RESTRICTED
Slovakiet		PRÍSNE TAJNÉ	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenien		STRONGO TAJNO	TAJNO	ZAUPNO	INTERNO
Spanien		SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Storbritannien ⁷		UK TOP SECRET	UK SECRET	INGEN ⁸	UK OFFICIAL-SENSITIVE ⁹

¹ Ældre australske dokumenter mærket CONFIDENTIAL skal behandles som HEMMELIGT. Australien bruger udover TOP SECRET og SECRET også mærkningen PROTECTED. Da der ikke findes en ækvivalerende dansk mærkning skal australsk PROTECTED behandles som FORTROLIGT

² I det finske forsvar: SALAINEN – VAIN NIMETTYJEN HENKILÖIDEN TIETOON (HEMMELIGT, kun for navngivne personer).

³ I det finske forsvar: EI TIETOJA SIVULLISILLE – SÄILYTETTÄVÄ LUKITUSSA PAIKASSA (Ikke for uvedkommende skal opbevares under lås).

⁴ TRÈS SECRET klassifikationsgraden er i Frankrig reserveret regeringen og bliver kun anvendt med Premierministerens godkendelse.

⁵ Frankrig anvender ikke denne klassifikation men FORTROLIGT/CONFIDENTIAL mærket materiale vil blive behandlet som SECRET

⁶ Singapore anvender udover de tre klassifikationer i skemaet endvidere OFFICIAL (CLOSED) som IKKE KLASSIFICERET

⁷ Storbritannien har pr. 2. april 2014 ændret sit klassifikationssystem og anvender herefter klassifikationsgraderne UK TOP SECRET, UK SECRET og UK OFFICIAL - SENSITIVE

⁸ Udenlandsk CONFIDENTIAL beskyttes som britisk SECRET. Britisk CONFIDENTIAL (klassificeret før 2. april 2014) skal beskyttes som dansk FORTROLIGT.

⁹ Informationer klassificeret OFFICIAL (uden tilføjelsen SENSITIVE) skal ikke sikkerhedsbeskyttes. Britiske informationer klassificeret RESTRICTED (klassificeret før 2. april 2014) skal beskyttes som dansk TIL TJENESTEBRUG.

Danmark		YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
NATO		COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
EU	engelsk	EU TOP SECRET	EU SECRET	EU CONFIDENTIAL	EU RESTRICTED
	fransk	TRÈS SECRET UE	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
FN		INGEN	STRICTLY CONFIDENTIAL	CONFIDENTIAL	INGEN
Sverige		HEMLIG/TOP SECRET	HEMLIG/SECRET	HEMLIG/CONFIDENTIAL ¹⁰	HEMLIG/RESTRICTED ¹¹
Sydkorea		TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
		(군사 1급 비밀)	(군사 Ⅱ급 비밀)	(군사 Ⅲ급 비밀)	(군사 대외비)
Tjekkiet		PŘÍSNĚ TAJNÉ	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
Tyrkiet		ÇOK GİZLİ	GİZLİ	ÖZEL	HİZMETE ÖZEL
Tyskland		STRENG GEHEIM	GEHEIM	VS-VERTRAULICH ¹²	VS-NUR FÜR DEN DIENST- GEBRAUCH ¹³
Ungarn		SZIGORÚAN TITKOS	TITKOS	BIZALMAS	KORLÁTOZOTT TERJES- ZTÉSÜ
USA		TOP SECRET	SECRET	CONFIDENTIAL	INGEN ¹⁴
Østrig		STRENG GEHEIM	GEHEIM	VERTRAULICH	EINGESCHRÄNKT

¹⁰ I Sverige anvendes klassifikationsgraderne HEMLIIG/CONFIDENTIAL og HEMLIIG/RESTRICTED kun af forsvarsmyndigheder. Dansk FTR og TTJ vil blive behandlet som HEMLIIG/SECRET af andre myndigheder. I forbindelse med projekter, hvor NATO-lande deltager, aftales klassifikationsgrader, svarende til NATO. Informationer fra Sverige, der alene er mærket HEMLIIG skal beskyttes som dansk HEMMELIGT.

¹¹ I Sverige anvendes klassifikationsgraderne HEMLIIG/CONFIDENTIAL og HEMLIIG/RESTRICTED kun af forsvarsmyndigheder. Dansk FTR og TTJ vil blive behandlet som HEMLIIG/SECRET af andre myndigheder. I forbindelse med projekter, hvor NATO-lande deltager, aftales klassifikationsgrader, svarende til NATO. Informationer fra Sverige, der alene er mærket HEMLIIG skal beskyttes som dansk HEMMELIGT.

¹² Tyskland: VS = Verschlusssache.

¹³ Tyskland: VS = Verschlusssache.

¹⁴ USA anvender ikke klassifikationsgraden RESTRICTED i sit nationale system, men håndterer og beskytter NATO RESTRICTED materialer i overensstemmelse med gældende regler i NATO.

PRAKTISK KLASSEKATIONSVJEJLEDNING

Denne vejledning skal opfattes som et supplement til de grundlæggende bestemmelser i kapitel 1.

1. YDERST HEMMELIGT (»COSMIC TOP SECRET«, »TRÈS SECRET UE« / »EU TOP SECRET«)	
Anvendelse	Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark, Nato eller EU eller en eller flere medlemslandes vitale interesser overordentlig alvorlig skade.
Hvornår	Ved lækage af oplysninger, der er klassificeret YDERST HEMMELIGT, er der sandsynlighed for: • at stabiliteten i Danmark, i en eller flere af Nato eller EU medlemslandene eller i venligsindede lande direkte kan bringes i fare. • at forbindelserne med venligsindede regeringer direkte kan skades i overordentlig alvorlig grad. • at et stort antal menneskeliv kan gå tabt. • at Danmarks eller en eller flere af medlemslandene i Nato eller EU eller andre bidragsydere operative effektivitet eller overordentligt vigtige sikkerheds- eller efterretningsoperationers fortsatte effektivitet kan skades i overordentlig alvorlig grad. • at økonomien i Danmark eller en eller flere af medlemslandene i Nato eller EU kan påføres alvorlig langvarig skade.
Påskrifter m.v.	YDERST HEMMELIGT påføres dokumenter med denne klassifikationsgrad. Hvor det er relevant, tilføjes særlig mærkning mekanisk eller i hånden. Klassifikationsgraden anføres midt på hver side foroven og forneden, og hver side nummereres. Hver side i dokumentet skal være forsynet med entydig identifikation udsteder, emne- og løbenummer og dato. Hvis dokumentet skal fordeles i flere eksemplarer, skal hvert eksemplar have et nummer, som anføres på første side sammen med det samlede sideantal. Evt. Bilag anføres på første side. Udstederen bør jævnligt gennemgå de tidligere udfærdigede klassificerede informationer med henblik på at nedklassificere eller afklassificere disse, i det omfang de hensyn, der betingede klassifikationsgraden, ikke længere er til stede.
Ned- og afklassificering samt destruktion	Afklassificering og nedklassificering må kun foretages af udstederen, som meddeler ændringen til de instanser, som efterfølgende har modtaget originaldokumentet eller et eksemplar heraf. Dokumenter, der er klassificeret YDERST HEMMELIGT, skal destrueres af to der til bemyndigede og sikkerhedsgodkendte personer. Begge skal underskrive tilintetgørelsesbeviset, der opbevares i 10 år. Elektronisk udarbejdede tilintetgørelsesbeviser udskrives, underskrives og gemmes som anført oven for. Tilintetgørelse registreres i journalsystemet. Overskydende eksemplarer og dokumenter, der ikke længere er brug for, destrueres. Dokumenter, der er klassificeret YDERST HEMMELIGT, herunder alt klassificeret affald, der stammer fra forberedelsen af dokumenter, der er klassificeret YDERST HEMMELIGT, som fx uanvendelige eksemplarer, arbejdstekster, noter og karbonpapir destrueres under opsyn af en medarbejder, der er sikkerhedsgodkendt og bemyndiget på dette niveau, ved makulering med en findelingsgrad svarende til sikkerhedsniveau 6.
Opbevaring	YDERST HEMMELIGT materiale skal opbevares i godkendt og aflåst opbevaringsmiddel militær klassificering a (sikringsskab, F&P blå klasse, hovedgruppe 2) med sikkerhedsgodkendt kombinationslås. Opbevaringsmidlet skal befinde sig inden for et sikret område, områdekategori 1, sikringsniveau 50. Materiale klassificeret YDERST HEMMELIGT må ikke opbevares på anden måde.

2. HEMMELIGT («NATO SECRET», «SECRET UE» / «EU SECRET»)	
Anvendelse	Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark, NATO, EU, eller en eller flere medlemslandes vitale interesser alvorlig skade.
Hvornår	Ved lækage af oplysninger, der er klassificeret HEMMELIGT, er der sandsynlighed for: • at der kan opstå internationale spændinger. • at forbindelserne med venligsindede regeringer kan lide alvorlig skade. • at det kan true menneskeliv direkte eller i alvorlig grad anfægte den offentlige orden eller den enkeltes sikkerhed eller frihed. • at det kan være til alvorlig skade for Danmarks eller en eller flere lande i NATO eller EU eller andre bidragsyderes styrkers operative effektivitet eller sikkerhed eller for meget værdifulde sikkerheds- eller efterretningsoperationers fortsatte effektivitet. • at det kan forvolde væsentlig skade for Danmark eller en eller flere lande i NATO eller EU finansielle, monetære, økonomiske og handelsmæssige interesser
Påskrifter m.v.	HEMMELIGT påføres dokumenter med denne klassifikationsgrad. Hvor det er relevant, tilføjes særlig mærkning mekanisk eller i hånden. Klassifikationsgraden anføres midt på hver side foroven og forneden, og hver side nummereres. Hver side i dokumentet skal være forsynet med entydig identifikation udsteder, emne- og løbenummer og dato. Hvis dokumentet skal fordeles i flere eksemplarer, skal hvert eksemplar have et nummer, som anføres på første side sammen med det samlede sideantal. Evt. bilag anføres på første side. Udstederen bør jævnligt gennemgå de tidligere udfærdigede klassificerede informationer med henblik på at nedklassificere eller afklassificere disse, i det omfang de hensyn, der betingede klassifikationsgraden, ikke længere er til stede.
Ned- og afklassificering samt destruktion	Afklassificering og nedklassificering må kun foretages af udstederen, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf. Dokumenter, der er klassificeret HEMMELIGT, skal destrueres af to der til bemyndigede og sikkerhedsgodkendte personer, begge skal underskrive tilintetgørelsesbeviset, der opbevares i 10 år. Elektronisk udarbejdede tilintetgørelsesbeviser udskrives, underskrives og gemmes som anført oven for. Tilintetgørelse registreres i journalsystemet. Overskydende eksemplarer og dokumenter, der ikke længere er brug for, destrueres. Dokumenter, der er klassificeret HEMMELIGT, herunder alt klassificeret affald fra udarbejdelsen af sådanne dokumenter, såsom uanvendelige eksemplarer, arbejdsudkast, maskinskrevne notater og karbonpapir, destrueres ved makulering med en findelingsgrad svarende til sikkerhedsniveau 5.
Opbevaring	HEMMELIGT materiale skal opbevares i godkendt og aflåst opbevaringsmiddel militær klassificering A (EN1143-1, GR 1 skab) med sikkerhedsgodkendt kombinationslås. Opbevaringsmidlet skal befinde sig inden for et sikret område, minimum områdekategori 2, sikringsniveau 30. Hvis opbevaringsmidlet er placeret i et sikret område, kategori 1 område, sikringsniveau 30, kan det erstattes af et skab med militær klassifikation B. Ved større mængder HEM klassificeret materiale, fx ved et hovedarkiv, anvendes sikringsniveau 40, og rummet indrettes som et egentligt arkivrum. Opbevares materiale klassificeret HEMMELIGT undtagelsesvis i overvåget område, områdekategori 4, skal den anslåede samlede mekaniske sikrings holdetid i minutter, som minimum være det dobbelte af reaktionstiden for indsatsstyrken. I sådanne tilfælde skal rådgivning indhentes ved FE.

3. FORTROLIGT (»NATO CONFIDENTIAL«, »CONFIDENTIEL UE« / »EU CONFIDENTIAL«)	
Anvendelse	Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark, NATO, EU, eller en eller flere medlemslandes vitale interesser skade.
Hvornår	Ved lækage af oplysninger, der er klassificeret FORTROLIGT, er der sandsynlighed for: • at de diplomatiske forbindelser kan lide skade, dvs. at det vil kunne medføre formelle protester eller andre sanktioner. • at det kan anfægte den enkeltes sikkerhed eller frihed. • at det kan være til skade for Danmarks eller en eller flere af NATO eller EU medlemslandes eller andre bidragsyderes styrkers operative effektivitet eller sikkerhed eller for værdifulde sikkerheds- eller efterretningsoperationers effektivitet. • at det kan undergrave større organisationers finansielle levedygtighed i væsentlig grad. • at det kan vanskeliggøre efterforskningen af eller gøre det lettere at begå alvorlig kriminalitet. • at det i væsentlig grad kan modvirke Danmarks eller en eller flere af NATO eller EU medlemslandes finansielle, monetære, økonomiske og handelsmæssige interesser.
Påskrifter m.v.	FORTROLIGT påføres dokumenter med denne klassifikationsgrad. Hvor det er relevant, tilføjes særlig mærkning mekanisk eller i hånden eller ved fortryk på registreret papir. Klassifikationen anføres midt på hver side foroven og forneden, og hver side nummereres. Hvert dokument skal være forsynet med referencenummer og dato. Evt. bilag anføres på første side. Udstederen bør jævnligt gennemgå de tidligere udfærdigede klassificerede informationer med henblik på at nedklassificere eller afklassificere disse, i det omfang de hensyn, der betingede klassifikationsgraden, ikke længere er til stede.
Ned- og afklassificering samt destruktion	Afklassificering og nedklassificering må kun foretages af udstederen, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf. Dokumenter, der er klassificeret FORTROLIGT, skal destrueres af personer, der er bemyndiget og sikkerhedsgodkendt dertil. Tilintetgørelse registreres i journalsystemet. Overskydende eksemplarer og dokumenter, der ikke længere er behov for, destrueres. Dokumenter, der er klassificeret FORTROLIGT, herunder alt klassificeret affald fra udarbejdelsen af sådanne dokumenter, såsom uanvendelige eksemplarer, arbejdsudkast, maskinskrevne notater og karbonpapir, destrueres ved makulering med en findelingsgrad svarende til sikkerhedsniveau 4.
Opbevaring	FORTROLIGT materiale skal opbevares i godkendt og aflåst opbevaringsmiddel som minimum militær klassificering B (sikringsskab, F&P GUL klasse, hovedgruppe 2). Opbevaringsmidlet skal befinde sig inden for et sikret område, minimum områdekategori 2, sikringsniveau 30. Ved større mængder FTR klassificeret materiale, fx ved et hovedarkiv anvendes sikringsniveau 40. Opbevares materiale klassificeret FORTROLIGT undtagelsesvis i overvåget område, områdekategori 4, skal den anslåede gennembrydnings- og/eller oplukningstid som minimum svare til den anslåede reaktionstid.

4. TIL TJENESTEBRUG (»NATO RESTRICTED«, »RESTREINT UE« / »EU RESTRICTED«)	
Anvendelse	Denne klassifikationsgrad anvendes til informationer, der ikke må offentliggøres eller komme til uvedkommendes kendskab.
Hvornår	Ved lækage af oplysninger, der er klassificeret TIL TJENESTEBRUG, er der sandsynlighed for: • at det kan påvirke de diplomatiske forbindelser negativt. • at det kan volde enkeltpersoner alvorlig problemer. • at det kan gøre det vanskeligere at opretholde medlemsstaternes eller andre bidragsydere styrkers operative effektivitet eller sikkerhed. • at det kan medføre økonomiske tab for enkeltpersoner eller virksomheder eller gøre det lettere for dem at opnå urimelig vinding eller fordel. • at det kan være et brud på garanteret tavshedspligt med hensyn til oplysninger fra tredjepart. • at det kan være en overtrædelse af lovgivningen om videregivelse af oplysninger. • at det kan vanskeliggøre efterforskningen af eller gøre det lettere at begå kriminalitet. • at det kan stille Danmark eller en eller flere af NATO eller EU medlemslande ringere i handelsmæssige eller politiske forhandlinger med andre parter
Påskrifter m.v.	TIL TJENESTEBRUG påføres dokumenter med denne klassifikationsgrad, og, hvor det er relevant, tilføjes særlig mærkning, der påføres mekanisk eller elektronisk. Klassifikationsgraden anføres midt på hver side foroven og forneden, og hver side nummereres. Hvert dokument skal være forsynet med referencenummer og dato. Udstederen skal så vidt muligt anføre en varighedsmærkning for klassifikationen, efter hvilken materialet kan afklassificeres. Udstederen bør jævnligt gennemgå de tidligere udfærdigede klassificerede informationer med henblik på at nedklassificere eller afklassificere disse, i det omfang de hensyn, der betingede klassifikationsgraden, ikke længere er til stede.
Ned- og afklassificering samt destruktion	Afklassificering og nedklassificering må kun foretages af udstederen, som meddeler ændringen til alle senere modtagere, som har fået tilsendt dokumentet eller et eksemplar heraf. Dokumenter, der er klassificeret TIL TJENESTEBRUG, kan tilintetgøres af personer, der som minimum er sikkerhedsgodkendt til TTJ. Overskydende eksemplarer og dokumenter, der ikke længere er brug for, destrueres ved makulering med en findelingsgrad svarende til sikkerhedsniveau 1. Nedklassificering af TTJ materiale medfører afklassificering.
Opbevaring	TIL TJENESTEBRUG materiale skal opbevares i aflåst gemme.

**MÆRKNING AF DOKUMENTER OG ANDRE INFORMATIONSBÆRENDE MEDIER
(EKSEMPLER)**

Dokumenter

Sikkerhedsklassifikation

TIL TJENESTEBRUG

FORTROLIGT

HEMMELIGT

Til: Værnsfælles Forsvarskommando

Kopi til: Forsvarsministeriets Materiel- og Indkøbstyrelse

Kastellet 30
2100 København Ø
Tlf.: 33 32 55 66
fe@fe-mail.dk
www.fe-dda.dk

Xnr. 1 af 6
Sidetal: 4

13. oktober 2015
Dokumentnr.: 123456

HEMMELIGT 1/4

Diskretion

FORTROLIGT P

FORTROLIGT K

TIL TJENESTEBRUG
FORTROLIGT K

Til: Værnsfælles Forsvarskommando

Kopi til: Forsvarsministeriets Materiel- og Indkøbstyrelse

Kastellet 30
2100 København Ø
Tlf.: 33 32 55 66
fe@fe-mail.dk
www.fe-dda.dk

13. oktober 2015
Dokumentnr.: 123456

FORTROLIGT K
TIL TJENESTEBRUG 1/4

Varighed

TIL TJENESTEBRUG
Afklassificeret 2015-12-31

FORSVARETS
EFTERRETNINGSTJENESTE

Til: Værnsfælles Forsvarskommando

Kopi til: Forsvarsministeriets Materiel- og Indkøbstyrelse

Kastellet 30
2100 København Ø
Tlf.: 33 32 55 66
fe@fe-mail.dk
www.fe-dda.dk

13. oktober 2015
Dokumentnr.: 123456

Afklassificeret 2015-12-31
TIL TJENESTEBRUG 1/4

Udbredelse

TIL TJENESTEBRUG
Afklassificeret 2015-12-31
KUN TIL INTERN BRUG I FE

HEMMELIGT
KUN TIL BRUG I PROJEKT KAMPFLY

Til: Værnsfælles Forsvarskommando

Kopi til: Forsvarsministeriets Materiel- og Indkøbstyrelse

Kastellet 30
2100 København Ø
Tlf.: 33 32 55 66
fe@fe-mail.dk
www.fe-dda.dk

13. oktober 2015
Dokumentnr.: 123456

KUN TIL BRUG I PROJEKT KAMPFLY
HEMMELIGT 1/4

Præsentation (PPT o.l.)



Digitale medier CD og DVD



USB og hukommelseskort



KONTORSIKKERHED

1. GENERELT

Personellet er ansvarlige for, at uvedkommende ikke får indsigt i eller adgang til klassificeret materiale. Hvor flere personer deler et kontor, skal der udpeges en person, der er ansvarlig for sikkerheden, herunder specielt for at alle sikkerhedsforanstaltninger er udført ved tjenestetids ophør.

Når kontoret forlades midlertidigt, skal personellet sikre sig, at uvedkommende ikke kan få adgang til klassificeret materiale.

Kontorer beliggende i en bygnings stueetage skal udstyres med gardiner, således at det udefra ikke er muligt at få indsigt i klassificeret materiale, der behandles på kontoret.

Ved tjenestetids ophør skal den sikkerhedsansvarlige kontrollere, at:

- Alle vinduer er lukket og haspet
- Eventuelle gitre er på plads og låst
- Klassificerede sager er placeret i korrekte opbevaringsmidler iht. klassifikationsgrad og sikringsniveau
- Harddiske, disketter og nøgler er udtaget af personlige computer mv. og korrekt opbevaret iht. klassifikationsgrad og sikringsniveau
- Alle opbevaringsmidler er aflåst
- Papirkurve er tømt
- Døre – hvor dette er bestemt – er aflåst
- Nøgler er placeret i korrekte opbevaringsmidler
- Eventuelle elektroniske overvågningsanlæg er tilkoblet.

I sikrede områder, kategori 1, bør efterkontrol finde sted ved foranstaltning af dertil bemyndiget personel eller vagtpersonel.

2. OPBEVARINGSMIDLER

Når klassificeret materiale ikke er under opsyn, kontrol eller beskyttelse, skal det opbevares i godkendte opbevaringsmidler.

FORHOLD VED AFHOLDELSE AF MØDER MV.

Myndigheder mfl. skal efter behov og forud for afholdelse af møder, drøftelser og instruktioner, der omfatter klassificerede informationer, gennemføre følgende foranstaltninger i eller i forbindelse med den aktuelle lokalitet (lokale mv.):

- Forhindre uvedkommendes mulighed for indsigt og fotografering gennem vinduer og andre åbninger (afblænding mv.).
- Forhindre direkte aflytning gennem vinduer, døre, vægge, ventilationskanaler, radiatorer osv. (aflåsning, afspærring og bevogtning).

- Fjerne eller afbryde installerede telefoner, højttaleranlæg og andre elektriske/elektroniske installationer, som ikke skal anvendes under arrangementet.
- Efterse alt inventar for aflytningsudstyr, herunder elektrisk/elektronisk udstyr, der skal anvendes under arrangementet, og tilgængelige åbninger mv. i bygningskonstruktionen.

Under afholdelse af et arrangement, der omfatter behandling af klassificerede informationer, skal opmærksomheden henledes på udstyr, som deltagerne medfører (mobiltelefoner og båndoptagere mv.). Opmærksomheden skal desuden henledes på deltagernes notater om behandlede klassificerede emner.

2.1 Eksempelvis "lukkeliste".

Da rutiner i forbindelse med daglig tjenestetids ophør kan forebygge uvedkommende indsigt, bortkomst og tyveri anbefales, at der udarbejdes tjek/lukkeliste som viser et minimum af tiltag som skal foretages når arbejdspladsen forlades. Lukke proceduren/checklisten skal være kendt og tilgængelig for den enkelte medarbejder.

Listen kan eksempelvis indeholde nedennævnte punkter, evt. suppleret med punkter som er specielt gældende/dækkende ved den enkelte myndighed.

- ☐ Kontroller, at klassificerede harddiske, er taget ud af PC og låst inde i korrekt opbevaringsmiddel
- ☐ Kontroller, at klassificerede bærbare PC er låst inde i korrekt opbevaringsmiddel
- ☐ Kontroller, at klassificeret materiel/materiale er låst inde i korrekt opbevaringsmiddel
- ☐ Kontroller, at vinduer er lukket og tilhaspet
- ☐ Kontroller, at evt. gitre er på plads og fastlåst
- ☐ Kontroller, at opbevaringsmidler er lukket og låst
- ☐ Kontroller, at sikkerhedsbetydende nøgler er til stede i nøgleopbevaringsmiddel og at dette låses/er låst
- ☐ Kontroller, at evt. rumovervågning ikke er tildækket
- ☐ Kontroller, at den elektroniske overvågning når denne tilkobles reagerer korrekt
- ☐ Kontroller aflåsning af yderdør når faciliteten forlades.

TILINTETGØRELSE AF INFORMATIONSBÆRENDE MATERIALE

Makulatorer afmærkes således, at det tydeligt fremgår hvilken klassifikation de maksimalt må tilintetgøre.

1. MAKULERING

Klassificeret materiale skal destrueres, således at makulaturen kan betegnes som værende afklassificeret. Dette medfører efternævnte minimumskrav til tilintetgørelse.

1.1 Materiale

1.1.1 Materiale (papir), der er klassificeret FTR og højere, tilintetgøres på en sådan måde, at materialet efter tilintetgørelsen ikke kan rekonstrueres, og dette indebærer, at materialet skal sønderskæres i makulator med krydsskær.

1.1.2 Materiale (papir) der er klassificeret TTJ og lavere, tilintetgøres på en sådan måde, at materialets indhold ikke umiddelbart kan komme til uvedkommendes kendskab, dvs., at materialet sønderskæres i makulator med strimmelskær.

1.1.3 Elektroniske lagermedier og andre typer lagermedier tilintetgøres ved makulering, så materialet efter tilintetgørelsen fremstår som enkle deforme partikler, som ikke kan rekonstrueres.

1.2 Findelingsgrad

Findelingsgraden af makulaturen udtrykkes ved sikkerhedsniveau 1-7 (DIN norm 66399), hvor sikkerhedsniveau 7 er største findelingsgrad.

Makulering af klassificeret informationsbærende materiale skal gennemføres jf. Nedenstående matriks (minimumskrav):

Klassifikation Medie	YHM, ATOMAL, krytomateriale og sensitivt materiale	HEM og FTR	TTJ
Papir	Minimum P6 (max. 10 mm ²)	Minimum P5 (max. 30 mm ²)	Minimum P1 (max. 2000 mm ²)
Optiske lagringsmedier CD, DVD	Minimum O6 (max. 5 mm ²)	Minimum O5 (max. 10 mm ²)	Minimum O3 (max. 160 mm ²)
Magnetiske lagringsmedier Disketter Videobånd Audiokassetter Farvebåndskassetter	Minimum T6 (max. 10 mm ²)	Minimum T5 (max. 30 mm ²)	Minimum T2 (max. 2000 mm ²)
Elektroniske lagringsmedier USB nøgler Chip kort Eksterne lagringsmedier	Minimum E6 (max. 1 mm ²)	Minimum E5 (max. 10 v)	Minimum E3 (max. 160 mm ²)
Hard diske (magnetiske)	Minimum H6 (max. 10 mm ²)	Minimum H5 (max. 320 mm ²)	Minimum H4 (max. 2000 mm ²)
Mikrofilm etc.	Minimum F6 (max. 0,5 mm ²)	Minimum F5 (max. 1 mm ²)	Minimum F3 (max 10 mm ²)

KAPITEL 2

PERSONELSIKKERHED

1. INDLEDNING

Personelsikkerhed omfatter foranstaltninger, som sikrer koncernens virksomhed gennem relevant sikkerhedsgodkendelse af personel, der skal have adgang til klassificeret materiale.

Endvidere omfatter personelsikkerhed foranstaltninger til beskyttelse af koncernens personel og personel med tilknytning til Forsvaret mod spionage, undergravende virksomhed, kompromittering, kriminel aktivitet samt terrorisme.

2. FORMÅL

Formålet med dette kapitel er at beskrive de minimumskrav og procedurer, der er gældende i forbindelse med sikkerhedsgodkendelse af personel, der skal udføre klassificeret arbejde for koncernen. Kapitlet beskriver desuden de personelrelaterede beskyttelsesforanstaltninger og sikkerhedsforskrifter, der skal iagttages under tjenesten.

3. ANSVAR

Chefen (direktøren, lederen, mfl.) er ansvarlig for udøvelse af personelsikkerheden ved institutioner og myndigheder. Chefen er ansvarlig for vurdering af den enkelte medarbejders sikkerhedsmæssige kvalifikationer, så som pålidelighed, sårbarhed, diskretion, loyalitet, adfærd og sikkerhedsforståelse i relation til tjenesten og ansættelsesforholdets art.

Chefen skal herunder sikre sig,

- at der foreligger nødvendig sikkerhedsgodkendelse forud for den faste ansættelse
- at bemyndigelse til indsigt i HEM og højere klassificeret materiale meddeles
- at need to know princippet præciseres, således at adgang til indsigt i klassificeret materiale alene er begrundet i et tjenstligt behov
- at sikkerhedsinstruktion, -uddannelse og -kontrol gennemføres jf. kapitel 1, bilag 3.

4. SIKKERHEDSGODKENDELSE AF PERSONEL

Alt personel, der fastansættes i forsvaret, skal sikkerhedsgodkendes. Alt personel, der beskæftiger sig med klassificerede informationer, skal være sikkerhedsgodkendt i overensstemmelse med kravet til den stilling, som personellet bestrider.

Værnepligtigt menigt personel og frivilligt personel i hjemmeværnet, for hvem der ikke kræves en egentlig sikkerhedsgodkendelse må beskæftiges med materiale, der er klassificeret TTJ, og meddeles viden med samme klassifikationsgrad. Hvis der er behov for, at sådant personel skal beskæftiges med materiale, der er klassificeret højere end TTJ, skal der foretages en sikkerhedsundersøgelse, og sikkerhedsgodkendelsen skal bekræftes skriftligt.

Værnepligtige ved Livgarden, Gardehusarregimentets Hesteskadron og Kongeskibet Dannebrog skal sikkerhedsgodkendes til FTR.

For personer, der ved Forsvarets Dag udtrykker interesse for senere ansættelse på kontrakt, vil Oplysningsskema 1 kunne udfyldes og indsendes til FE.

Udvælgelse af personel, der meddeles kryptoautorisation, finder sted i henhold til bestemmelserne i bilag 3 til afsnit II til kapitel 6. Det er væsentligt, at personellet har den fornødne uddannelse og erfaring. Krav til sikkerhedsgodkendelse fremgår af anførte kapitel.

Ingen må beskæftige sig med informationer og materiel, der er klassificeret højere end TTJ, før sikkerhedsgodkendelse foreligger. Chefen kan dog inden for eget myndighedsområde midlertidigt dispensere herfra og meddele indsigt i én klassifikationsgrad højere (FTR), når omstændighederne taler for det.

I tilfælde, hvor der for en medarbejder, godkendt til HEM/NS/SECRET, UE SECRET, opstår et pludseligt kortvarigt behov for indsigt i informationer klassificeret YHM/CTS/ TRÉS SECRET UE/FOCAL TOP SECRET, kan chefen inden for eget myndighedsområde bemyndige den pågældende medarbejder denne indsigt. Bemyndigelsen skal være skriftlig, opgave- og tidsbestemt, og inddrages, når der intet behov er mere. Bemyndigelsen arkiveres i 10 år.

Såfremt der efter meddelt sikkerhedsgodkendelse opstår tvivl om en persons sikkerhedsmæssige kvalifikationer kan chefen - ligeledes inden for eget myndighedsområde - inddrage den meddelte bemyndigelse til beskæftigelse med klassificerede informationer. Forholdene indberettes til FE.

Nærmere retningslinjer for indstilling om sikkerhedsgodkendelse af personel samt regler, der skal iagttages, når godkendelse foreligger, fremgår af bilag 1.

5. SIKKERHEDSUDDANNELSE

Alt personel, der ansættes i koncernen, skal gennemgå sikkerhedsuddannelse som beskrevet i kapitel 1 bilag 3. Det skal understreges, at personel, der efter meddelt sikkerhedsgodkendelse er bemyndiget til beskæftigelse med FTR og HEM klassificeret materiale, skal instrueres om de gældende bestemmelser for den omhandlede klassifikationsgrad.

5.1 Tavshedspligt

Enhver har tavshedspligt med hensyn til de forhold, som vedkommende under sin tjeneste bliver bekendt med, og hvis hemmeligholdelse ifølge sagens natur er påkrævet eller foreskrevet. Dette følger af den almindelige lovgivning og er for forsvarets militære og civile personel fastsat som en tjenestebestemmelse ved Forsvarsministeriets cirkulære nr. 2.kt. 04-701-15 af 20 JAN 2006 (KFF B.3-4). Overtrædelser af tavshedspligten straffes bl.a. efter straffeloven og militær straffelov.

Tavshedspligten omfatter:

- Alle informationer, der er klassificerede YHM, HEM, FTR eller TTJ (samt tilsvarende udenlandske klassifikationer), eller er påført særlige need to know mærkninger som f.eks. POF eller FTR-K
- Enhver oplysning, der ifølge lov eller anden gyldig bestemmelse er betegnet som fortrolig, og
- Enhver anden oplysning, som det er nødvendigt at hemmeligholde af hensyn til varetagelsen af væsentlige hensyn til offentlige og private interesser.

Er man i tvivl om, hvorvidt en påtænkt videregivelse af informationer vil være i strid med tavshedspligten, skal man spørge sin nærmeste overordnede chef. Denne skal ved sit svar være opmærksom på, at forsvarets medarbejdere har den samme ytringsfrihed som andre offentligt ansatte. Er man ikke tilfreds med chefens svar, kan man klage til næsthøjere chef, som det er fastsat i KFF B.3-4, §5.

Tavshedspligten ophører ikke, når man forlader tjenesten, hvorfor den i sådanne tilfælde skal indskræpes.

Alt personel, der skal sikkerhedsgodkendes til HEM eller højere, skal have tavshedspligten indskræpet og underskrive den særlige erklæring der er en del af Oplysnings-skema 2 og 3. Hvis der vurderes at være særligt behov herfor, kan chefer for niveau III myndigheder og højere beslutte, at erklæringen også skal benyttes i forhold til personel med sikkerhedsgodkendelse til en lavere klassifikationsgrad.

6. SÆRLIGE FORHOLD

6.1 Tjenesterejser til udlandet

I forbindelse med tjenesterejser og udsendelser af enheder til lande, hvor der vurderes at være en sikkerhedsmæssig risiko, skal personellet gives en grundig sikkerhedsinstruktion af sikkerhedsofficeren.

Vejledninger vedrørende almindelig rejsesikkerhed kan hentes på Udenrigsministeriets hjemmeside (<http://www.um.dk>), der indeholder råd og oplysninger om en række lande og områder.

Ved udsendelse af enheder til deltagelse i internationale operationer, øvelsesaktiviteter, herunder udvekslingsbesøg og flådebesøg, kræves der normalt ikke sikkerhedscertifikat for hver enkelt deltager. Den udsendende myndighed skal afklare forholdet i hvert enkelt tilfælde.

For information om Forsvarets procedurer for ansøgning om adgang til at foretage tjenesterejser til udlandet og om bæring af dansk uniform i udlandet henvises til [FKOBST 810-1](#), Tjenesterejser til udlandet for enkeltpersoner og mindre grupper.

6.2 Ikke-tjenstlige rejser til udlandet

Der er generelt ingen restriktioner i mulighederne for at foretage ikke-tjenstlige rejser til udlandet. Chefen kan dog fastsætte begrænsninger for personel, der besidder sensitive informationer.

Personel, der agter at foretage en ikke-tjenstlig rejse til lande, hvor der vurderes at være en sikkerhedsmæssig risiko, kan anmode tjenestestedets sikkerhedsofficer om en sikkerhedsinstruktion.

Efter hjemkomst skal den rejsende, såfremt vedkommende har været udsat for særlige hændelser af sikkerhedsmæssig karakter, meddele dette til chefen eller sikkerhedsofficeren på tjenestestedet, der skriftligt underretter FE.

Vejledninger vedrørende almindelig rejsesikkerhed kan hentes på Udenrigsministeriets hjemmeside (<http://www.um.dk>), der indeholder råd og oplysninger om en række lande og områder.

6.3 Adgangsforhold for nationale delegerede ved møder, konferencer, kurser mv. i hovedkvarterer/-institutioner

Personel, der deltager i møder ved NATO hovedkvarterer, skal som minimum være sikkerhedsgodkendt til HEM/NS.

Personel, der ikke har en sikkerhedsgodkendelse, kan deltage i møder, hvor dagsordenen ikke er klassificeret, såfremt der foreligger en godkendelse fra mødets leder/sekretær.

I alle tilfælde gælder, at dansk delegation/-element/-support unit, senest 10 dage inden mødets afholdelse, skal have modtaget oplysninger på mødedeltagerne ved et Certificate of Security Clearance.

Tilsvarende regler gælder for besøg ved EU-møder. I tvivlstilfælde skal man have afklaret spørgsmålene inden tilmelding til mødet, kurset, konferencen mv.

6.4 Bopæl i udlandet

For personel i forsvaret, der forretter tjeneste i Danmark, og som er bosat eller ønsker at bosætte sig i udlandet, gælder i visse tilfælde særlige regler, der fremgår af underbilag 6 til bilag 1.

6.5 Mistænkelig adfærd

Personel i forsvaret og personel med tilknytning til forsvaret kan udgøre potentielle mål for fremmed efterretningsvirksomhed.

Det påhviler derfor alt personel at rapportere til egen institution, myndighed eller arbejdsplads om enhver kontakt med personer, hvis adfærd kan give anledning til mistanke om, at der foreligger en sikkerhedsmæssig risiko.

Såfremt sikkerhedsgodkendt personel vurderes at udgøre en sikkerhedsrisiko, kan chefen (direktøren, lederen mfl.) inddrage den pågældendes adgang til klassificeret materiale midlertidigt. Forholdene indberettes til FE.

6.6 Forbindelse med udlændinge

For så vidt angår institutioners, myndigheders og enkeltpersoners forbindelser med udlændinge henvises til KFF B.0-2.

FE skal underrettes om aktiviteter med udenlandsk deltagelse, såfremt disse ikke fremgår af FKO årsprogrammer, øvelsesoversigter eller befalinger. Underretning er ikke nødvendig, hvor den udenlandske deltagelse kun omfatter personer fra NATO- og EU-lande.

6.6.1 Tjenstlige aktiviteter

6.6.1.1 NATO og EU-lande

Tjenstlige aktiviteter med dansk og udenlandsk deltagelse omfattende øvelsesvirksomhed, udvekslingsprogrammer og idrætsarrangementer mv. fremgår af FKO årsprogrammer, øvelsesoversigter og befalinger.

6.6.1.2 Øvrige lande

Tjenstlige aktiviteter med dansk og udenlandsk deltagelse i fælles arrangementer herunder OSCE-aktiviteter (inspektioner, besøg, mv.), FN-aktiviteter, PfP-øvelsesaktiviteter, sportsarrangementer, konferencer og samarbejdsaftaler mv. skal godkendes af Forsvarsministeriet i hvert enkelt tilfælde.

6.6.2 Anden forbindelse mellem forsvarets personel og udlændinge

Ved modtagelse af indbydelse til reception o.l. fra enkeltpersoner, organisationer eller repræsentationer fra lande, der vurderes at udgøre en sikkerhedsmæssig risiko, skal FE straks underrettes.

6.7 Dødsfald

Når en person, der har haft adgang til klassificeret materiale, afgår ved døden, skal sikkerhedsofficeren i overværelse af et vidne snarest mønstre det klassificerede materiale, som afdøde var ansvarlig for ved myndigheden. Med de efterladtes tilladelse og eventuelle bistand skal sikkerhedsofficeren tilsvarende sikre sig, at der ikke findes klassificeret information samt våben og ammunition i den afdødes hjem. Såfremt dette indebærer besøg i hjemmet, skal besøget gennemføres i overværelse af et militært vidne.

7. BESKYTTELSE AF PERSONEL

Når man bevæger sig i det offentlige rum (fysisk og digitalt), skal man aftage sit ID-kort eller adgangskort. Det gælder også, når man er i et missionsområde (ophold uden for en lejr/perimeter), på tjenesterejse eller under fotografering ved egen eller ekstern presse.

ID-kortet eller adgangskortet er personligt og indeholder personoplysninger, der kan kompromitteres, ligesom der er øget risiko for tab, forfalskning eller elektronisk kopiering ved brug i det offentlige rum.

Personel i forsvaret og personel med tilknytning til forsvaret må – især i krisesituationer samt under FORHØJET BEREDSKAB og KRIGSTILSTAND – anses for potentielle mål for terroraktivitet. Der henvises i den forbindelse til [FKOBST O.120-1](#).

8. STØTTEVÆRKTØJ

Til brug for internationale operationer er der udarbejdet et støtteværktøj (kapitel 5 bilag 2 pkt. 5), der kan hjælpe sikkerhedsofficeren ved dennes vurdering af behovet for sikkerhedsgodkendelser. Værktøjets del 2 fokuserer på personelkategorier og funktioner, der i en mission kan kræve højere godkendelser. Endvidere behandler værktøjet generelle -, specifikke og vedligeholdende sikkerhedsuddannelser.

SIKKERHEDSGODKENDELSE AF PERSONEL

Underbilag:

1. Oversigt over anvendelse af oplysningsskemaer mv.
2. Sikkerhedscertifikat.
3. Certificate of Security Clearance (COSC).
4. NATO Personnel Security Clearance Certificate (NSCC).
5. EU Security Certificate.
6. Forhold vedrørende sikkerhedsgodkendelse for personel ved bosættelse i udlandet.

1. FORMÅL

At fastsætte procedurer for indstilling om sikkerhedsgodkendelse af personel samt fastsætte regler, der skal iagttages, når godkendelse foreligger.

2. OMFANG

De anførte forhold gælder for personel, der er ansat eller søger ansættelse inden for Forsvarsministeriets koncernområde og i virksomheder, der udfører arbejde for dansk forsvar, NATO eller EU samt for personel, der udfører arbejde i direkte tilknytning til koncernens myndigheder og institutioner, hvor arbejdet forudsætter en sikkerhedsgodkendelse.

3. GENERELT

De nationale klassifikationsgrader YHM, HEM, FTR og TTJ ækvivalerer de tilsvarende NATO-klassifikationsgrader CTS, NS, NC og NR, samt de tilsvarende EU klassifikationsgrader.

4. INDSTILLELSE MYNDIGHED

Indstilling af personel til sikkerhedsgodkendelse kan foretages af følgende:

4.1. Forsvarsministeriet og underliggende styrelser og myndigheder.

Forsvarsministeriets departement (FMN),
Forsvarskommandoen (FKO),
Hjemmeværnskommandoen (HJK),
Beredskabsstyrelsen (BRS),
Forsvarets Efterretningstjeneste (FE),
Forsvarsakademiet (FAK),
Forsvarsministeriets Materiel- og Indkøbsstyrelse (FMI),
Forsvarsministeriets Personalestyrelse (FPS),
Forsvarsministeriets Ejendomsstyrelse (FES),
Forsvarsministeriets Auditørkorps (FAUK).

4.2. Fornyelser af eksisterende sikkerhedsgodkendelser.

FPS udsender påmindelse om fornyelse til den enkelte medarbejder, og myndigheden fremsender selv oplysningsskemaet.

4.3. Ældste danske Officer.

Ældste danske Officer ved NATO eller EU-stabe og -myndigheder samt forsvarsattachéer fremsender via FPS.

4.4. Virksomheder.

Sikkerhedsgodkendte civile virksomheder, sender direkte til FE.

Personer ved øvrige civile virksomheder indstilles af den brugende myndighed, som sender direkte til FE.

5. KRAV OM SIKKERHEDSGODKENDELSE

Den indstillende myndighed eller virksomhed fastsætter hvilken sikkerhedsgodkendelse personellet skal have, i overensstemmelse med den tjeneste eller det arbejde, der skal udføres. Myndighederne skal tage stilling til, hvorvidt især den militære medarbejder skal indstilles til national godkendelse eller NATO-godkendelse. Når oplysningsskemaet fremsendes, skal det klart fremgå, hvorvidt indstillingen gælder en national eller NATO-godkendelse. NATO-godkendelsen indeholder også en national godkendelse, mens det modsatte ikke er tilfældet. Godkendelsen skal som hovedregel være meddelt inden medarbejderen tiltræder stillingen, og tavshedspligten skal altid indskræpes.

5.1 For følgende kategorier af personel gælder de anførte minimumskrav til sikkerhedsgodkendelse:

Personelkategori	Godkendelsesgrad, minimum	Bemærkninger
Officersgruppen - Fastansatte - Reserven	HEMMELIGT FORTROLIGT	
Befalingsmænd - Fastansatte - Reserven	FORTROLIGT FORTROLIGT	
Menige - Fastansatte - Reserven	FORTROLIGT FORTROLIGT	
Værnepligtige	FORTROLIGT	Kun for tjeneste ved Livgarden, Gardehusarregimentets Hesteskadron og Kongeskibet Dannebrog
Auditørpersonel	HEMMELIGT	
Gejstligt personel	FORTROLIGT	
Militære musikere	FORTROLIGT	
Operativt personel ved Jægerkorpset og Frømandskorpset	COSMIC TOP SECRET	Gælder kun fastansat personel Rådighedspersonel kan som udgangspunkt meddeles begrænset adgang til COSMIC TOP SECRET i henhold til reglerne herfor (se kapitel 2 punkt 4)
Personel med adgang til opbevaringssteder for våben, ammunition og eksplosivstoffer m.v.	HEMMELIGT	
Personel på civiluddannelse	FORTROLIGT	Dog kan hidtidig godkendelse til HEMMELIGT fortsætte, såfremt vedkommende i de undervisningsfrie perioder under CU påtænkes at skulle forrette tjeneste i en stilling, hvortil godkendelse til HEMMELIGT er påkrævet

5.2. IT nøglepersonel

IT nøglepersonel omfatter personel, som vedligeholder og driftsbetjener informationssystemer og netværk, og har administrative rettigheder.

Personellet godkendes som følger:

YDERST HEMMELIGT/COSMIC TOP SECRET.

IT nøglepersonel på systemer, der er godkendt til behandling af informationer klassificeret HEMMELIGT/NATO SECRET eller højere.

HEMMELIGT.

IT nøglepersonel på systemer, der er godkendt til behandling af informationer klassificeret TIL TJENESTEBRUG/NATO RESTRICTED eller FORTROLIGT/NATO CONFIDENTIAL.

FORTROLIGT.

IT nøglepersonel på Internet eller systemer, der ikke er godkendt til behandling af klassificerede informationer.

Godkendelse af IT nøglepersonel må ikke være den eneste sikringsforanstaltning, som sikrer mod misbrug af privilegerede rettigheder. I det omfang det kan lade sig gøre, skal IT nøglepersonels adfærd logges og loggen skal gennemgås af myndigheden med jævne mellemrum. Se endvidere kapitel 6 afsnit 2 punkt A.9.2.3.

6. INDSTILLINGSPROCEDURE

6.1 Ved indstilling til eller ved fornyelse af sikkerhedsgodkendelse anvendes et oplysnings-skema (1-2-3) i henhold til underbilag 1. Oplysningsskema 1-3 findes tillige i en engelsk-sproget udgave (Information form 1-3).

Link til oplysningsskemaerne, som skrivbare skabeloner, findes bagerst i denne bestemmelse.

6.2 Oplysningsskemaerne indeholder en samtykkeerklæring, der skal underskrives af såvel den, der indstilles til sikkerhedsgodkendelse, som dennes ægtefælle eller samlever.

6.3 Indgår en sikkerhedsgodkendt person ægteskab eller får en fast samlever, skal der på ny udfærdiges oplysningsskema.

6.4 Godkendelse til YHM kan tidligst opnås, når den pågældende 1) har været sikkerhedsgodkendt til HEM i mindst de seneste seks måneder, og 2) i denne periode har forrettet tjeneste eller været ansat inden for Forsvarsministeriets koncern eller i den civile virksomhed.

FE kan i særlige tilfælde dispensere fra disse tidsmæssige krav.

6.5 For personel, der ikke umiddelbart opfylder betingelserne for erhvervelse af en godkendelse til YHM, men hvis senere tjeneste eller arbejde forudsætter en sådan sikkerhedsgodkendelse, udfyldes oplysningsskema 2 med henblik på en forhåndsundersøgelse til YHM. Hvis den pågældende ikke allerede er sikkerhedsgodkendt til HEM, vil der blive med-delt en sådan godkendelse, når FE forhåndsundersøgelse er afsluttet.

6.6 Såfremt indstilling omfatter godkendelse til materiale, der indbefatter mærkninger og betegnelser, i henhold til kapitel 1, skal indstillende myndighed anføre dette på oplysnings-skemaet.

Ved indstilling om fornyelse af sikkerhedsgodkendelse anvendes oplysningsskema 1 (TTJ/NR og FTR/NC) eller oplysningsskema 2 (HEM/NS og YHM/CTS), som angivet i underbilag.

7. SÆRLIGE FORHOLD I FORBINDELSE MED INDSTILLING

For følgende personalekategorier gælder særlige forhold ved indstilling til sikkerhedsgodkendelse:

7.1 Personel uden dansk statsborgerskab, der ønsker tjeneste inden for Forsvarsministeriets koncern.

Ved indstilling om sikkerhedsgodkendelse af personel uden dansk statsborgerskab, som skal forrette tjeneste inden for koncernområdet, skal oplysningsskemaet bilægges den ansvarlige myndigheds skriftlige bemyndigelse til ansættelse. (Gælder ikke ansatte i civile virksomheder).

Af hensyn til FE muligheder for at tilvejebringe vandelsoplysninger er det normalt en forudsætning for sikkerhedsgodkendelse, at den pågældende person inden for de seneste 7 år har været bosat i Danmark eller i lande, der er medlem af NATO og/eller EU.

7.2 Udenlandske elevers deltagelse i uddannelse.

Når undervisning og uddannelse af udenlandske elever finder sted ved koncernens myndigheder, herunder bl.a. Forsvarsakademiet og officerssskolerne, gennemføres følgende procedure, som sikrer udenlandske elevers bedst mulige udbytte af den militære uddannelse i Danmark:

- For elever fra NATO eller EU medlemslande og lande med hvilke Forsvarsministeriet har sikkerhedsaftaler jf. kapitel 1 skal elever medbringe nationalt udstedt sikkerhedscertifikat, som umiddelbart kan accepteres.
Når udenlandske forsvarsministerier eller andre udenlandske myndigheder meddeler navne og personlige data på elever, de ønsker at sende på danske militære uddannelser eller træningsophold, skal disse myndigheder tillige meddele den enkelte persons nationale grad af sikkerhedsgodkendelse. Eleven medgives et dokument eller certifikat som dokumenterer sikkerhedsgodkendelsen. Dokumentet/certifikatet skal afleveres til det danske uddannelsessted.
- For elever fra ikke NATO eller EU medlemslande og fra lande, hvormed der ikke er indgået sikkerhedsaftale, indsendes sikkerhedsdokumentet eller sikkerhedscertifikatet til FE for afgørelse minimum 14 dage før påbegyndelse af uddannelsen/opholdet.

SIKKERHEDSSAMTALE

FE gennemfører sikkerhedssamtale (SIKSAM) med personel, der indstilles til godkendelsen YHM og CTS. Der afholdes endvidere SIKSAM med alt personel, der beordres til tjeneste i internationale stabe i udlandet eller skal ansættes ved FE.

Med mellemrum føres opfølgende sikkerhedssamtale med personel til tjeneste i udlandet.

MEDDELELSE OM SIKKERHEDSGODKENDELSE

Når sikkerhedsgodkendelsen foreligger, meddeler FE dette i DeMars. Såfremt den indstillende institution, myndighed eller virksomhed ikke har DeMars adgang, vil den modtage skriftlig underretning herom.

For personel, der beordres til tjeneste i NATO eller EU-stabe, underrettes den danske repræsentation ved den pågældende stab om sikkerhedsgodkendelsen.

Afslag på indstilling om sikkerhedsgodkendelse vil blive meddelt direkte til den berørte person. I skrivelsen gives der en begrundelse for afslaget. Skrivelsen vil være mærket Personoplysning fortrolig.

Endvidere vil afslaget blive meddelt indstillende institution, myndighed eller virksomhed i særlig skrivelse. Årsagen til afslaget vil ikke blive anført. Skrivelsen vil være mærket Personoplysning fortrolig.

8. SIKKERHEDSCERTIFIKAT

For personel, der godkendes til YHM eller CTS udstedes et sikkerhedscertifikat på dansk (se underbilag 2 til bilag 1), der bekræfter den pågældendes sikkerhedsgodkendelse.

For personel ved nationale elementer i internationale stabe og ved forsvarsattaché-embeder udstedes der desuden, uanset godkendelsesgrad, et NATO Personnel Security Clearance Certificate (alternativt et EU Security Certificate) (se underbilag).

Sikkerhedscertifikatet opbevares ved det tjenestested, hvis chef skal bemyndige den pågældende indsigt i klassificeret materiale.

Sikkerhedscertifikatet skal underskrives af vedkommende, det er udstedt på (certifikatets pkt. 2), ligesom tjenestestedets sikkerhedsofficer ved sin underskrift bekræfter, at den pågældende er instrueret i overensstemmelse med teksten på certifikatet (certifikatets pkt. 3). Derefter bekræfter tjenestestedets chef (direktør, leder, mfl.), ved sin underskrift den pågældendes bemyndigelse til indsigt i klassificeret materiale i henhold til det tjenstlige behov (certifikatets pkt. 4, bagsiden).

Den i certifikatets pkt. 5 anførte sikkerhedsinstruktion skal gives mindst én gang om året, og den pågældende skal kvittere for at have modtaget instruktionen, der kan gives mundtligt til den sikkerhedsgodkendte person (evt. flere i et samlet forum) eller i skriftlig form. Anvendes sikkerhedsgodkendelsen kun i forbindelse med designering, kan instruktion og underskrift foretages efter fremmøde ved designeringsenheden, og de periodiske instruktioner kan herefter foretages ved fremmøde i forbindelse med tjeneste i designeringsfunktionen.

Ved afgang fra den tjenestefunktion, der har begrundet udstedelse af sikkerhedscertifikatet, underskriver den pågældende certifikatets pkt. 6, og tjenestestedet eller designeringsstedet afmelder derefter sikkerhedsgodkendelsen ved påtegning af certifikatet, der returneres til FE.

Ved fornyelse af sikkerhedsgodkendelse og udstedelse af nyt sikkerhedscertifikat destrueres det tidligere certifikat ved sikkerhedsofficerens/chefens foranstaltning.

For kryptoautorisation udstedes kryptocertifikat til personel, der skal have adgang til materiale, mærket KRYPTO/CRYPTO. Certifikatet må kun udstedes, hvis der foreligger bekræftelse på den krævede sikkerhedsgodkendelse og sikkerhedsbelæring er givet.

CERTIFIKAT TIL BRUG VED INTOPS, MØDER, KONFERENCER, KURSER MV. I NATO ELLER EU

For personel, der skal deltage i INTOPS, møder, konferencer, kurser mv. inden for NATO eller EU og som skal have adgang til klassificeret materiale, udsteder tjenestestedet et CERTIFICATE OF SECURITY CLEARANCE (se underbilag), der bekræfter den pågældendes sikkerhedsgodkendelse. Certifikatet sendes til den myndighed, der er ansvarlig for at give den pågældende person bemyndigelse til indsigt i omhandlede materiale.

9. PERSONEL TIL TJENESTE I NATO ELLER EU

Før personel tiltræder tjeneste i NATO eller EU-stabe, skal personellet være sikkerhedsgodkendt ved beordrende myndigheds foranstaltning i overensstemmelse med kravet til den stilling, der skal bestrides. Indstillende myndighed orienterer om beordringen ved skrivelse

til FE. Skrivelsen skal være FE i hænde senest 3 måneder før stillingen skal tiltrædes og skal indeholde flg. oplysninger:

- CPR-nummer
- MA-nummer
- Samtlige fornavne og efternavn
- Udstationeringsperioden
- Myndighed hvortil certifikatet skal sendes.

FE kan udover det danske sikkerhedscertifikat, jf. pkt. 10, evt. udstede et NATO eller EU Personnel Security Clearance Certificate, jf. underbilag . Disse certifikater udstedes kun efter behov og konkret anmodning).

10. SIKKERHEDSGODKENDELSERS GYLDIGHED

Sikkerhedsgodkendelser har følgende gyldighedsperioder:

Klassifikationsgrad:

TIL TJENESTE- BRUG	NATO RESTRICTED	RESTREINT UE/EU RESTRICTED	5 år
FORTROLIGT	NATO CONFIDENTIAL	CONFIDENTIEL UE/EU CONFIDENTIAL	5 år
HEMMELIGT	NATO SECRET	SECRET UE/EU SECRET	5 år
YDERST HEM- MELIGT	COSMIC TOP SECRET	TRÈS SECRET UE/EU TOP SECRET	5 år

10.1 Personer med bopæl i udlandet meddeles godkendelser for kortere perioder, afhængig af hvor i udlandet bopælen er beliggende.

11. FORHOLD EFTER MEDDELT SIKKERHEDSGODKENDELSE

11.1 Sikkerhedsinstruktion.

Personel, der er meddelt sikkerhedsgodkendelse, skal gives en sikkerhedsinstruktion, der udover generelle sikkerhedsmæssige forhold også skal omhandle forhold af lokal karakter, jf. sikkerhedsinstruksen.

Tavshedspligten skal altid indskræpes.

Se også kapitel 1, bilag 3.

11.2 Bemyndigelse.

Chefen fastsætter i hvilket omfang, den pågældende skal bemyndiges indsigt i klassificeret materiale.

Personel, der er sikkerhedsgodkendt til HEM eller højere, skal enten være opført på en bemyndigelsesliste eller være omfattet af en generel bemyndigelse givet af chefen i institutionens eller myndighedens sikkerhedsinstruks.

11.3 Særlige forhold.

Såfremt der efter meddelt sikkerhedsgodkendelse opstår tvivl om en persons sikkerhedsmæssige kvalifikationer, skal chefen (direktøren, lederen mfl.) efter forholdene begrænse den pågældendes adgang til klassificerede informationer eller materiel og områder ved myndigheden eller virksomheden. Forholdene indberettes til FE.

11.3.1 Militær straf

Når en sikkerhedsgodkendt person ikendes en militær straf, skal FE skriftligt orienteres ved kopi af straffebladsformular.

11.4 Oplysningspligt.

Personel, der er sikkerhedsgodkendt, er forpligtet til at underrette myndigheden eller virksomheden, hvis vedkommende kommer i konflikt med lovgivningen. Underretningspligten omfatter ikke bøder for overtrædelse af færdselsloven, medmindre bøden skyldes spirituskørsel eller førerretten samtidig er blevet frakendt. Myndigheden eller virksomheden tilsender FE indberetning herom.

11.5 Ændringer og tilføjelser til personeloplysninger.

Institutioner, myndigheder og virksomheder skal løbende underrette FE om følgende oplysninger for personel, der er meddelt sikkerhedsgodkendelse til FTR eller højere:

- Afgang fra uddannelse eller kursus, hvortil der er meddelt sikkerhedsgodkendelse, såfremt afgang er begrundet i sikkerhedsmæssige forhold
- Årsag til afskedigelse eller kontraktophævelse "i utide"
- Navneændring
- Ændring af fast bopæl til udlandet
- Der skal ske underretning ved indgåelse af ægteskab eller fast samlivsforhold. Se pkt. 6.3.

I tilfælde af ophævelse af ægteskab/samlivsforhold skal der tilsvarende ske underretning.

12. AFMELDING AF SIKKERHEDSGODKENDELSE

Ved hjemsendelse og pensionering, afskedigelse eller opsigelse af ansættelsesforholdet bortfalder sikkerhedsgodkendelsen. FPS, institutionen eller virksomheden er i disse tilfælde ansvarlig for at afmelde sikkerhedsgodkendelsen hos FE. Det samme gælder dødsfald.

OVERSIGHT OVER ANVENDELSE AF OPLYSNINGSSKEMAER MV.

VED INDSTILLING TIL ↓ ↓	ANVENDES →	SKEMA ¹		
		1	2	3
TIL TJENESTEBRUG (<i>NATO RESTRICTED, RESTREINT UE</i>)		X		
FORTROLIGT (<i>NATO CONFIDENTIAL, CONFIDENTIEL (UE)</i>)		X		
HEMMELIGT (<i>NATO SECRET, SECRET UE</i>)				
a. Godkendelse (1. gang)			X	
b. Fornyelse eller generhvervelse				X
c. Ved indgåelse af ægteskab herunder fast samlivsforhold				X
YDERST HEMMELIGT (<i>COSMIC TOP SECRET, TRÉS SECRET UE, FOCAL TOP SECRET</i>)				
a. Den indstillede har ikke tidligere været godkendt til HEMMELIGT eller YDERST HEMMELIGT			X	
b. Fornyelse				X
c. Ved indgåelse af ægteskab herunder fast samlivsforhold				X

¹ Oplysningsskema 1, 2 og 3 findes i både dansk- og engelsksproget udgave.

EKSEMPEL PÅ SIKKERHEDSCERTIFIKAT

Sikkerhedscertifikat

FORSVARETS
EFTERRETNINGSTJENESTEKastellet 30
2100 København Ø
Telefon: 33 32 55 66
godkendelser@fe-ddis.dk
www.fe-ddis.dk3. maj 2017
Sagsnr. 30019-16

1

Anders Andersen

311260-9999 Seniorsergent HRN

er hermed godkendt til at måtte få indseende i nationale/NATO/EU sager klassificeret:

YDERST HEMMELIGT

Sikkerhedsgodkendelsen er gældende til: [Udløbsdato]

Underskrift

Peter Sloth

orlogskaptajn

Leder af Element for Sikkerhedsgodkendelser

- 2 Undertegnede erklærer herved, at jeg er instrueret om de nationale/NATO/EU-sikkerhedsdirektiver/-bestemmelser, der gælder for behandling af nationale/NATO-sager klassificeret som anført i pkt. 1. Jeg er herunder blevet gjort bekendt med, at sådanne sager kræver en særlig behandling, og at de indeholder oplysninger, hvis videregivelse uden tilladelse kan skade den danske stat i **yderst alvorlig grad**, og/eller kan forårsage **overordentlig alvorlig skade** for NATO eller EU, samt at brud på tavshedspligten efter omstændighederne straffes efter straffelovens § 152 og den militære straffelovs §§ 17 og 32. Jeg erklærer endvidere, at jeg fuldt ud har forstået det særlige ansvar, der påhviler mig med hensyn til opbevaring af sager klassificeret, som anført i pkt.1.

Sted: _____

Dato: _____

Underskrift

- 3 Undertegnede sikkerhedsofficer har d.d. instrueret underskriveren om de særlige nationale/NATO-sikkerhedsdirektiver/-bestemmelser, der gælder for behandling af sager klassificeret som anført i pkt.1.

Det attesteres, at nærværende certifikat er underskrevet i mit påsyn.

Sted: _____

Dato: _____

Underskrift

Grad, navn, myndighed

4

Dato: _____

Grad/navn

bemyndiges hermed adgang til: _____

Underskrift

Chef/myndighed

- 5 Undertegnede erklærer herved at have modtaget sikkerhedsinstruktion om de særlige nationale/NATO sikkerhedsdirektiver/-bestemmelser, der er gældende for sager, som anført under pkt.1.

Dato: _____

Underskrift _____

Sikkerhedsofficer/attestation _____

- 6 Undertegnede, der afgår fra tjenestestedet/ophører med at være beskæftiget med arbejde, der nødvendiggør adgang til sager klassificeret som anført under pkt.1, erklærer herved, at jeg er instrueret om det særlige og vedvarende ansvar, der er pålagt mig med hensyn til hemmeligholdelsen af de oplysninger, der indeholdes i disse sager. Jeg er indforstået med, at jeg fortsat er underkastet tavshedspligten og at brud på denne efter omstændighederne straffes efter straffelovens § 152 og den militære straffelovs §§ 17 og 32.

Sted: _____

Dato: _____

Underskrift

Påtegninger ved afmelding: _____

ATTESTATION OF NATO PERSONNEL SECURITY CLEARANCE

Bilaget blev med rettelse 42, erstattet af disse link til den skrivbare skabelon.

[FIIN link](#)

[Internet link](#)

EKSEMPEL PÅ NATO SECURITY CERTIFICATE

NATO UNCLASSIFIED

DANISH DEFENCE
INTELLIGENCE SERVICE

Kastellet 30
DK-2100 Copenhagen
Tel: +45 33 32 55 66
rsp@fe-ddis.dk
www.fe-ddis.dk

May 2, 2014
Reference: [Sagsnummer]

NATO Personnel Security Clearance Certificate

1. Certification is hereby given that:
Full Name: **[Fornavne] [Efternavn]**

Date and Place of Birth: **30. september 2013, [Fødested], Denmark**

has been granted a security clearance by the Government of **DENMARK**

in accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and is, therefore, declared suitable to be entrusted with information classified up to and including:

NATO SECRET

2. The validity of this certificate will expire not later than **[Udløbsdato]**

Signed: Ingrid Kynde Nielsen

Title: MJ/DNKA

Date of Issue: May 2, 2014

Official government stamp

Contact details of the issuing authority: Phone **+45 33 32 55 66** E-mail **Milsik@fe-ddis.dk**

Source: NATO Directive AC/35-D/2000 Appendix 1 Annex 1

NATO UNCLASSIFIED

EKSEMPEL PÅ EU SECURITY CERTIFICATE

EU UNCLASSIFIED

DANISH DEFENCE
INTELLIGENCE SERVICEKastellet 30
DK-2100 Copenhagen
Tel: +45 33 32 55 66
rsp@fe-ddis.dk
www.fe-ddis.dk

25. februar 2014

Reference: [Sagsnummer]

EU Security Certificate**This is to certify that:**

[Fornavne] [Efternavn]

[Fødested], [Fødselsdag], Denmark

is the holder of a security clearance established by the Government of **DENMARK**

In conformity with EU regulations and may receive information up to and including:

EU SECRET/ SECRET UE

The present certificate expires on: [Udløbsdato]

Signed: Ingrid Kynde Nielsen

Title: MJ/DNK A

Official government stamp

Date: [Afsendt]

EU UNCLASSIFIED

**FORHOLD VEDRØRENDE SIKKERHEDSGODKENDELSE
AF PERSONEL VED BOSÆTTELSE I UDLANDET.****1. FORMÅL**

At fastsætte retningslinjer, der skal følges, når personel, der er eller påtænkes meddelt sikkerhedsgodkendelse, beslutter at bosætte sig eller allerede bor i udlandet.

2. OMFANG

De anførte retningslinjer er gældende for militært og civilt personel, godkendt til klassifikationsgraderne HEM eller YHM, der forretter tjeneste i Danmark og er bosat eller beslutter at bosætte sig i udlandet.

Militært og civilt personel, der er godkendt til FTR eller til TTJ, og som allerede er bosat i udlandet og forretter tjeneste i Danmark, vil ligeledes være undergivet nærværende retningslinjer, såfremt det pågældende personel ønskes sikkerhedsgodkendt til HEM eller højere.

3. GENERELT

Personel, der er godkendt til klassifikationsgraden HEM og højere, er forpligtet til skriftligt at meddele tjenestestedet, såfremt pågældende agter at bosætte sig i udlandet.

Chefen (direktøren, lederen, mfl.) afgør, hvorvidt den pågældende sidder inde med sensitiv viden, der skønnes ikke at være forenelig med bosættelse i udlandet. Vurderes dette at være tilfældet, træffer institutionen, myndigheden eller tjenestestedet foranstaltninger til at ændre tjenestefunktion og sikkerhedsgodkendelse i overensstemmelse hermed, såfremt den pågældende fastholder at ville bosætte sig i udlandet.

Institutionen, myndigheden eller tjenestestedet meddeler i alle tilfælde skriftligt den pågældende sin stillingtagen. Der sendes efterretningskopi til FE.

For personel, der er godkendt til klassifikationsgraden YHM, foretager institutionen, myndigheden eller tjenestestedet en vurdering af, hvorvidt opretholdelse af sikkerhedsgodkendelsen er forenelig med bosættelse i udlandet. Vurderingen påføres eller vedlægges en indberetning, der sendes til FE, som træffer afgørelse i sagen.

4. OPLYSNINGSPLIGT

Personel, der er omfattet af disse bestemmelser, er forpligtet til at underrette tjenestestedet, såfremt vedkommende kommer i konflikt med lovgivningen i det land, hvor pågældende har valgt at bosætte sig. Institutionen, myndigheden eller tjenestestedet tilsender FE indberetning herom.

PROCEDURER VED UDENLANDSK VIP-BESØG

Ref.:

FKOPLAN OP.120-1, Forsvarets Beredskabsplan.

1. INDLEDNING

Det kan ikke udelukkes, at betydningsfulde udenlandske personer, der aflægger besøg ved forsvaret – politiske ledere, embedsmænd og højtstående officerer mv. – af forskellige grunde kan være potentielle mål for terroraktioner eller andre kriminelle handlinger under deres ophold i Danmark, hvorfor en nøje planlægning ved værtsmyndigheden skal finde sted.

2. RAPPORTERING

Værtsmyndigheden iværksætter snarest efter, at besøget er kendt, rapportering til Forsvarets Efterretningstjeneste (FE) og Forsvarskommandoen (FKO).

2.1. Rapportens indhold.

Følgende bør fremgå af rapporten:

- Hvem den besøgende er
- Hvornår besøget finder sted
- Program for besøget, evt. et foreløbigt program
- En evt. trusselvurdering og/eller særlige sikkerhedskrav fra den besøgendes sikkerhedsorganisation
- Om der medbringes livvagter, bevæbnede eller ubevæbnede.

De ovenfor anførte oplysninger vil normalt ikke kunne fremskaffes eller afklares i forbindelse med den indledende planlægning, men fremkommer ofte som stykvise informationer i planlægningsfasen. Det er derfor vigtigt, at værtsmyndigheden løbende orienterer om besøgets planlægning og tilgåede oplysninger. Det skal understreges, at værtsmyndigheden har det fulde ansvar for tilvejebringelsen af relevante oplysninger.

2.2. Sikkerhedsmæssige krav.

Medmindre der foreligger særlige sikkerhedsmæssige krav fra den besøgendes side anlægges sikkerhedsniveauet på baggrund af de danske myndigheders trusselvurdering.

2.3. Livvagter.

Værtsmyndigheden skal tilsikre, hvor det foreligger oplyst at der medbringes livvagter, at der indhentes oplysninger om navne, persondata samt våbentype og -nummer. Dette skal anvendes til udfærdigelse af midlertidig våben- og bæringstilladelse, som gives af Rigspolitichefen.

For udenlandske livvagters færden på dansk område gælder følgende bestemmelser, som håndhæves af Rigspolitichefen:

- Der gives aldrig tilladelse til bæring af automatiske våben
- Der skal i hvert enkelt tilfælde søges om våben- og bæringstilladelse
- Der vil i de tilfælde, hvor der evt. gives våben- og bæringstilladelse til medfølgende livvagter, ske attachering af danske livvagter

- Afvæbning af udenlandske livvagter vil finde sted, hvis der ikke foreligger en våbentilladelse.

3. TRUSSELSVURDERING

På baggrund af værtsmyndighedens rapportering vil der, koordineret mellem FE og Rigspolitechefen, blive udarbejdet trusselsvurderinger for besøget, såfremt det skønnes nødvendigt. Form og indhold kan variere efter forholdene.

Trusselsvurderingen er grundlaget for den anbefaling Rigspolitechefen giver lokale politimyndigheder vedrørende sikkerhedsforanstaltninger, herunder anvendelse af livvagter, samt den anbefaling, som FE giver værtsmyndigheden.

4. PLANLÆGNING

Afhængigt af besøgets art kan det være nødvendigt at afholde planlægningsmøder.

Værtsmyndigheden skal sikre, at den lokale politikreds og evt. FE er repræsenteret med henblik på tilrettelægning af de sikkerhedsmæssige foranstaltninger, der anses for nødvendige i henhold til trusselsvurderingen.

5. ANSVARSFORDELING

Det sikkerhedsmæssige ansvar ved VIP-besøg skal tilstræbes fordelt således:

5.1. Personsikkerhed – livvagter.

Ansaret påhviler Rigspolitechefen såvel inden- som udenfor militært område.

5.2. Områdesikkerhed – bevogtning af besøgsstedet.

5.2.1. Militært område.

Ansaret påhviler den lokale militære chef. Hvor et besøg inddrager flere militære områder eller militære myndigheder, har værtsmyndigheden det koordinerende ansvar således, at de sikkerhedsmæssige tiltag fremstår ensartet og afbalanceret på alle besøgssteder. Det kan være praktisk i et vist omfang at anvende enkeltforanstaltninger fra ref. kapitel 2, bilag 2, underbilag 1, Sikkerhedsberedskabsforanstaltninger, idet alle myndigheder i forvejen har udarbejdet detailplaner for iværksættelse heraf.

5.2.2. Civilt område.

Ansaret påhviler under alle forhold Rigspolitechefen og den lokale politikreds. Hvor særlige forhold nødvendiggør anvendelse af militært personel, skal dette ske efter de fastsatte regler i ref. kapitel 10, bilag 2, Særlige hjælp til politiet.

PRÆCISERING AF GÆLDENDE REGLER VEDRØRENDE TAVSHEDSPLIGT

Bilaget blev med rettelse 42, erstattet af disse link til den skrivbare skabelon.

[FIIN link](#)

[Internet link](#)

KAPITEL 3

MATERIELSIKKERHED

1. INDLEDNING

Materielsikkerhed omfatter foranstaltninger til beskyttelse af koncernens materiel - herunder våben, ammunition og eksplosivstoffer - mod spionage, sabotage samt hærværk, og tyveri mv.

Foranstaltningerne omfatter beskyttelse af forsvarets materiel under alle forhold, herunder produktion, anskaffelse, opbevaring, drift og udfasning.

De sikringsmæssige foranstaltninger fastlægges ud fra en konkret risikovurdering, hvori bl.a. skal indgå:

- fastsat sikkerhedsklassifikation
- vurderet operativ betydning
- anvendelsesmulighed
- mulighed for genanskaffelse
- økonomisk værdi.

2. FORMÅL

Formålet med dette kapitel er at beskrive de minimumskrav, der er gældende for beskyttelse af koncernens materiel.

I de tilfælde hvor NATO, EU eller tilsvarende sikkerhedskrav til håndtering og opbevaring af materiel er højere eller markant anderledes end tilsvarende nationale, vil det fremgå af teksten.

3. ANSVAR

Chefen (direktøren, lederen mfl.) er ansvarlig for udøvelse af samt kontrol med materielsikkerheden inden for eget myndighedsområde.

Chefen er ansvarlig for, at klassificeret samt vitalt og/eller sensitivt materiel, herunder våben, ammunition og eksplosivstoffer, opbevares i henhold til:

- sikkerhedsmæssige minimumskrav som beskrevet i nærværende kapitel
- sikkerhedsbestemmelser for magasinering af ammunition og eksplosivstoffer (eksplosivstofsikkerhed)
- miljø - og arbejdssikkerhed
- materiefaglige bekendtgørelser.

Chefen er tillige ansvarlig for, at personel, der udpeges til at beskæftige sig med materiel, som kræver sikkerhedsbeskyttelse, har den fornødne sikkerhedsgodkendelse, bemyndigelse og sikkerhedsmæssige uddannelse.

4. KLASSIFIKATION, INDDDELING OG MÆRKNING

Materielanskaffende myndighed er ansvarlig for fastsættelse og ajourføring af klassifikation for materiel omfattende klassifikationsgraderne FTR og højere. På tilsvarende vis skal materielanskaffende myndighed markere centralt vurderet vitalt og sensitivt materiel i materielssystemet DeMars.

Chefen er ansvarlig for, at lokalt vurderet vitalt og sensitivt materiel indgår i risikovurderingen jf. kap. 9.

Materiel, hvor sikringsmæssige foranstaltninger fastlægges, inddeles således:

4.1. Klassificeret materiel.

Materiel, hvor en egentlig klassifikation er fastsat.

Klassificeret materiel har varierende dimensioner, karakter og anvendelse, og det er således ikke muligt at fastsætte generelle retningslinjer for klassifikationsmærkning af materiel, materieldele og komponenter mv. Såfremt en klassificeret materielgenstand kan adskilles i flere dele, skal hver del klassificeres separat. Hvor klassifikationsmærkningen vurderes at være påkrævet, udføres denne i overensstemmelse med de i kapitel 1 anførte principper. Klassifikationsmærkning må ikke direkte kunne iagttages af uvedkommende. Dette princip gælder ikke for printere, scannere, makulatorer og kopimaskiner o.l. der skal afmærkes med den klassifikationsgrad de må anvendes til.

4.2. Vitalt materiel.

Materiel, for hvilket der gælder særlige forhold vedrørende:

- vurderet operativ betydning
- vurderet mulighed for genanskaffelse
- økonomisk værdi.

4.3. Sensitivt materiel.

Materiel, for hvilket der gælder særlige forhold vedrørende:

- særlig sikkerhedsrisiko (rettet mod forsvaret eller andre myndigheder)
- uretmæssig anvendelse (attraktivt, tyvetækeligt)
- materiel hvor der kontraktligt er indgået aftale om særlige sikkerhedsmæssige foranstaltninger.

4.4. Øvrigt materiel.

Materiel, der ikke falder ind under pkt. 5.1, 5.2 og 5.3.

5. OPBEVARINGSKRAV OG OMRÅDEINDDDELING

Områdeinddeling og sikringsniveau, mekanisk sikring, elektronisk overvågning og bevogtning fremgår af kapitel 7.

5.1. Klassificeret materiel.

5.1.1. Inden for et etablissemments perimeterhegn, kategori 1-3, (Egentlig bevogtning).

- Materiel, der er klassificeret YHM, skal opbevares og sikres i Sikret område, kategori 1, sikringsniveau 60.

- Materiel, der er klassificeret HEM, skal opbevares og sikres i Sikret område, kategori 1, sikringsniveau 50 eller i Sikret område, kategori 2, sikringsniveau 40 i et klasse A opbevaringsmiddel.
- Materiel, der er klassificeret FTR, skal opbevares og sikres i Sikret område, kategori 2, sikringsniveau 40.
- Materiel, der er klassificeret TTJ, kan opbevares i Kontrolleret område, kategori 3, sikringsniveau 10/20.

Hvis materiellet har en sådan dimension, at det er muligt/rimeligt at opbevare de klassificerede dele i et klasse A (jf. EN 1143-1 grade 0 eller bedre eller SS3492) eller B opbevaringsmiddel (Jf. F&P GUL klasse hovedgruppe 2), følges bestemmelserne som gældende for dokumenter (se kapitel 4).

Under særlige omstændigheder, hvor dette ikke kan opfyldes, kan klassificeret samt vitalt og/eller sensitivt materiel opbevares i et overvåget område, områdekategori 4. FE skal inddrages i det enkelte tilfælde m.h.p. at foretage en vurdering af de samlede sikringsmæssige tiltag. Disse skal tilgodese forholdet mellem den samlede anslåede gennembrydnings- og/ eller oplukningstid jf. F&P klassificering i forhold til den forventelige indsatstid fra reaktionsstyrke og/eller politi. Dette forhold opnås ved en øget anvendelse af mekanisk sikring og elektronisk overvågning i forhold til de fastsatte sikringsniveauer jf. kapitel 7. Som princip skal den samlede mekaniske sikrings holdetid i minutter, som minimum være det dobbelte af reaktionstiden for indsatsstyrken.

Hjemmeværnskommandoen foretager vurderingen inden for eget myndighedsområde,

5.1.2. Uden for et etablissemments perimeterhegn, kategori 4, (Bevogtningsmæssigt tilsyn).

- Materiel, der er klassificeret TTJ kan opbevares i Overvåget område, kategori 4, sikringsniveau 10-40.

En samlet oversigt fremgår af efterfølgende matrix.

Opbevaringskrav for klassificeret materiel områdeinddeling/sikringsniveau

			SIKRINGSNIVEAU					KLASSIFICERET MATERIEL
			10/ 20	30	40	50	60	
OMRÅDEINDELING	1	SIKRET					X	YHM
					(X) ¹	X	(X) ²	HEM
	2			X ³	X			FTR
	3	KONTROLLRET	X					TTJ
	4	OVERVÅGET	X	X	X			TTJ

Beskrivelse af sikringsniveau fremgår af bilag 3 til kapitel 7.

6. VITALT OG/ELLER SENSITIVT MATERIEL**6.1. Materiel.**

Materiel, der er af vital operativ betydning, og hvor genforsyning er vanskelig, tidskrævende eller økonomisk ressourcekrævende, samt hvor materiellet er anvendeligt i uretmæssig sammenhæng, skal generelt opbevares i Sikret område, kategori 1, sikringsniveau 50-60 eller Sikret område, kategori 2, sikringsniveau 30-40.

Oversigt over materiel - der henføres til kategorien vitalt og/eller sensitivt materiel - fremgår af bilag 1.

¹ Hvis materielgenstanden opbevares i et Klasse A opbevaringsmiddel.

² Anvendes hvis der vurderes at være en særlig sikkerhedsrisiko f.eks. håndbårne missilsystemer

³ Hvis materielgenstanden opbevares i et Klasse A opbevaringsmiddel.

6.2. Håndvåben generelt.

Håndvåben skal – såfremt de ikke er under direkte fysisk kontrol – som minimum opbevares i Sikret område, kategori 2, sikringsniveau 40.

Oversigt over håndvåben og vitale dele fremgår af bilag 1 (se bilag 1).

6.2.1. Håndvåben opbevaret ved enheden (UAFD/AFD).

Våben opbevares med vital våbendel udtaget.

Våben opbevares i våbenopbevaringsrum.

Vital våbendel opbevares separat i stålskab, klasse A, (fx våbenskab) i våbenopbevaringsrum.

Våbenopbevaringsrummet etableres i Sikret område, kategori 2, sikringsniveau 40.

Mindre mængder håndvåben kan – hvor de samlede sikringsløsninger vurderes tilstrækkelige – opbevares i Sikret område, kategori 2, sikringsniveau 30 med vital del udtaget. Styrrammer uden vitale dele og vitale dele skal opbevares i hvert sit klasse A opbevaringsmiddel.

Pistoler kan opbevares samlet, såfremt de opbevares i sikret område, kategori 2, sikringsniveau 40 i et grade 1 opbevaringsmiddel jf. EN 1143-1, samt at sikringsdøren er en RC 4 jf. EN 1627-30 eller en grade 1 dør jf. EN 1143-1.

6.2.2. Håndvåben oplagt ved myndigheden (NIV III/II).

6.2.2.1. Inden for et etablissemments perimeterhegn, kategori 1-3 (Egentlig bevogtning).

Våben oplægges i våbenopbevaringsrum, depot eller magasin. Afhængig af de samlede sikringsløsninger oplægges våben på følgende måde:

- Våben kan oplægges i depot i Sikret område, kategori 2, sikringsniveau 40. Den vitale våbendel skal udtages og opbevares i et klasse A opbevaringsmiddel.
- Våben kan undtagelsesvis oplægges i funktionsduelig stand i lokaliteter, der opfylder kravene til Sikret område, kategori 1, sikringsniveau 50, hvor rummet opfylder kravene til et boksrum eller et arkivrum jf. UNDERBILAG 5 til BILAG 2 til KAPITEL 7.
- Våbenplatforme (F.eks. Fly, kampvogne og skibe) vil normalt rumme såvel klassificerede som vital/sensitive komponenter og data. Våbenplatformens sikring skal fastlægges på baggrund af en risikovurdering af de beskyttelseskrævende aktiver jf. kapitel 9. Foranstaltninger til beskyttelse af aktiverne bør normalt beskrives i sikringsniveau(er). Hvis det ikke er hensigtsmæssigt bør kravene beskrives som angivet i Dansk Standard (DS) eller Europæiske Norm (EN). Anskaffende myndighed, er ansvarlig for at sikringskravene til beskyttelse af våbenplatformen er udarbejdet, inden udlevering til anvendelse sker.
- De eksisterende våbenplatforme, hvor der ikke allerede er udarbejdet krav til sikring, skal af brugende enhed beskyttes i overensstemmelse med lokal udarbejdet risikovurdering.

6.2.2.2. Uden for et etablissemments perimeterhegn, kategori 4.

Tunge våben kan oplægges i depot eller magasin¹ under anvendelse af minimum sikringsniveau 10 efter udarbejdelse af risikovurdering.

¹ Hvis magasinet ikke fremgår af magasinoversigten jf. kap 7. skal der indhentes en tillades fra FE før benyttelse af magasinet må foretages.

6.2.2.3.

Håndvåben må ikke opbevares i områdekategori 4. HJV er undtaget for denne regel idet HJV-våben er opbevaret under skærpede krav jf. HJV-bestemmelser. Tunge våben oplægges med evt. vital våbendel udtaget. Vital våbendel opbevares adskilt fra våben i et andet depot eller magasin.

Vitale våbendele skal som minimum opbevares i opbevaringsmiddel, klasse A.

6.2.3. To-faktoradgang til funktionsduelige håndvåben i Danmark.

6.2.3.1. Stabe og enheder.

I våbenopbevaringsrum, hvor vitale våbendele opbevares i særskilt boks, skab eller lign., skal det tilsikres, at samme personer ikke har adgang til både våbenopbevaringsrum og til skab/boks med vital våbendel.

I de tilfælde, hvor der er flere brugere af våbenkammer/rum indeholdende skabe/bokse til vital våbendel, fx delinger i en underafdeling, skal vital våbendel opbevares i delingens eget skab/boks, og de enkelte skabe/bokse skal udstyres med elektronisk kodelås (sidstnævnte foranstaltning skal ske inden udgangen af 2023).

Der skal være to personer med autoriseret adgang til stede ved ud- og indlevering af håndvåben med vital del. Der er således krav om to personer med autoriseret adgang for at kunne samle et funktionsdueligt våben.

Sker adgangen til og oplåsning af rum, boks eller skab til vital våbendel via et adgangskontrolsystem, kan ovennævnte metode afløses af to autoriserede personer, der inden for et kort tidsrum, begge anvender separat kodet kort med egen kode for at få adgang.

Det er et chefansvar, at de vitale våbendele optælles efter brug og før aflåsning.

6.2.3.2. Våbenværksteder.

Der skal være to personer med autoriseret adgang til våbenværkstedet til stede, når der gives adgang til opbevaringsrummene for funktionsduelige våben. Ved arbejdstids ophør skal der ligeledes være to personer med autoriseret adgang til våbenværkstedet til stede, når opbevaringsrummene for funktionsduelige våben aflåses.

6.2.3.3. Depoter.

Der skal være to personer med autoriseret adgang til stede i forbindelse med ind- og udlevering af funktionsduelige våben fra depot.

Med depot menes der i denne sammenhæng våbendepoter ved Forsvarsministeriets Materiel- og Indkøbsstyrelse (Forsvarets Forsyning, Depot og Distribution, Lager Danmark).

6.2.3.4. Undtagelser.

Undtaget for to-faktoradgang er enheder og enkeltpersoner, der er indsatte eller udfører beordret vagttjeneste.

Chefen for hjemmeværnet kan dispensere for alternative sikkerheds-løsninger

6.3. Håndvåbenammunition.

Håndvåbenammunition skal - såfremt ammunition ikke er under direkte fysisk kontrol - generelt opbevares og sikres i Sikret område, kategori 2, sikringsniveau 40.

6.3.1. Håndvåbenammunition opbevaret ved enheden (UAFD/AFD).

Håndvåbenammunition opbevares i:

- ammunitionsmagasin (større mængde)

- ammunitionsskab og -boks (mindre mængde).

Ammunitionsskab og -boks anvendes til opbevaring af ammunition, der skal være klar til hurtig udlevering, fx vagtammunition og beredskabsammunition.

Opbevaringsmidler opstilles i enhedens våbenopbevaringsrum, og opbevaringsmidler skal som minimum svare til opbevaringsmiddel, klasse A.

Våbenopbevaringsrummet etableres i Sikret område, kategori 2, sikringsniveau 40. Der etableres normalt ikke adgangskontrolanlæg med sluse til våbenopbevaringsrum.

6.3.2. Håndvåbenammunition oplagt ved myndigheden (NIV III/II).

6.3.2.1. Inden for et etablissemments perimeterhegn, kategori 1-3, (Egentlig bevogtning).

Håndvåbenammunition oplægges i ammunitionsmagasin under anvendelse af sikringsniveau 40.

6.3.2.2. Uden for et etablissemments perimeterhegn, kategori 4,

Håndvåbenammunition opbevares i ammunitionsmagasin samt lokaliteter, der er godkendt som opbevaringssteder for hjemmeværnets ammunition.

Magasin samt opbevaringslokaliteter skal som minimum sikres som Overvåget område, kategori 4, sikringsniveau 40.

6.4. Eksplosivstoffer.

Eksplosivstoffer, herunder håndgranater og miner med sampakkede detonatorer skal som minimum opbevares i ammunitionsmagasin, ekskl. Type 1, i Overvåget område, kategori 4, sikringsniveau 40.

Eksplosivstoffer, herunder håndgranater og miner, uden sampakkede detonatorer skal som minimum opbevares i ammunitionsmagasin ekskl. Type 1 i Overvåget område, kategori 4, sikringsniveau 30.

6.5. Våben og våbensystemer med særlig sikkerhedsrisiko.

Våben og våbensystemer med særlig sikkerhedsrisiko skal opbevares og sikres i Sikret område, kategori 1, sikringsniveau 50-60.

For visse våbensystemer er der kontraktligt aftalt særlige sikkerhedsmæssige foranstaltninger.

6.6. Vitalt og/eller sensitivt materiel.

Sikringskrav for opbevaring/oplægning af vitalt og/eller sensitivt materiel fremgår af bilag 1 med underbilag.

7. OPBEVARING AF UDLÅNT VÅBEN OG AMMUNITION PÅ TJENESTESTED

Myndigheden kan tillade, at et enkelt våben opbevares tillige med tilhørende beredskabsammunition på våbenkammer eller kontor, hvis det befinder sig i sikret område, minimum områdekategori 2 sikringsniveau 40 i et klasse A opbevaringsmiddel.

Bestemmelserne herfor fremgår af bilag 2.

8. OPBEVARING AF MILITÆRE- OG CIVILE SKYTTEFORENINGERS VÅBEN

Myndigheden kan give militære skytteforeninger og i visse tilfælde civile skytteforeninger tilladelse til opbevaring af håndvåben på militære etablissementer inden for perimeterhegn.

Myndigheden udgiver bestemmelser for opbevaring af våbnene, og disse bestemmelser skal tiltrædes skriftligt af skytteforeningen.

Våbnene skal opbevares fysisk separeret fra forsvarets våben, men kan opbevares i samme fysisk sikrede lokaliteter.

Våbnene opbevares således:

- Våben oplægges med vital våbendel udtaget
- Vital våbendel oplægges adskilt fra våben
- Våben oplægges i våbenopbevaringsrum, depot eller magasin. Opbevaringsforholdene skal opfylde minimumskrav iht. sikringsniveau 40, og vitale våbendele skal opbevares i opbevaringsmiddel, minimum klasse A.

Myndigheden har til enhver tid ansvaret for, at opbevaringsbestemmelserne overholdes. Våbnene skal mønstres årligt og der skal udfærdiges mønstringsrapport der skal forlægges den for området ansvarlige chef til godkendelse.

9. ØVRIGT MATERIEL

Øvrigt materiel herunder tunge våben opbevares under foranstaltninger, der hæmmer/hindrer tyveri. Materiellet kan opbevares i Kontrolleret område, kategori 3, sikringsniveau 10/20/30/40, eller i Overvåget område, kategori 4, sikringsniveau 10/20/30/40 efter gennemført risikovurdering. Ved behov for beskyttelse i højere sikringsniveauer skal FE inddrages med henblik på at opnå en ressource-og hensigtsmæssig løsning.

10. PRODUKTION

Ved planlægning og udførelse af produktion af militært materiel, skal styringsorganer mfl. - eventuelt den udpegede sikkerhedsofficer - løbende sikre sig, at de i gældende bestemmelser foreskrevne sikringsmæssige foranstaltninger gennemføres under projektets enkelte faser. Det skal herunder sikres, at udarbejdelse og ajourføring af detaljeret klassifikationsvejledning omfatter samtlige materielgenstande i det omhandlede projekt.

Den sikkerhedsmæssige beskrivelse i forbindelse med projektering og installering af klassificeret materiel skal omfatte fornødne beskyttelsesforanstaltninger gældende for såvel militære myndigheder som civile firmaer. Eftersyn og reparation af klassificeret materiel må kun udføres af de militære og civile værksteder, som er sikkerhedsgodkendt til den omhandlede klassifikationsgrad.

Civile firmaer/værksteder er endvidere omfattet af kapitel 8, Industrisikkerhed.

11. EMBALLERING OG FORSENDELSE/TRANSPORT

Ved forsendelse/transport af materiel, klassificeret FTR eller højere samt vitalt og/eller sensitivt materiel, skal afsendende myndighed sikre sig, at modtagende myndighed er autoriseret til at modtage forsendelsen. Afsendende myndighed er desuden ansvarlig for udarbejdelse af de til forsendelsen nødvendige kontroldokumenter.

Bestemmelser for emballering og forsendelse/transport fremgår af bilag 3.

12. MATERIELSIKKERHED UNDER OPERATIVE FORHOLD MV.

Myndigheds/enhedschefer er ansvarlige for, at klassificeret eller vitalt og/eller sensitivt materiel til enhver tid er under direkte fysisk kontrol eller sikret efter minimumskravene i nærværende kapitel.

I fm. med gennemførelse af internationale operationer kan chefen, hvor det vurderes nødvendigt af operative grunde, fravige de fastsatte minimumskrav til materielsikkerheden. Fravigelse skal baseres på en konkret vurdering af alle risikofaktorer. I sådanne tilfælde skal foresatte myndighed underrettes.

13. MØNSTRING

Ved mønstring af materiel forstås, at materiellets tilstedeværelse er konstateret, eller at kvittering for aflevering/udlån foreligger. Materiel, der er klassificeret HEM/NS og højere, skal mønstres én gang årligt, efter endt anvendelse samt før og efter forsendelse/transport.

Materiel, der er klassificeret FTR/NC og lavere, mønstres ikke i sikkerhedsmæssig henseende.

Mønstring i sikkerhedsmæssig henseende medfører ikke ændringer i FMI-foranstaltninger til beholdningskontrol.

Alle våbentyper, vitalt og/eller sensitivt materiel og eksplosivstoffer skal mønstres årligt. Der skal udarbejdes mønstringsrapport der skal godkendes af den ansvarlige chef. Mønstringsrapporten skal opbevares i mindst 5 år. Mønstringsrapporten kan godt være elektronisk.

14. KOMPROMITTERING, BORTKOMST ELLER BESKADIGELSE

I tilfælde af kompromittering, bortkomst eller beskadigelse af klassificeret eller vitalt og/eller sensitivt materiel iværksætter enheden/myndigheden de fornødne undersøgelser - eventuelt med støtte af auditor og/eller politi - herunder foranstaltninger til imødegåelse af skadevirkning.

15. RAPPORTERING

Såfremt klassificeret materiel og vitalt og/eller sensitivt materiel bortkommer eller formodes kompromitteret, skal der straks indberettes herom til FE (se kapitel 10).

Ved bortkomst af våben, våbendele, ammunition og eksplosivstoffer rapporteres der digitalt under anvendelse af FMI-database (se kapitel 10, pkt. 5.2).

Hvis det bortkomne atter kommer til veje, orienteres de myndigheder, som har fået anmeldelse om bortkomsten. Endvidere foretages aflysning af iværksat efterlysning ved politiet.

OMFANG AF VÅBEN, AMMUNITION OG VITALT OG/ELLER SENSITIVT MATERIEL DER KRÆVER SÆRLIG SIKKERHEDSBESKYTTELSE

Underbilag:

Uddrag af opbevaringskrav for vitalt og/eller sensitivt materiel, våben og ammunition mv.

1. VITALT OG/ELLER SENSITIVT MATERIEL

1.1. Materiel.

Til kategorien vitalt og/eller sensitivt materiel **kan** henføres materiel, der er af vital operativ betydning.

Endvidere kan efternævnte materiel henføres:

- sigteoptik
- mørkekampudstyr, herunder håndholdt materiel
- laserudstyr
- pyroteknisk materiel
- radiostationer, mandbårne
- kommunikationsudstyr
- vanedannende medicin, herunder morfinpræparater, medicinsk sprit og formalin.

Andre materielbeholdninger og forsyningsgenstande, fx køretøjer, uniformer og udrustning, henføres til samme kategori afhængig af en aktuel risikovurdering.

1.2. Våben, våbensystemer, ammunition og eksplosivstoffer.

Til kategorien vitalt og/eller sensitivt materiel **skal** henføres:

- håndvåben
- håndvåbenammunition
- eksplosivstoffer
- panserværnsvåben, mandbårne
- luftværnsmissiler, mandbårne.

2. HÅNDVÅBEN

Håndvåben, der ud fra en sikkerhedsmæssig vurdering er individregistreret, omfatter:

- Pistol
- Maskinpistol
- Gevær/riffel (inkl. 12.7 mm riffel)
- Maskingevær
- Instruktionsvåben.

3. VITALE VÅBENDELE

VÅBEN	Pibe	Tromle/ kammerstykke	Bundstykke/ lås
Pistol M/49	X		
Pistol, øvrige	X		X
Revolver		X	
Maskinpistol			X
Gevær/riffel			X
Maskingevær			X
Tungt maskingevær M/50			X ¹
Instruktionsvåben/gevær			X
Særlige våben	Udpeges af materielanskaffende myndighed		

4. SIKRINGSNIVEAU FOR OPBEVARING/OPLÆGNING AF VÅBEN, AMMUNITION OG EKSPLOSIVSTOFFER SAMT VITALT OG/ELLER SENSITIVT MATERIEL

Efterfølgende sikringskrav er minimumskrav for opbevaring/oplægning af våben, ammunition og eksplosivstoffer.

4.1. Inden for et etablissemments perimeterhegn, kategori 1-3, (Egentlig bevogtning).**4.1.1. SIKRINGSNIVEAU 60.**

Våben/våbensystemer, hvor der kontraktligt er aftalt særlige sikkerhedsmæssige foranstaltninger. F. eks. STINGER, Luftværnsmissil m/93.

4.1.2. SIKRINGSNIVEAU 50.

- Våben/våbensystemer, med særlig sikkerhedsrisiko
- Håndvåben i funktionsduelig stand efter FE godkendelse
- Panserværnsvåben
- FLV Nærsikringsvåben M/92.

4.1.3. SIKRINGSNIVEAU 40.

- Håndvåben generelt
- 12,7 mm riffel
- Håndvåbenammunition
- 84 mm, Dysekanon
- 40 mm, Granatkaster

¹ På 12,7 mm TMG, M/50 er bagpladen vital våbendel og skal opbevares som en vital våbendel i et klasse A skab.

- 37 mm, Gasgevær
- 10 mm, Pistol
- Eksplosivstoffer, herunder håndgranater og miner, med sampakkede detonatorer
- Detonatorer
- Mørkekampmateriel, håndholdt
- Større mængder/opmagasinering af vanedannende medicin, herunder medicinsk sprit og formalin, opbevaret i klasse B opbevaringsmiddel eller tilsvarende.

4.1.4. SIKRINGSNIVEAU 30.

- Håndvåben med vital del udtaget, hvor de samlede sikringsløsninger – mekanisk sikring, elektronisk overvågning og bevogtning – vurderes tilstrækkelige. Såvel våben uden vitale dele som de vitale dele opbevares i hver sit klasse A opbevaringsmiddel
- Ammunition med sprængladninger til tunge våben
- Eksplosivstoffer, herunder håndgranater og miner, uden sampakkede detonatorer
- Øvrige tændmidler som tændere, sprængsnor, tændsnor, m.v.

4.1.5. SIKRINGSNIVEAU 10/20.

- Funktionsudrustning udleveret til personel
- Tunge våben som f.eks. 155 mm haubitser
- Ammunition uden sprængladninger til tunge våben.

4.2. Uden for et etablissemments perimeterhegn, kategori 4, (Bevogtningsmæssigt tilsyn).

4.2.1. SIKRINGSNIVEAU 40.

4.2.1.1. I depot eller magasin der er godkendt jf. kap. 7.

- Håndvåben med vital våbendel udtaget (depoter/magasiner der er godkendt til formålet af FE)
- Vital våbendel i klasse A opbevaringsmiddel
- Håndvåbenammunition
- Detonatorer
- Ammunition med sprængladninger til tunge våben
- Eksplosivstoffer, herunder håndgranater og miner, med sampakkede detonatorer.

4.2.2. SIKRINGSNIVEAU 30.

4.2.2.1. I ammunitionsmagasin ekskl. type 1.

- Ammunition uden sprængladninger til tunge våben
- Drivladninger til tunge våben
- Eksplosivstoffer, herunder håndgranater og miner, uden sampakkede detonatorer
- Øvrige tændmidler som tændere, sprængsnor, tændsnor mv.

4.2.3. SIKRINGSNIVEAU 10 / 20.

- Tunge våben.

Oversigt med uddrag over minimumskrav (sikringsniveau) fremgår af underbilag 1.

**UDDRAG AF OPBEVARINGSKRAV FOR VITALT OG/ELLER SENSITIVT MATERIEL,
VÅBEN, AMMUNITION OG EKSPLOSIVSTOFFER
OMRÅDEINDELING/SIKRINGSNIVEAU**

Tal i kolonne ref. henviser til pkt. i bilag 1.

			Sikringsniveau					Våben/ammunition/eksplosivstoffer	REF. BILAG 1 KAP 3
			10 20	30	40	50	60		
Områdeinddeling	1	Sikret					X	Særlig sikkerhedsrisiko	4.1.2
						X		Panserværnsvåben, M/95, M/97, m.v.	4.1.2
						X		Håndvåben (funktionsduelig, FE skal godkende)	4.1.2
			(X	X			Håndvåben generelt	4.1.3	
				X			Mørkekamp mat., håndholdt	4.1.3	
			(X	X			Vital våbendel	4.1.3	
				X			Håndvåbenammunition	4.1.3	
				X			84 mm. Dysekanon	4.1.3	
				X			40 mm. Granatkaster	4.1.3	
				X			Øvrige tændmidler herunder spræng- og tændsnor	4.1.4	
	3	Kontrolleret							
			X					Ammunition uden sprængladning til tunge våben	4.1.5
	4	Overvåget			X			Håndvåben uden vital våbendel	4.2.1.1
					X			Vital våbendel (i klasse A opbevaringsmiddel)	4.2.1.1
					X			Håndvåbenammunition	4.2.1.1
					X			Ekspllosivstoffer m.v. med sampakkede detonatorer	4.2.1.1
				X				Ekspllosivstoffer m.v. uden sampakkede detonatorer	4.2.2.1
					X			Detonatorer	4.2.1.1
			X					Tunge våben	4.2.3
					X			Ammunition med sprængladning til tunge våben	4.2.1.1
				X				Ammunition uden sprængladning til tunge våben	4.2.2.1
				X				Drivladninger til tunge våben	4.2.2.1
				X				Øvrige tændmidler herunder spræng- og tændsnor	4.2.2.1

Ovennævnte genstande er anført under anvendelse af laveste sikringsniveau og kan skærpes hvor det sikkerhedsmæssigt skønnes nødvendig efter gennemført risikovurdering

Beskrivelse af sikringsniveau fremgår af bilag 1 til kapitel 7.

(X): Sikringsniveauet kan anvendes når de samlede sikringsløsninger vurderes tilstrækkelige. Der er normalt kun tale om et enkelt våben.

SIKKERHEDSBESTEMMELSER VEDRØRENDE OPBEVARING AF UDLÅNT VÅBEN OG AMMUNITION

1. OMFANG

Bestemmelsen er gældende for personel i forsvaret, der får våben og evt. tilhørende ammunition i udlån, iht. myndighedens bestemmelse, herunder bruttolandsskytter, der får våben udlånt til brug ved træning og deltagelse i konkurrencer.

For hjemmeværnet gælder endvidere supplerende bestemmelser fastsat af Chefen for Hjemmeværnet.

2. OPBEVARING PÅ PRIVAT BOPÆL

Bruttolandsskytter kan, såfremt der er tvingende grunde, søge om tilladelse til at opbevare våben og ammunition på bopælen.

Udlånte våben og ammunition skal opbevares i et af forsvaret godkendt og udleveret våbenskab og efter nedenstående retningslinjer:

- Vital del skal altid udtages og anbringes i et aflåst gemme
- Ammunition skal opbevares for sig i et andet aflåst gemme.

Nøgler til de aflåste gemmer skal opbevares utilgængeligt for uvedkommende.

Når boligen forlades, skal døre, der giver adgang til boligen, være låst, og vinduer skal være lukkede og tilhaspet.

Våben og ammunition må ikke efterlades i boligen, såfremt ovenstående regler ikke kan efterleves; men skal i så fald enten opbevares på tjenestestedet ved låntagers foranstaltning eller udleverende myndigheds foranstaltning.

3. OPBEVARING PÅ TJENESTESTED

Udlånt våben og ammunition, skal opbevares på tjenestestedet, og skal opbevares efter bestemmelserne i kapitel 3.

Opbevaring skal ske i våbenopbevaringsrum e. lign efter aftale med tjenestestedets sikkerhedsofficer.

4. OPBEVARING UDEN FOR TJENESTESTED

I forbindelse med konkurrenceskydninger i forsvaret, skal våben og ammunition, når disse ikke anvendes, opbevares efter bestemmelserne i kapitel 3, ved arrangørernes foranstaltning.

Skal våben og ammunitionen undtagelsesvis opbevares uden for militært etablissement f.eks. i en skydeklub, skal dette aftales med SIKOF og være i overensstemmelse med de civile regler på området.

Våbnet skal dog altid opbevares med den vitale del udtaget.

5. TYVERI, BORTKOMST, TILVEJEKOMST

Såfremt våben, dele heraf og/eller ammunition bortkommer, skal der straks indberettes herom til FE og udleverende myndighed ved benyttelse af særlig rapportblanket (se kapitel 10).

Ved tyveri/bortkomst foretages følgende:

- Låntageren underretter sin myndighed/enhed, og anmeldelse til den lokale politimyndighed, såfremt våbnet har været opbevaret privat eller i civil skydeklub, foretages straks telefonisk.
- Myndigheden/enheden rapporterer snarest til FE pr. telefon eller FIIN.
- Myndigheden/enheden underretter - ved hændelser der vurderes at blive gjort til genstand for omtale i medierne – Forsvarskommandoen og Forsvarsministeriet herom. Hjemmeværnets tjenestesteder underretter Hjemmeværnskommandoen, Forsvarets Efterretningstjeneste og Forsvarsministeriet.
- Myndigheden/enheden indhenter ved den lokale politimyndighed journalnummer på anmeldelsen og rapporterer tyveriet/bortkomsten på rapportblanket, snarest efter at hændelsen er konstateret.

Hvis det bortkomne atter kommer til veje, orienteres de myndigheder, som har fået anmeldelse om bortkomsten, og aflysning af iværksat efterlysning ved politiet foretages, ved anvendelse af rapportblanket.

Skade som følge af brand eller anden ødelæggelse indberettes til udleverende myndighed med angivelse af de nærmere omstændigheder, samt om politianmeldelse er foretaget. Eventuelle rester af våbnet sendes til den udleverende myndighed tillige med rapportblanketten.

6. BEKENDTGØRELSE

Bruttolandsholdsskytter der får udleveret våben og ammunition, skal af den udleverende myndighed gøres bekendt med ovenstående ved udlevering af:

- Kopi af nærværende bilag (sikkerhed)
- Et eksemplar af rapportblanket (rapportering, se kapitel 10).

Øvrige retningslinjer for udlån efter udleverende myndigheds bestemmelse (forvaltning).

SIKKERHEDSBESTEMMELSER VED EMBALLERING OG FORSENDELSE/TRANSPORT AF KLASIFICERET- SAMT VITALT OG/ELLER SENSITIVT MATERIEL

Underbilag:

Lufttransport af klassificeret materiale til/fra USA.

1. FORMÅL

At fastlægge sikkerhedsbestemmelser for emballering og forsendelse/transport af klassificeret -, samt vitalt og/eller sensitivt materiel.

2. UDFØRELSE

Disse sikkerhedsbestemmelser danner grundlag for myndighedernes forsendelse/transport af klassificeret materiel og vitalt og/eller sensitivt materiel, herunder materieltransporter arrangeret af Forsvarsministeriets Materiel- og Indkøbsstyrelse under anvendelse af militær kurértjeneste, militær transport eller civil transport.

Ved forsendelse med civile transportfirmaer/agenturer skal disse forinden være sikkerhedsgodkendt. Oplysning herom kan indhentes hos FE.

Ved forsendelse til/fra udlandet skal planlægningen gennemføres således, at klassificeret materiel ikke passerer lande, der vurderes at udgøre en sikkerhedsmæssig risiko.

3. EMBALLERING

Ved emballering af klassificeret materiel samt materiel med særlig sikkerhedsrisiko, der kan rummes i autoriserede kuverter eller tilsvarende emballering, herunder pakker, gælder de sikkerhedsmæssige forhold, som er anført i Kapitel 4, Dokumentsikkerhed.

Materiel, der er klassificeret TTJ, pakkes i en efter forholdene forsvarlig emballering, der kan modstå normalt forekommende påvirkninger under forsendelse.

Ved emballering af materiel, der er klassificeret FTR og højere, som ikke kan rummes i autoriserede kuverter eller tilsvarende emballage, skal det omhandlede materiel pakkes i en indre og en ydre emballage, hvor:

- Den indre emballage klassifikationsmærkes og forsegles med sikkerhedstape eller med en af afsenderen kontrolleret plombering.
- Den ydre emballage skal være af solidt materiale, (metal-/træemballage), der enten sikres ved aflåsning med sikkerhedsgodkendt lås, engangslås, eller med solidt fastgjort stålspændebånd.
Den ydre emballage skal være af en sådan beskaffenhed, at uvedkommende ikke kan få indsigt i den indre emballage. Den ydre emballage må ikke klassifikationsmærkes. Aflåst container, aflåst lastrum eller aflåst jernbanevogn kan erstatte den ydre emballage.

Hvor en klassificeret komponent er indbygget eller monteret i en materielgenstand, kan denne materielgenstand opfattes som den indre emballage under forudsætning af, at den klassificerede komponent ikke er synlig eller direkte tilgængelig for uvedkommende.

4. FORSENDELSE

Forsendelse af klassificeret materiel, samt vitalt og/eller sensitivt materiel skal fortrinsvis finde sted med militære transportmidler.

Ved forsendelse af materiel klassificeret FTR og højere skal afsendende myndighed sikre sig, at modtagende myndighed er autoriseret til at modtage forsendelsen.

Når den militære kurértjeneste ikke anvendes ved forsendelse af materiel, der er klassificeret FTR og højere, er afsendende myndighed ansvarlig for, at modtagende myndighed ved klassificeret signal informeres om:

- forsendelsens art mv.
- afsendelsestidspunkt og -sted
- transportmåde og -rute
- kolliantal og -mærkning
- klassifikationsgrad
- data for sikkerhedsvagt(er)
- forventet ankomsttid.

Modtagende myndighed er ansvarlig for, at afsendende myndighed orienteres om afleveringssted og navn med data på personel, der er autoriseret til at modtage materiellet.

Forsendelse finder sted således:

FORSENDELSE INDLAND (excl. FÆRØERNE OG GRØNLAND)		
TTJ	FTR	HEM
Pakkepost	Pakkepost, rekommanderet	Militær kurér
Civil transport	Militær transport	Militær transport
Militær transport	Civil transport	(Konstant overvågning)
FORSENDELSE UDLAND (inkl. FÆRØERNE OG GRØNLAND)		
TTJ	FTR	HEM
Pakkepost	Militær kurér	Militær kurér
(Aftale med modtager)	Militær transport	Militær transport
Civil transport	Civil transport	Civil transport
Militær transport		(Konstant overvågning)

Udover udarbejdelse af fornødne kontroldokumenter er afsendende myndighed desuden ansvarlig for, at der træffes foranstaltninger til, at toldbehandling mv. under forsendelsen ikke medfører kompromittering af det omhandlede materiel. Ligeledes skal det sikres, at materiellet ikke henligger på forsendelsesetablissementer (banegårde, havne, lufthavne, grænsestationer) uden iagttagelse af den sikkerhedsbeskyttelse, der er krævet for det omhandlede materiel.

Forsendelsesmåde eller -rute må ikke medføre, at tilsynsansvaret for materiel, der er klassificeret FTR/NC eller højere, overdrages til personer fra lande, der ikke er tilsluttet NATO.

4.1. Forsendelse med skib.

Ved forsendelse med skib må NATO-klassificeret materiel kun forsendes med skib, der er hjemmehørende i et NATO-land, og hvor såvel skibets ejer som dets fører er statsborger i et NATO-land.

Skibet må ikke besejle territorialfarvande henhørende under lande, der vurderes at udgøre en sikkerhedsrisiko, og skibet må kun anløbe havne i ikke NATO-lande efter samråd med FE i hvert enkelt tilfælde. Med mindre særlig aftale foreligger, er samme begrænsning gældende for nationalt klassificeret materiel.

4.2. Forsendelse med fly.

Ved forsendelse med fly må NATO-klassificeret materiel normalt kun forsendes med fly, der er indregistreret i et NATO-land, og hvor flyets fører er statsborger i et NATO-land. SAS-fly, hvor føreren er dansk eller norsk statsborger, kan dog anvendes - uanset flyets indregistreringsland. Medmindre særlig aftale foreligger, er samme begrænsning gældende for nationalt klassificeret materiel.

Ved forsendelse med fly skal direkte flyvning til bestemmelsesstedet foretrækkes. Planlagt mellemlanding i et ikke NATO-land må kun finde sted efter aftale med FE, og passage af luftrummet over lande, der vurderes at udgøre en sikkerhedsrisiko, bør ikke finde sted.

5. FORSENDELSE/TRANSPORT AF PERSONLIGT VÅBEN MED TILHØRENDE AMMUNITION

Personligt håndvåben og eventuelt udleveret ammunition bør følge personalet.

Ved landevejs-, jernbane- og søtransport skal personligt våben og ammunition være under konstant kontrol.

Ved lufttransport i forsvarets fly kan funktionsdueligt håndvåben med tilhørende ammunition medbringes over den strækning, hvor det er tjenstligt påkrævet.

Passagerer, der ønsker at medbringe private våben, skal fremvise fornøden våbentilladelse. Vital våbendel kan transporteres i luftfartøjets kabine, medens våbnet skal transporteres som indskrevet bagage i luftfartøjets lastrum eller et andet for passagerer utilgængeligt sted.

Ved lufttransport med civile danske luftfartøjer - såvel inden for som uden for dansk område - kan våben og ammunition transporteres i luftfartøjets kabine således:

- Funktionsdueligt tjenestevåben med tilhørende ammunition, der medbringes af militært personel over den strækning, hvor det er tjenstligt påkrævet.
- Våben, der af militært personel under kommando medtages under flyvning med luftfartøj, specielt chartret til befordring af militært personel, under forudsætning af, at våben ikke indeholder ammunition, og ammunition ikke transporteres i kabinen.
- Vital våbendel, hvor militært personel som enkeltrejsende skal medføre tjenestevåben til anvendelse på ankomststedet. Våbnet skal transporteres som indskrevet bagage i luftfartøjets lastrum.

Militære enheder/enkeltpersoner, der ønsker at medbringe eller forsende våben og ammunition med civile danske luftfartøjer som anført ovenfor, er pligtige til over for vedkommande luftfartsselskab at give alle oplysninger om det materiel, der ønskes medbragt eller forsendt.

For luftfartøjer, som af forsvaret chartres til transport af enheder og materiel, aftales bestemmelser for transport af våben og ammunition med charterselskabet direkte.

6. FORSENDELSE/TRANSPORT AF VÅBEN

Ved forsendelse med militær transport uden ledsagepersonel, med civil transport eller med offentlige transportmidler skal vital våbendel udtages af våbnet. Våben og vital våbendel skal forsendes i to af hinanden uafhængige forsendelser.

Afsender meddeler modtager om afsendelsestidspunkt og forventet modtagelsestidspunkt for forsendelsen af våben og våbendele.

Modtager underretter afsender, såfremt forsendelsen ikke er modtaget senest 48 timer efter forventet modtagelsestidspunkt.

Afsender iværksætter efterforskning af forsendelsen ved manglende modtagelse. Det må af forsendelsens ydre emballage ikke fremgå, at forsendelsen indeholder våben eller våbendele.

Forsendelse af våben og våbendele skal altid plomberes og sikres ved aflåsning med sikkerhedsgodkendt lås, engangslås eller stålspændebånd.

7. OVERVÅGNING, SIKRING OG BEVOGTNING AF SÆRLIGE TRANSPORTER

Ved transport af vitalt og/eller sensitivt materiel (våben, ammunition og eksplosivstoffer) skal den for transporten ansvarlige myndighed foretage en risikovurdering, der danner grundlag for omfang af overvågning, sikring og bevogtning af transporten.

Ved lufttransport kan de sikkerhedsmæssige overvejelser normalt begrænses til sikkerhedsforanstaltninger i lufthavne og på flyvestationer ved ind- og udladning, medens søtransport kræver sikkerhedsforanstaltninger i havneområder herunder foranstaltninger i tilslutning til laste- og lossefaciliteter. Ved landtransport ad landevej og jernbane skal sikkerhedsforanstaltningerne gennemføres ved hjælp af ledsagepersonel transporteret i ledsagekøretøj eller jernbanevogn.

Ved transport af vitalt og/eller sensitivt materiel, der på baggrund af en risikovurdering kræver egentlig bevogtning, skal ledsagepersonellet være militært personel. Ved øvrige transporter af vitalt og/eller sensitivt materiel kan ledsagepersonellet være militært eller civilt personel.

Ledsagepersonellet skal transporteres i køretøj, der ikke indgår som transportkøretøj, og være af et sådant antal og en sådan uddannelse samt være udrustet og eventuelt bevæbnet, således at den for transporten nødvendige overvågning, sikring og bevogtning kan etableres og opretholdes.

8. SÆRLIGE BESTEMMELSER

Ved forsendelse af materiel, hvor hensynet til materiellets art, karakter eller værdi kræver en sikkerhedsbeskyttelse, der ikke skyldes fastsat klassifikation, iværksættes denne efter omstændighederne i hvert enkelt tilfælde.

Ved forsendelse af kryptoudstyr og kryptonøglematerialer mv. henvises til kapitel 6 (se bilag 3 til afsnit II).

Ved forsendelse (jernbane-, blokvogns- eller skibstransport) af mobile enheder (køretøjer, containere mv.) uden ledsagepersonel skal materiel, der er klassificeret TTJ være låst inde i de mobile enheder. Materiel, der er klassificeret FTR eller højere samt vitalt og/eller sensitivt materiel, skal udtages af de mobile enheder og transporteres ved den militære styrkes foranstaltning.

9. TRANSPORT AF AMMUNITION OG EKSPLOSIVSTOFFER (FARLIGT GODS)

Ved forsendelse af ammunition og eksplosivstoffer henvises endvidere til sikkerhedsbestemmelser udarbejdet af FMI, [FMIBST 061-2](#), Bestemmelse for vejtransport af ammunition og eksplosivstoffer.

LUFTTRANSPORT AF KLASSIFICERET MATERIALE TIL/FRA USA**1. OMFANG**

Forsendelserne omfatter nationalt klassificeret materiale til og med HEM og udføres på følgende måder:

1.1. Forsendelse fra Danmark til USA.

- Afsender foranlediger klassificeret forsendelse afleveret til transportagenturet. Dette kan foregå enten ved aflevering med kurér til transportagenturet eller ved dettes afhentning af forsendelsen
- Transportagenturet opbevarer forsendelsen i et af FE godkendt opbevaringsmiddel indtil aflevering til SAS mod kvittering. Boksen forsegles af transportagenturet
- Transportagenturets medarbejder overvåger anbringelse af forsendelsen i sikkerhedsboks og ledsager SAS medarbejder under transport af sikkerhedsboks til flyet, samt overvåger anbringelse af boks i lastrum
- Transportagenturets medarbejder forbliver i lufthavnen, indtil flyet er lettet
- Transportagenturet underretter skriftligt kontoret i USA om, at transporten er afgået fra København
- Transportagenturets godkendte medarbejder i USA modtager på SAS-Terminalen den forseglede boks straks efter ankomst, hvor agenturet kvitterer for modtagelsen
- Transportagenturet afleverer forsendelsen til modtageren.

1.2. Forsendelse fra USA til Danmark.

- Afsender sender den klassificerede post som "Registered Mail" eller med godkendt transportselskab til transportagenturet
- Transportagenturet kvitterer for modtagelse af forsendelsen og opbevarer denne i et af Defence Investigative Service godkendt opbevaringsmiddel
- Transportagenturet arrangerer forsendelse med SAS ved først mulige afgang
- Forsendelsen bringes af transportagenturet til SAS, NEWARK AIRPORT
- Forsendelsen anbringes i sikkerhedsboks, som forsegles med plombe af transportagenturet
- Sikkerhedsboksen bringes ud til SAS flyet og anbringes i lastrum af SAS personale ca. en time før afgang
- Transportagenturets medarbejder forbliver i lufthavnen, indtil flyet er lettet
- Transportagenturet underretter skriftligt kontoret i København om, at transporten er afgået fra USA
- En af transportagenturets godkendte medarbejdere møder sammen med SAS personale flyet i Kastrup og overvåger udtagning samt transport af sikkerhedsboks til terminal, hvor agenturet kvitterer for modtagelsen.
Forseglingen må kun brydes af transportagenturet.
- Transportagenturet afleverer forsendelsen til modtageren.

KAPITEL 4

DOKUMENTSIKKERHED

1. INDLEDNING

Dokumentsikkerhed omfatter foranstaltninger, der skal beskytte alle former for informationsbærende materialer mod spionage, kompromittering og tab. Beskyttelsesforanstaltningerne omfatter en kombination af klassifikation og mærkning, krav til fysisk opbevaring og håndtering, forsendelse mv. Desuden gælder "need to know" princippet, hvilket betyder, at adgang til klassificeret materiale skal være tjenstlig begrundet.

Når der i det efterfølgende nævnes TTJ, FTR, HEM eller YHM menes tillige de tilsvarende NATO, EU og WEU klassifikationsgrader jf. kapitel 1.

I de tilfælde hvor NATO, EU eller WEU sikkerhedskrav til håndtering og opbevaring er højere eller markant anderledes end de tilsvarende nationale, vil det fremgå af teksten.

2. FORMÅL

Formålet med dette kapitel er at beskrive de minimumskrav og procedurer, der er gældende for opbevaring og håndtering af klassificerede informationsbærende materialer.

3. ANSVAR

Chefen (direktøren, lederen m.fl.) er ansvarlig for planlægning, udførelse og kontrol af dokumentsikkerheden inden for eget myndighedsområde.

Enhver, der er beskæftiget med informationsbærende materiale, er over for chefen ansvarlig for udførelse af nødvendige sikkerhedsmæssige foranstaltninger.

Ingen har alene i kraft af sin tjenestestilling, grad eller sikkerhedsgodkendelse adgang til YHM, HEM, FTR eller tilsvarende klassificerede eller mærkede dokumenter.

4. BEMYNDIGELSE

Ved institutioner og myndigheder skal der føres en fortegnelse over personel, der af chefen er bemyndiget til behandling af materiale, der er klassificeret YHM eller HEM. Bemyndigelsen gives på baggrund af den enkeltes sikkerhedsgodkendelse og tjenstlige behov.

Chefen kan, såfremt omstændighederne taler herfor, fastsætte en generel bemyndigelse til adgang til materiale, klassificeret HEM. Den generelle bemyndigelse skal i så fald fremgå af myndighedens sikkerhedsinstruks, som skal være autoriseret af chefen.

5. KLASSIFIKATION OG KLASSIFIKATIONSMÆRKNING

5.1 Klassifikation af informationsbærende materiale.

Klassifikation af informationsbærende materiale skal gennemføres i overensstemmelse med principperne i kapitel 1.

5.2 Retningslinjer for klassificering.

Ved klassifikation af informationsbærende materiale gælder følgende retningslinjer:

- Skriftlige udfærdigelser uanset form skal klassificeres efter deres indhold, se bilag 5 til kapitel 1

- Skriftlige udfærdigelser uanset form skal mærkes efter deres indhold, se bilag 6 til kapitel 1
- En følgeskrivelse klassificeres efter sit indhold og mindst lige så højt som dertil hørende klassificerede tillæg og bilag
- Uden tillæg og bilag kan en følgeskrivelse nedklassificeres
- Uddrag af et dokument klassificeres under hensyn til uddragets indhold
- Oversættelser, afskrifter og fotokopier - uanset form - klassificeres som det originale dokument, se endvidere pkt. 7.5
- Journaler o.l. klassificeres normalt TTJ. Såfremt den enkelte emnebeskrivelse eller den samlede informationsmængde omfatter højere klassificerede informationer, anvendes en tilsvarende højere klassifikation. Elektroniske journaler kan dog aldrig klassificeres højere end det pågældende it-system er godkendt til
- Mødereferater, arbejds papirer, notater mv. klassificeres under hensyn til det samlede indhold
- Dokumenter af større omfang klassificeres under hensyn til helheden. Enkelte afsnit og punkter kan om nødvendigt klassificeres lavere end det samlede dokument.

6. ÆNDRING AF KLASSEFIKATION

Alene udstedende myndighed kan ændre klassifikationen på informationsbærende materiale. Myndigheden er i så fald ansvarlig for, at alle modtagere underrettes.

Ved ændring af klassifikation overstreges den oprindelige klassifikationsgrad, og den nye påføres (evt. stemples) med anførelse af reference på samtlige eksemplarer. Endvidere rettes journal, mv. i overensstemmelse hermed. Hvis behov for sikkerhedsbeskyttelse af materialet bortfalder helt, skal det mærkes "AFKLASSIFICERET".

7. UDFÆRDIGELSE OG FREMSTILLING

Produktion af informationsbærende materiale omfatter udarbejdelse og fremstilling, herunder fastsættelse af klassifikation og fordeling.

Materialer, herunder koncepter, der danner grundlag for udarbejdelse og fremstilling, skal tilintetgøres eller opbevares og behandles i henhold til klassifikationen.

Såfremt sagsbehandlingen ikke umiddelbart afsluttes, skal materialet registreres.

7.1 YHM, HEM

Materiale, der er klassificeret YHM eller HEM, skal:

- klassifikationsmærkes, se bilag 6 til kapitel 1
- eksemplarnummereres
- forsynes med eksemplarfordeling af det samlede antal fremstillede eksemplarer
- indeholde angivelse af det totale sideantal
- sidenummereres
- forsynes på alle sider med entydig identifikation omfattende udsteder (i forkortet form), emne- og løbenummer samt dato, som f.eks. "FKO OPN 153.00-008 2006-02-23".

7.1.1 Liste over effektive sider.

Dokumenter mv. - herunder publikationer, klassificeret YHM eller HEM, der ajourføres ved udskiftning af blade, skal forsynes med "Liste over effektive sider".

7.2 FTR og TTJ

Materiale, der er klassificeret FTR eller TTJ, skal

- klassifikationsmærkes, se bilag 6 til kapitel 1
- sidenummereres.

7.3 Emneangivelse.

Emne på en skrivelse, må uanset skrivelserens indhold, ikke være klassificeret højere end TTJ. Om nødvendigt må emnet omskrives eller forkortes, så det ikke overstiger klassifikationen TTJ.

7.4 Reproduktion.

YHM klassificerede informationer må i almindelighed ikke fotokopieres eller anden måde reproduceres uden forud indhentet bemyndigelse fra udstederen. Hvis modtageren ikke uden væsentlig ulempe kan afvente udstederens bemyndigelse, og det anses for absolut påkrævet at gengive informationerne yderligere, må dette kun ske efter bemyndigelse fra myndighedens chef i hvert enkelt tilfælde.

Reproduktion, herunder uddrag, afskrifter, fotokopier, optryk, oversættelser og kopier printet fra elektroniske medier, der er klassificeret HEM eller højere skal:

- registreres i journal mv.
- forsynes med påskriften "UDDRAG", "AFSKRIFT", "KOPI", "OPTRYK" eller "OVERSÆTTELSE"
- forsynes med originalinformationens journal- og eksemplarnummer tillige med angivelse af udsteder
- eksemplarnummereres med anvendelse af selvstændig nummerrække og fordeling.

Den udstedende myndighed kan begrænse adgangen til reproduktion med følgende påskrift: "Uddrag/oversættelse/afskrift/fotokopi/optryk må ikke foretages uden udstederens tilladelse

Bestemmelser for reproduktion skal indgå i den lokale sikkerhedsinstruks.

7.5 Sagsbehandlingsmateriale.

Klassificeret sagsbehandlingsmateriale skal tilintetgøres dagligt uden udfærdigelse af tilintetgørelsesbevis og registrering eller registreres og opbevares i henhold til klassifikationen. Bestemmelser for håndtering af sagsbehandlingsmateriale skal indgå i den lokale sikkerhedsinstruks.

8. PAKNING OG EMBALLERING TIL FORSENDELSE/TRANSPORT

Klargøring af klassificeret materiale til forsendelse/transport omfatter kontroloptælling af materialet, pakning og emballering.

[Kvitterings blanket](#) klargøres og vedlægges nationalt eller NATO materiale, der er klassificeret HEM eller højere. For EU materiale vedlægges kvitterings blanket for materiale, der er klassificeret FTR eller højere.

Returnerede kvitteringer, som vedrører nationalt eller NATO materiale, opbevares indtil sagerne afleveres til Rigsarkivet eller nedklassificeres til FTR eller lavere. Returnerede kvitteringer som vedrører EU materiale opbevares indtil sagerne nedklassificeres til TTJ eller lavere.

Herefter kan kvitteringerne tilintetgøres.

Pakkes flere enkeltsager, der er klassificeret HEM eller højere, i samme emballage, skal afsenderen desuden udarbejde en følgeskrivelse over indholdet. Fortegnelsen vedlægges materialet, mens kopi af følgeskrivelsen forbliver hos afsenderen.

Afsender skal føre kontrol med at kvitteringer returneres fra modtager. Ved manglende kvittering rykkes senest efter en måned for indenlands forsendelser. For udenlands forsendelser rykkes senest efter to måneder.

8.1 YHM, HEM og FTR.

YHM, HEM og FTR klassificeret materiale skal under forsendelse eller transport forsynes med en indre og en ydre emballage.

8.1.1 Emballering.

8.1.1.1 Indre emballage.

Såfremt materialet kan rummes i kuverter, anvendes en kuvert som den indre emballage. Kuverten klæbes til, forsegles og påføres klassifikation, angivelse af modtager og afsendende myndigheds officielle stempel. Sikkerhedstape klæbes henover klæberande og stempel således, at indholdet ikke kan tages ud af den indre emballage uden at beskadige sikkerhedstapen, jf. bilag 1. Såfremt en myndighed ikke råder over autoriseret sikkerhedstape, men anvender et laksegl, skal man sikre sig, at lakseglet er tyndt og smeltet til over sammenlukningen af emballagen. Signetaftrykket skal være fuldt læsbart.

I stedet for en forseglet kuvert kan der anvendes en autoriseret og godkendt manipulationsikret konvolut (forseglingskonvolut), jf. bilag 1. Klassificeret materiale, der kun må ses og/eller behandles af en begrænset personkreds, forsynes på forsiden og den indre emballage med påtegningen:

"KUN FOR.(ONLY FOR).. eller " MÅ KUN ÅBNES AF.. (TO BE OPENED ONLY BY)....." med anførelse af grad, navn og myndighed. Er der tale om flere modtagere, anføres disse i prioritetsrækkefølge. Forseglingskonvoluttens unikke nummer skal fremgå af/være påført følgeskrivelsen.

Såfremt materialet ikke kan rummes i autoriserede kuverter/forseglingskonvolutter, anvendes en forsvarlig indre emballage, der klassifikationsmærkes og forsegles jf. bilag 1.

Den autoriserede sikkerhedstape, plomberbar taske og plomber beskyttes som materiale, der er klassificeret TTJ. Signeter til laksegl skal som minimum beskyttes som materiale klassificeret FTR. (NATO lak- og engangssegl skal beskyttes som materiale klassificeret NATO SECRET).

8.1.1.2 Ydre emballage.

Som ydre emballage anvendes en forsvarlig indpakning (kuvert eller andet). Den ydre emballage må ikke bære klassifikationsmærkning. Emballagen påføres adresseangivelse, afsender og et forsendelsesnummer for hver forsendelse. Den ydre emballage kan erstattes af transportkasse/indsats til mappe eller plomberet kurersæk eller plomberbar taske. I så fald skal den indre emballage forsynes med de forannævnte påtegninger. Plomberbare tasker og plomber skal rekvireres ved Forsvarets Låsetjeneste der fører individregnskab over udleverede tasker og udleverede plombe nummerserier. Rekvirenten er selv ansvarlig for den videre distribution.

8.1.2 Forsendelse med Forsvarets Kurørtjeneste eller særlig kurer.

Ved forsendelse med Forsvarets kurørtjeneste eller særlig kurør, forsynes den ydre emballage med påtegningen "KUN MED KURER"/"BY COURIER ONLY". Hvor den ydre emballage udelades, forsynes den indre emballage med denne påtegning.

8.2 TTJ

Materiale, der er klassificeret TTJ, skal pakkes i en efter forholdene forsvarlig emballering (kuverter eller anden emballering), der kan modstå normalt forekommende påvirkninger under forsendelse/transport.

9. INTERN FORSENDELSE/TRANSPORT

Intern forsendelse/transport af klassificeret materiale omfatter forsendelse/transport:

- i og mellem bygninger inden for en myndigheds lokalgeografiske område
- mellem en myndigheds lokale, men geografisk adskilte områder
- mellem forskellige myndigheder inden for samme lokalgeografiske område.

Intern forsendelse/transport af materiale, der er klassificeret FTR eller højere, må udføres af bemyndigede personer (kontorbetjente m.fl.), der skal være godkendt til samme klassifikation som det transporterede materiale. Det transporterede materiale skal være i forseglet emballage og/eller i aflåst transportkasse eller indsats til mappe, hvortil den person, som transporterer materialet, ikke har nøgle, eller i en plomberbar taske.

Desuden må intern forsendelse/transport af materiale, som er klassificeret FTR eller højere, udføres af personer, der er bemyndigede til at behandle materialet, idet materialet overdrages fra hånd til hånd uden mulighed for uvedkommendes indsigt.

Afsenderen er ansvarlig for kontrollen med den interne transport og udarbejdelse af eventuelt internt kvitteringssystem for klassificeret materiale. Under intern forsendelse/transport af materiale, der er klassificeret TTJ, skal der træffes foranstaltninger, så materialet ikke bliver tilgængeligt for uvedkommende.

10. EKSTERN FORSENDELSE/TRANSPORT

Ved ekstern forsendelse til ind- og udland af klassificeret materiale gælder:

- YHM og HEM klassificeret materiale må kun forsendes med kurér
- Til udlandet må FTR kun sendes med kurér. Inden for Danmark kan FTR klassificeret materiale sendes som rekommanderet post. Forsendelse som rekommanderet post til Grønland og Færøerne bør dog kun ske, såfremt det efter en konkret vurdering i det enkelte tilfælde skønnes forsvarligt
- TTJ og materiale der ikke er klassificeret, må sendes som almindelig post
- Materiale, der ikke er klassificeret må sendes via Internettet, idet der dog skal tages hensyn til evt. særlig mærkning, der fordrer beskyttelse.

Oversigter over beskyttelsesforanstaltninger ved forsendelse eller medbringelse af informationsbærende materiale fremgår af bilag 2 og bilag 3. Krav til transport og emballering af klassificeret materiel fremgår af kapitel 3.

Forsendelse kan tillige finde sted ved anvendelse af forsvarrets godkendte netværks- og kommunikationssystemer. Materialets klassifikation må ikke overskride den klassifikationsgrad, der er fastsat for det enkelte system.

11. MEDBRINGELSE UDEN FOR TJENESTESTEDET

Medbringelse af materiale klassificeret FTR og højere kræver:

- chefens bemyndigelse
- at [fortegnelse over medbragt materiale](#) er udarbejdet jf.

11.1 Medbringelse indenlands.

11.1.1 YHM og HEM.

Sådan medbringelse kræver:

- at materialet emballeres som anført i pkt. 8.1.1.1
- at materialet medbringes i en godkendt og aflåst transportkasse eller tilsvarende indsats i mappe eller i en plomberbar taske.

Materiale klassificeret YHM må **ikke** medbringes til privat bopæl.

11.1.2 FTR.

Sådan medbringelse kræver, at materialet emballeres (dobbeltkuverteres) som anført i pkt. 8.1.1.1. og 8.1.1.2. eller emballeres som anført i pkt. 8.1.1.1. og føres i en godkendt og aflåst transportkasse eller tilsvarende indsats i mappe eller i en plomberbar taske.

11.2 Medbringelse udenlands.

11.2.1 YHM

Materiale klassificeret YHM må **IKKE** medbringes til udlandet.

11.2.2 HEM og FTR

Sådan medbringelse kræver:

- at materialet føres i godkendt aflåst transportkasse eller tilsvarende indsats i mappe eller i en plomberbar taske
- at [Nato Courier Certificate](#) medbringes.

11.3 TTJ materiale i ind- og udland.

Materiale, der er klassificeret TTJ, kan umiddelbart medbringes.

11.4 Medbringelse til missionsområder, under øvelsesvirksomhed mv.

Ved medbringelse af klassificeret materiale til missionsområder eller deployering, togt og øvelse mv. i ind- og udland gælder de minimumskrav, der er beskrevet oven for. Der henvises i øvrigt til kapitel 5, Operationssikkerhed.

I fm. gennemførelse af internationale operationer, kan myndighedschefen fravige minimumskravene på baggrund af en konkret risikovurdering i hvert enkelt tilfælde.

11.5 Øvrige forhold der skal iagttages ved medbringelse

- Klassificeret materiale må kun medbringes af personer, der er sikkerhedsgodkendt og bemyndiget til behandling af det medbragte materiale
- Det klassificerede materiale må ikke fremtages på offentlige steder
- Materialet skal enten være i konstant personlig varetægt eller anbringes beskyttet, som foreskrevet i bilag 5.

Når materialet medbringes på tjenesterejse i NATO, eller EU lande, kan den rejsende normalt afvise toldeftersyn af materialet, såfremt dette er emballeret og forseglet, og den rejsende kan forevise behørigt udfyldt [Nato Courier Certificate](#). Hvis toldmyndigheden alligevel insisterer på at foretage eftersyn af materialet, skal den rejsende i første omgang foreslå, at materialet bliver gennemlyst. Hvis eftersynet er uafvendeligt skal den rejsende sørge for:

- at åbningen af materialet foretages af den rejsende selv
- at materialet åbnes et sted, hvor det ikke er synligt for uvedkommende

- at toldmyndigheden kun ser det absolut mest nødvendige af materialet
- at materialet efterfølgende bliver pakket og forseglet
- at toldmyndigheden afgiver kvittering for åbning af materialet
- at få oplyst data (navn mm.) på den person, som har forestået toldeftersynet.

Ved hjemkomst udfærdiges kompromitteringsrapport jf. kap. 10.

Forsendelse/medbringelse af informationsbærende materiale fremgår af bilag 2.

12. MODTAGELSE

12.1. Modtagelse af dokumenter klassificeret til og med YHM.

Myndigheder og institutioner, der modtager eller har ansvaret for videresendelse af materiale klassificeret FTR eller højere, skal udpege en eller flere personer, som bemyndiges til at modtage, kvittere for og åbne det tilsendte, klassificerede materiale. Bemyndigelsen skal fremgå af myndighedens sikkerhedsinstruks. Som minimum angives den/de bemyndigedes funktioner.

Ved modtagelse af emballerede, klassificerede forsendelser skal modtageren kontrollere, at emballagen er intakt. Hvis der er indikationer på, at forsendelsen har været forsøgt åbnet, rapporteres der straks til myndighedens sikkerhedsofficer, før proceduren fortsættes.

Ved åbning af HEM materiale kontrolleres, at materialet er komplet (kontrol af sider, tillæg, bilag, underbilag mv.) i henhold til den vedlagte kvittering, og at materialet er korrekt klassifikationsmærket. Kvitteringen underskrives og returneres straks til afsenderen.

12.2. Modtagelse af dokumenter mærket CTS eller ATOMAL.

For modtagelse og opbevaring af dokumenter mærket COSMIC TOP SECRET (CTS) og/eller ATOMAL gælder følgende retningslinjer:

Opbevaring af dokumenter mærket CTS og/eller ATOMAL må alene finde sted i Forsvarsministeriets (FMN) centralregistratur, eller et af FE godkendt underregistratur.

Udveksling af dokumenter mærket CTS og/eller ATOMAL, må alene ske gennem FMN centralregistratur. Såfremt et underregistratur eller anden myndighed modtager dokumenter mærket CTS og/eller ATOMAL uden om FMN centralregistratur, skal centralregistraturen straks underrettes.

12.3. Forholdsregler ved modtagelse af dokumenter mærket eller klassificeret højere end myndigheden kan håndterer.

Ved modtagelse af dokumenter der er mærket eller klassificeret højere end myndigheden kan håndtere, skal dette straks overdrages til SIKOF eller myndighedschefen for videre foranstaltning.

Såfremt dokumentet er mærket ATOMAL eller klassificeret CTS skal SIKOF eller myndighedschefen uopsætteligt kontakte FMN centralregistratur eller FE for vejledning.

13. REGISTRERING

Registrering af modtaget klassificeret materiale skal finde sted før materialet fordeles. Følgende oplysninger skal som minimum fremgå af journalen:

- udsteder, klassifikation, emnenummer, løbenummer og dato
- fuld angivelse af emne og dato for indførelse på postliste

- eksemplarnummer, tillæg og bilag
- modtagers eget registreringsnummer, herunder løbenummer, dato og evt. afvigende emnenummer
- rutning inden for egen myndighed.

Materiale, der modtages via et af forswarets godkendte netværk, registreres og behandles som øvrigt klassificeret materiale.

14. SAGSVANDRING OG FORDELING

14.1 Internt

Enhver intern sagsvandring mellem afdelinger, sektioner, sagsbehandlere mv. skal registreres ved myndigheden enten i journalen eller ved etablerede kontrolpunkter.

14.2 Uden for forsvaret

Myndigheder mfl. der i medfør af det tjenstlige behov omtaler eller overdrager klassificeret materiale til enkeltpersoner, erhvervssammenslutninger, private virksomheder o.l. uden for koncernen, skal sikre sig, at:

- modtageren er sikkerhedsgodkendt til den pågældende klassifikation
- sikkerhedsdeklaration iht. til kapitel 8 bilag 2 til afsnit II er udarbejdet, inden omtale eller overdragelse finder sted
- kun nødvendige dele af materialet omtales eller overdrages.

14.3 Internationale stabe

For videregivelse af informationer til udlændinge og dansk personel i internationale stabe m.fl. gælder:

- Til personel i NATO-stabe og – organer må videregives de informationer, der er en følge af det tjenstlige behov i NATO-sammenhæng, forudsat at modtageren er sikkerhedsgodkendt til det pågældende klassifikationsniveau.
- Til personel i andre internationale stabe må informationer, der er klassificeret højere end TTJ, kun videregives, når der foreligger et tjenstligt behov, og når modtageren er autoriseret til at modtage de omhandlede informationer.

14.4 Andre udenlandske myndigheder mv.

Til andre udenlandske myndigheder, institutioner, virksomheder mv. må der kun videregives informationer, som fremgår af alment tilgængelige kilder, med mindre der er tale om frigivet information.

Procedurer vedrørende frigivelse af klassificeret national information til ikke-NATO lande eller særlige internationale organisationer fremgår af bilag 4. Procedurer vedrørende frigivelse af klassificeret NATO/EU/WEU information fremgår af respektive organisationers sikkerhedsbestemmelser.

15. OPBEVARING

Klassificeret informationsbærende materiale skal opbevares i overensstemmelse med bilag 5 i sikkerhedsgodkendte opbevaringsmidler af militærklassificering A eller B og placeret i sikre områder og under sikringsniveauer, jf. kapitel 7.

Som sikkerhedsgodkendte opbevaringsmidler anses endvidere boksrums, arkivrum samt opbevaringsmidler, der er godkendt som anført i underbilag 5 til bilag 2 til kapitel 7.

16. MØNSTRING

16.1 Årlige mønstringer.

Informationsbærende materiale, der er klassificeret YHM og HEM, skal mønstres mindst én gang hvert kalenderår.

Materiale, der er klassificeret FTR og lavere, mønstres ikke i sikkerhedsmæssig henseende. Årlige mønstringer skal gennemføres som totalmønstringer, dvs. mønstring af den samlede beholdning ved myndigheden.

Mønstringer tilrettelægges og iværksættes af myndighedens sikkerhedsofficer, der skal føre kontrol med mønstringens omfang, mønstringsgrundlagets tilstrækkelighed, mønstringens gennemførelse og den efterfølgende mønstringsrapportering.

Når en person afgår fra myndigheden/enheden, skal det klassificerede materiale, den pågældende har udleveret, mønstres og afleveres.

16.2 Mønstring ved afgang

Når en leder af et sekretariat, arkiv eller tilsvarende afgår, skal der ved myndigheden eller myndighederne gennemføres en totalmønstring af YHM og HEM klassificeret materiale.

Sådanne mønstringer skal afsluttes inden fratrædelse. Når en person, med adgang til klassificeret materiale, afgår ved døden, forholdes som anført i kapitel 2.

16.3 Afslutning af mønstring

Klassificeret materiale anses for mønstret, når:

- den faktiske tilstedeværelse er konstateret ved optælling af sider, tillæg, bilag, underbilag mv. i overensstemmelse med skrivelse, følgeskrivelse, forside, adressat- eller fordelingsliste samt eventuel liste over effektive sider
- materiale, opbevaret i ubrudt forseglingskonvolut med en bemyndiget persons underskrift, er til stede
- kvittering fra eksternt myndighed foreligger
- bevis for tilintetgørelse foreligger eller
- bortkomstrapportering er iværksat i henhold til kapitel 10.

De uregelmæssigheder der konstateres under en mønstring, herunder bortkomster, skal fremgå af mønstringsrapporten.

Mønstringsrapporten skal forelægges myndighedens chef til underskrift og opbevares ved myndigheden i mindst 10 år.

17. SANERING

Sanering omfatter udtagelse og tilintetgørelse af ikke bevaringsværdige arkivalier i muligt omfang. Denne proces skal så vidt muligt gennemføres løbende, men kan med fordel ske i forbindelse med den årlige mønstring.

18. TILINTETGØRELSE

Klassificeret informationsbærende materiale kan tilintetgøres:

- ifølge påtegning på materialet
- efter udstedende myndigheds bestemmelser (skriftlig meddelelse)
- efter opbevarende myndigheds eller tjenestesteds bestemmelse.

18.1 Tilintetgørelse af YHM og HEM.

Tilintetgørelse af YHM og HEM skal udføres af to hertil bemyndigede, sikkerhedsgodkendte personer, der efter afsluttet tilintetgørelse skal underskrive et tilintetgørelsesbevis.

18.1.1 Tilintetgørelsesbevis.

Tilintetgørelsesbeviser nummereres fortløbende inden for kalenderåret og opbevares i mindst 10 år. Rettelsesmeddelelser kan i attesteret stand erstatte tilintetgørelsesbeviset. Ved tilintetgørelse af YHM og HEM klassificerede dokumenter følges nedenstående procedure.

- Tilintetgørelsesbevis skal udfærdiges, og den ikke anvendte nederste del af blanketten annulleres med en skråstreg. Dækkende beskrivelse skal anføres. Ved rettelser anføres numrene på udtagne sider, hvis rettelsesmeddelelse ikke anvendes som [tilintetgørelsesbevis](#)
Ved elektronisk udarbejdet tilintetgørelsesbevis skal dette foreligge i udskrevet form, hvor underskrift af de bemyndigede personer skal påføres
- Elektronisk udarbejdede tilintetgørelsesbeviser skal som minimum indeholde samme informationer som anført på tilintetgørelsesbevis for klassificeret materiale
- De to bemyndigede, sikkerhedsgodkendte personer skal sammen kontrollere materialet efter det forberedte tilintetgørelsesbevis, idet fuld kontrol af sider, tillæg, bilag, underbilag mv. gennemføres af begge
- Når tilintetgørelsen har fundet sted ajourføres journalen mv. ved påføring af tilintetgørelsesbevisnummer/år.
I elektroniske journaler angives tilintetgørelse samt tilintetgørelsesbevisnummer/år i de dertil indrettede felter
- Tilintetgørelse af øvelsessignaler finder normalt sted ved afslutningen af øvelsen. Ved tilintetgørelsen vil en signallog sammenhæftet med et tilintetgørelsesbevis med korrekt udfyldt hoved samt underskrifter være dækkende. Det forudsættes, at signalerne anført på loggen er fuldt identificerbare. Hvis øvelsessignaler gemmes ud over 30 dage skal disse registreres på normal vis.

Tilintetgørelsesproceduren skal gennemføres i én uafbrudt forretningsgang.

18.2 Tilintetgørelse af FTR.

Tilintetgørelse af FTR klassificeret materiale skal udføres af en hertil bemyndiget, sikkerhedsgodkendt person. Tilintetgørelsen skal registreres i journalen.

18.3 Tilintetgørelse af TTJ.

Tilintetgørelse af TTJ kan udføres af personer, der som minimum er godkendt til TTJ.

18.4 Tilintetgørelsesmåder.

Tilintetgørelse af klassificeret materiale gennemføres ved anvendelsen af makuleringsmaskiner eller under særlige omstændigheder ved brænding.

19. RETTELSE AF KLASIFICEREDE PUBLIKATIONER M.V.

Medarbejdere, der pålægges rettelsesarbejde og kontrol, skal være instrueret i fornødent omfang.

Rettelser i publikationer, der er klassificeret FTR eller højere, skal ske under iagttagelse af nedennævnte kontrolforanstaltninger.

19.1 HEM

For publikationer, klassificeret HEM, følges nedenstående procedure:

- rettelsesblade skal kontroltælles ved modtagelsen på baggrund af rettelsesmeddelelsens oversigt over nye blade
- rettelsens udførelse skal kontrolleres af en anden person end den, der udfører rettelsen
- udtagne blade skal kontrolleres efter rettelsesmeddelelsen
- rettelse og kontrol skal attesteres af begge involverede på publikationens rettelses- eller kontrolblad.

19.2 FTR.

For publikationer, klassificeret FTR, følges nedenstående procedure:

- rettelsesblade skal kontroltælles ved modtagelsen på baggrund af rettelsesmeddelelsens oversigt over nye blade
- udtagne blade skal kontrolleres efter rettelsesmeddelelsen
- rettelse og kontrol skal attesteres på publikationens rettelses- eller kontrolblad.

20. STØTTEVÆRKTØJ

Til brug for internationale operationer er der udarbejdet et støtteværktøj (kap 5 bilag 2), der kan hjælpe sikkerhedsofficeren ved hans vurdering af dokumentsikkerheden. Værktøjets del 5, fokuserer på de opgaver og funktioner, der er nødvendige for sikker behandling og opbevaring af klassificerede informationer.

EMBALERING OG FORSEGLING AF KLASSIFICEREDE SAMT VITALE- OG SENSITIVE MATERIALER OG DOKUMENTER

1. KUVERT

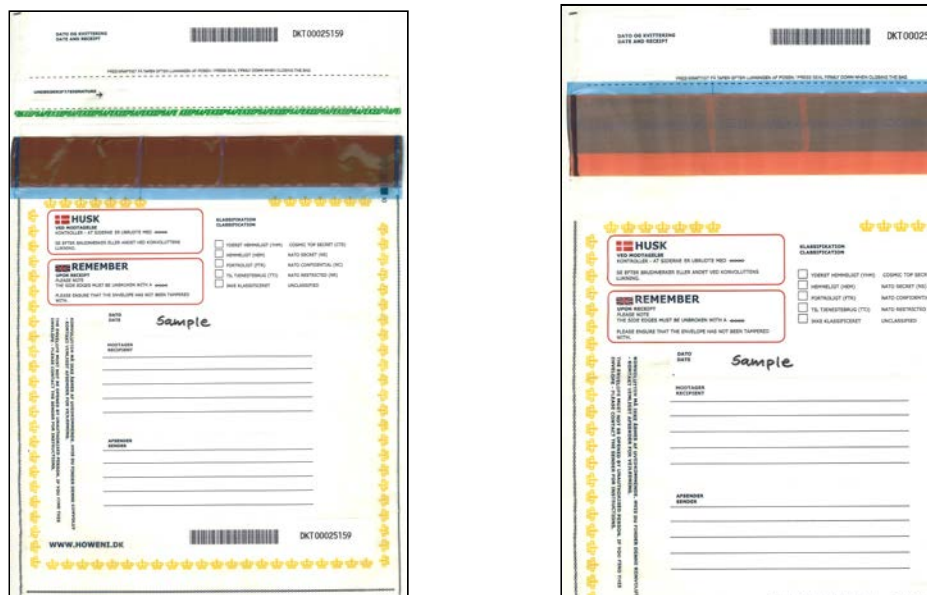


Figur 4. 4. 1

Eksempel på placering af sikkerhedstape og myndighedsstempel på inderkuvert

2. FORSEGLINGSKONVOLUT

Som alternativ til anvendelse af kuvert med sikkerhedstape kan der anvendes forseglingskonvolut. Konvolutten er af plast og findes i to typer hvoraf den ene er transparent. Konvolutterne rekvireres igennem SAP.



Figur 4. 4. 2

Eksempel på forseglingskonvolut før- og efter lukning

3. PAKKE



Figur 4. 4. 3

Eksempel på placering af sikkerhedstape sejl garn og myndighedsstempel på inderpakke

4. PLOMBERBAR TASKE



Figur 4. 4. 4

Billede af taskens forside.

Bemærk at det er politiet, der modtager henvendelser, hvis tasken afleveres som hittegods eller lignende.

De anvendte plomber er af et unikt design og skal altid undersøges for brud ved modtagelse af tasken. Tasken rekvireres igennem SAP.



Figur 4. 4. 5
Taskens syning

For at modvirke manipulation af tasken, er der anvendt en ind- og udvendig flerfarvet tråd. Trådens ubrudthed bør altid kontrolleres ved modtagelse af tasken. Tasken skal kasseres, hvis den ved almindelig slitage er blevet brudt eller beskadiget.

5. VARENUMRE

Plomberbar taske	8460-22-620-0795
Plomber for taske	5340-22-620-0793
Forseglingskonvolut, X-RAY	7530-22-620-8129
Forseglingskonvolut, transparent	7530-22-620-8131

FORSENDELSE / MEDBRINGELSE AF INFORMATIONSBÆRENDE NATIONALT OG NATO MATERIALE

INDLAND 						NATO-LAND, FÆRØERNE & GRØNLAND   						
NC-NS-CTS ATOMAL	YHM / CTS	HEM / NS	FTR / NC	TTJ / NR	NU		NU	TTJ / NR	FTR / NC	HEM / NS	YHM / CTS	NC-NS-CTS ATOMAL
FORSENDELSE												
				✓	✓	Kan sendes som almindelig postforsendelse.	✓	✓				
			✓			Kan sendes som rekommanderet postforsendelse.			✓ 1)			
			✓			Kan sendes som kurerforsendelse.						
✓	✓	✓				Skal sendes som kurerforsendelse.			✓	✓	✓	✓
✓	✓	✓				Kvitteringsformular vedlægges.				✓	✓	✓
		✓	✓	✓	✓	Efter indhentet tilladelse fra Forsvarets Efterretningstjeneste kan nationale klassificerede sager forsendes til adressater i lande, som ikke er tilknyttet NATO, og som ikke vurderes at udgøre en sikkerhedsrisiko, under overholdelse af kravene for forsendelse i Danmark.						
MEDBRINGELSE TIL PRIVAT BOPÆL												
				✓	✓	Kan umiddelbart medbringes.	For personel, der forretter tjeneste i NATO-stabe m.fl., gælder de for den pågældende stab m.fl. givne sikkerhedsbestemmelser.					
		v2)	v2)			Kan med chefens tilladelse medbringes til privat bopæl.						
✓	✓					Må under ingen omstændigheder medbringes til privat bopæl.						
MEDBRINGELSE PÅ TJENESTEREJSE												
				✓	✓	Kan umiddelbart medbringes.	✓	✓				
	✓	✓	✓			Kan medbringes under overholdelse af nedenstående regler for medbringelse.			✓	✓		
						YHM/CTS må ikke medbringes på tjenesterejse til udlandet.					✓	
✓						NC – NS – CTS mærket "ATOMAL" må under ingen omstændigheder medbringes på tjenesterejse.						✓
						Efter indhentet tilladelse fra Forsvarets Efterretningstjeneste kan nationale klassificerede sager medbringes på tjenesterejser til lande, som ikke er tilknyttet NATO, under overholdelse af regler for medbringelse.	✓	✓	✓	✓		
MEDBRINGELSE PÅ TJENESTEREJSE, NÅR FØLGENDE KRAV ER OPFYLDT												
	✓	✓	✓			– Fortegnelse (se bilag 5) over medbragte sager er udfærdiget.			✓	✓		
	✓	✓				– Sagerne skal medbringes i godkendt og aflåst transportkasse/mappe med indsats/plomberbar taske.			✓	✓		
			✓			– Sager kan medbringes dobbeltkuverteret /forseglingskonvolut eller i godkendt og aflåst transportkasse/mappe med indsats/plomberbar taske.						
	✓	✓	✓			– Sager skal være i konstant personlig varetægt.		✓	✓	✓		
	✓	✓	✓			– Sagerne skal, såfremt de ikke er i personlig varetægt, opbevares på et sikret område.			✓	✓		
						– NATO COURIER CERTIFICATE skal medbringes.			✓	✓		
	✓	✓	✓			– Den rejsende skal være sikkerhedsgodkendt til den klassifikationsgrad, der medbringes.		✓	✓	✓		
						– Den rejsende skal opgive rejserute og rejseplan.			✓	✓		
						– Rejsen må ikke medføre passage af et IKKE-NATO-LAND.			✓	✓		
						– Flyrejse må ikke medføre mellemlanding i lande, der vurderes at udgøre en sikkerhedsrisiko.			✓	✓		

- 1) Forsendelse til/fra Færøerne og Grønland af FTR/NC materiale kan, hvis omstændighederne nødvendiggør dette, finde sted som rekommanderet post.
- 2) Vedrørende transport og opbevaring - samme regler som for "Medbringelse på tjenesterejse".

**FORSENDELSE / MEDBRINGELSE AF INFORMATIONSBÆRENDE WEU¹ OG EU MATE-
RIALE**

INDLAND						EU LANDE				
TRÉS SECRET UE	SECRET UE	CONFIDENTIEL UE	RESTREINT UE	EU UNCLASSIFIED		EU UNCLASSIFIED	RESTREINT UE	CONFIDENTIEL UE	SECRET UE	TRÉS SECRET UE
FORSENDELSE										
			✓	✓	Kan sendes som almindelig postforsendelse.	✓	✓			
		✓			Kan sendes som rekommanderet postforsendelse.					
		✓			Kan sendes som kurerforsendelse.					
✓	✓				Skal sendes som kurerforsendelse.			✓	✓	✓
✓	✓	✓			Kvitteringsformular vedlægges.			✓	✓	✓
MEDBRINGELSE TIL PRIVAT BOPÆL										
	v2)	v2)	v2)	v2)	Kan med chefens tilladelse medbringes til privat bopæl.	For personel, der forreter tjeneste i EU/WEU-stabe m.fl., gælder de for den pågældende stab m.fl. givne sikkerhedsbestemmelser.				
✓					Må aldrig medbringes på privat bopæl.					
MEDBRINGELSE PÅ TJENESTEREJSE										
			✓	✓	Kan umiddelbart medbringes.	✓	✓			
MEDBRINGELSE PÅ TJENESTEREJSE, NÅR FØLGENDE KRAV ER OPFYLDT										
					– Må under ingen omstændigheder medbringes på tjenesterejse i udlandet.					✓
✓	✓	✓			– Fortegnelse (se bilag 5) over medbragte sager skal udfærdiges.			✓	✓	
✓	✓				– Sagerne skal medbringes i godkendt og aflåst transportkasse/mappe med indsats/plomberbar taske.			✓	✓	
		✓			– Sager kan medbringes dobbeltkuverteret /forseglings konvolut eller i godkendt og aflåst transportkasse/mappe med indsats/plomberbar taske.					
✓	✓	✓			– Sager skal være i konstant personlig varetægt.			✓	✓	
✓	✓	✓			– Sagerne skal, såfremt de ikke er i personlig varetægt, opbevares på et sikret område.			✓	✓	
					– WEU/EU COURIER CERTIFICATE skal medbringes.			✓	✓	
✓	✓	✓			– Den rejsende skal være sikkerhedsgodkendt til den klassifikationsgrad, der medbringes.			✓	✓	
					– Den rejsende skal opgive rejserute og rejseplan.			✓	✓	
					– Rejsen må ikke medføre passage af et IKKE-WEU/EU-LAND.			✓	✓	
					– Flyrejse må ikke medføre mellemlanding i lande, der vurderes at udgøre en sikkerhedsrisiko.			✓	✓	

- 1) WEU er alene nævnt, da der stadig kan cirkulere dokumenter med denne mærkning
- 2) Vedrørende transport og opbevaring - samme regler som for "Medbringelse på tjenesterejse".

PROCEDURE FOR FRIGIVELSE AF KLASIFICERET NATIONAL MILITÆR INFORMATION TIL IKKE-NATO LANDE OG SÆRLIGE INTERNATIONALE ORGANISATIONER

Underbilag:

1. Minimum Standards for the Protection of Classified Information released by Denmark.
2. Security Assurance governing the Release of Classified Information to NON-NATO Nations and Organisations which include NON-NATO Nations.

1. GENERELT

Klassificeret information er national ejendom og denne skal varetages og beskyttes i henhold til danske sikkerhedsbestemmelser. Klassificeret national information må kun frigives til ikke-NATO lande eller internationale organisationer, i hvis medlemskreds er ikke-NATO lande efter nærmere fastsatte frigivelseskriterier.

2. FRIGIVELSESKRITERER

Ansøgning om frigivelse af klassificeret information til og med HEMMELIGT behandles på baggrund af bilaterale aftaler med nationer eller internationale organisationer, omfattende øvelsessamarbejde, uddannelsesprogrammer, materielprojekter mv., når der foreligger et behov herfor (need-to-know) og hvor der ligger en fælles sikkerhedsaftale underskrevet af begge parter.

Ansøgning om frigivelse af klassificeret information til ikke-NATO lande og internationale organisationer, i hvis medlemskreds er ikke-NATO lande og som ikke har indgået en sikkerhedsaftale med Danmark behandles på baggrund af anmodning fra nationale militære myndigheder (sponsorerne). Sponsoren er ansvarlig for, at modtageren har bekræftet, at danske minimumskrav til sikkerhedsbeskyttelse vil blive opfyldt, og at en underskrevet sikkerhedserklæring foreligger, jf. underbilag 1 og 2.

3. FRIGIVENDE MYNDIGHED

Informationer klassificeret YDERST HEMMELIGT må **ikke** frigives.

Tilladelse til frigivelse af information klassificeret HEMMELIGT udøves af Forsvarets Efterretningstjeneste (FE).

Tilladelse til frigivelse af information klassificeret til og med FORTROLIGT udøves af NIV II eller højere myndigheder.

Det er den frigivende myndigheds ansvar, at den udvekslede information kun frigives efter indhentet udtalelse fra udstederen.

4. ANMODNING OM FRIGIVELSE

Anmodning om frigivelse skal indeholde følgende oplysninger:

- a) Formål og begrundelse (fælles projekt, andet samarbejde, øvelser etc.)
- b) Identifikation af dokument(er) indeholdende den klassificerede information (reference, dato og klassifikation)
- c) Beskrivelse af informationen, som skal frigives (hele dokumentet, dele af dokumentet eller uddrag af dokumentet)

- d) I fm. generisk frigivelse (dvs. specifikke emneområder, specifikke serier af dokumenter, fremtidige dokumenter eller serier af dokumenter etc.) oplyses højeste klassifikation.

5. ADMINISTRATION MED FRIGIVELSE

Frigivende myndighed iværksætter og styrer den autoriserede frigivelse af klassificeret national information. Frigivende myndighed fører detaljerede oversigter over såvel den frigivne information som modtagerne heraf.

Oversigter over frigivet information til og med FORTROLIGT indsendes en gang årligt til FE af den frigivende myndighed pr. 31. december. Oversigterne skal være FE i hænde senest 31. januar året efter.

MINIMUM STANDARDS FOR THE PROTECTION OF CLASSIFIED INFORMATION RELEASED BY DENMARK

1. UNCLASSIFIED

UNCLASSIFIED information will be handled as official information, but does not require any specific security protection. It may be transmitted through public postal and telecommunications systems. Documents may be reproduced as required by recipients.

2. RESTRICTED

RESTRICTED information will be handled and stored in areas where the public is denied access. Transmission of RESTRICTED documents may be achieved through public postal systems as registered mail. When no secure means of communications is available and speed of delivery is essential, RESTRICTED information may be transmitted by public telefax or telex. Documents may be reproduced as required by recipients.

3. CONFIDENTIAL

CONFIDENTIAL information will be handled and stored in areas to which access is controlled. Access to the information will be restricted to designated personnel who are security cleared and have the appropriate need-to-know for the subject matter.

CONFIDENTIAL documents will be stored in containers with good quality locks, the keys or combinations to which will be held by designated security personnel. Transmission of CONFIDENTIAL documents will be through diplomatic courier or military messenger services. For electrical transmission of CONFIDENTIAL information a cryptographic system authorised by the relevant national authority is required. Documents may be reproduced by an authorised official of the receiving organisation; records will show the number of copies reproduced and their disposition.

4. SECRET

SECRET information will be handled and stored in areas to which access is controlled and restricted to designated, security cleared personnel. Access to the information will be restricted to designated personnel who are security cleared and have the appropriate need-to-know for the subject matter. SECRET documents will be stored in containers with good quality locks, the keys or combinations to which will be held by designated security cleared personnel. Transmission of SECRET documents will be through diplomatic courier or military messenger system. For electrical transmission of SECRET information, a cryptographic system authorised by the relevant national authority is required. Documents may only be reproduced upon written authorisation by a designated control officer; records will show the number of copies reproduced and their disposition.

**SECURITY ASSURANCE GOVERNING THE RELEASE OF CLASSIFIED INFORMATION
TO NON-NATO NATIONS AND ORGANISATIONS WHICH INCLUDE NON-NATO NA-
TIONS**

Before classified information can be released to non-NATO nations or organisations which include non-NATO nations, the sponsor will establish a written agreement signed by the recipient that the latter undertakes to:

- (a) protect and safeguard the information and material of other Party;
- (b) ensure that classified information and material will maintain the security classifications established by any Party with respect to information and material originated by that Party and safeguard such information and material to agreed common standards based on the minimum standards contained in enclosed appendix.
- (c) not use the exchanged information and material for purposes other than those laid down in the framework of the respective programmes and the decisions and resolutions pertaining to these programmes;
- (d) not disclose such information and material to third parties without the consent of the originator;
- (e) have all persons of its nationality who, in the conduct of their official duties, require or may have access to classified information released, appropriately cleared before they are granted access to such information.

OPBEVARING AF INFORMATIONSBÆRENDE KLASSIFICERET MATERIALE

1. GENERELT

Generelt skal informationsbærende materiale klassificeret FTR og højere opbevares i sikrede områder, områdekategori 1 eller 2.

Under særlige omstændigheder, hvor dette ikke kan opfyldes, kan materialet opbevares i overvåget område, områdekategori 4. FE skal inddrages i det enkelte tilfælde m.h.p. at foretage en vurdering af de samlede risici og beskyttelsesforanstaltninger. Disse skal tilgodeses forholdet mellem den samlede anslåede gennembrydnings- og/eller oplukningstid jf. Forsikring & Pensions (F&P) klassificering i forhold til den forventelige reaktionstid fra vagtstyrke, vagtselskab og/eller politi. Dette forhold opnås ved en øget anvendelse af mekanisk sikring og elektronisk overvågning i forhold til de fastsatte sikringsniveauer jf. kapitel 7. Hjemmeværnskommandoen foretager vurderingen indenfor eget myndighedsområde. Se endvidere kapitel 7, bilag 2, underbilag 5, punkt 8, side 7.2.5.3.

2. YDERST HEMMELIGT

Materiale klassificeret YHM skal opbevares i godkendt og aflåst opbevaringsmiddel militær klassificering A, EN1143-1, GRADE 1, (eller sikringsskab, F&P BLÅ klasse hovedgruppe 2) med sikkerhedsgodkendt kombinationslås. Opbevaringsmidlet skal befinde sig inden for et sikret område, områdekategori 1, sikringsniveau 50.

Materiale klassificeret YHM må ikke opbevares på anden måde.

Opbevares materiale klassificeret YHM undtagelsesvis ved civile sikkerhedsgodkendte virksomheder, **skal** FE tilladelse forinden indhentes i det enkelte tilfælde.

3. HEMMELIGT

Materiale klassificeret HEM skal opbevares i godkendt og aflåst opbevaringsmiddel militær klassificering A (sikringsskab, F&P BLÅ klasse, hovedgruppe 2) med sikkerhedsgodkendt kombinationslås. Er reaktionstiden for indsatsstyrken mindre end 5 minutter, kan der i stedet for et klasse A opbevaringsmiddel anvendes et klasse B opbevaringsmiddel. Opbevaringsmidlet skal befinde sig inden for et sikret område, minimum områdekategori 2 sikringsniveau 30 således, at der ved mindre mængder klassificeret materiale hos fx sagsbehandlere anvendes sikringsniveau 30 og ved større mængder klassificeret materiale ved fx en myndigheds hovedarkiv anvendes sikringsniveau 40. Ønskes materiale opbevaret på åbne hylder skal dette ske i arkivrum jf. bestemmelserne i kapitel 7.

Opbevares materiale klassificeret HEM undtagelsesvis i overvåget område, områdekategori 4 skal den anslåede samlede mekaniske sikrings holdetid i minutter, som minimum være det dobbelte af reaktionstiden for indsatsstyrken. Dette opnås bla. ved anvendelse af opbevaringsmidler af F&P RØD klasse, hovedgruppe 2 (eller andet opbevaringsmiddel, godkendt efter EN-1143-1 norm, min. GRADE 1) med sikkerhedsgodkendt elektronisk eller mekanisk kombinationslås suppleret med yderligere elektronisk overvågning etableret som verificeret alarm.

4. FORTROLIGT

Materiale klassificeret FTR skal opbevares i godkendt og aflåst opbevaringsmiddel som minimum militær klassificering B, EN1143-1, GRADE 0, (sikringsskab, F&P GUL klasse hovedgruppe 2). Opbevaringsmidlet skal befinde sig inden for et sikret område, minimum områdekategori 2, sikringsniveau 30 eller 40 således, at der ved mindre mængder klassificeret materiale hos fx. sagsbehandlere anvendes sikringsniveau 30 og ved større mængder klassificeret materiale ved fx. en myndigheds hovedarkiv anvendes sikringsniveau 40.

Opbevares materiale klassificeret FTR undtagelsesvis i overvåget område, områdekategori 4 skal den anslåede gennembrydnings- og/eller oplukningstid svare til den anslåede reaktionstid. Dette kan bl.a. opnås ved anvendelse af kraftigere opbevaringsmidler med sikkerhedsgodkendt kombinationslås, kombineret med yderligere elektronisk overvågning evt. etableret som verificeret alarm.

5. TIL TJENESTEBRUG

Materiale klassificeret TTJ skal opbevares i aflåst gemme.

6. OPBEVARING VED CIVILE MYNDIGHEDER OG INSTITUTIONER

Overdrages undtagelsesvis klassificeret informationsbærende materiale til enkeltpersoner, erhvervssammenslutninger, private virksomheder o. lign. samt den offentlige administration skal FE godkendelse indhentes i det enkelte tilfælde inden overdragelsen finder sted. FE foranlediger.

KAPITEL 5

OPERATIONSSIKKERHED

Bilag:

1. Plan for og eksempler på opretholdelse af operationssikkerhed.
2. Introduktion og vejledning til støtteværktøj for etablering af militær sikkerhed i internationale missioner.

1. DEFINITIONER

Operationssikkerhed er den løbende proces, som giver egne operationer og øvelser den fornødne sikkerhed, og som gennem anvendelse af passive og/eller aktive tiltag, hindrer en modstander eller tredjepart i at indhente oplysninger om egne og allierede styrkers dispositioner, kapaciteter og intentioner (AAP 6).

Operationssikkerhed er den del af styrkebeskyttelsen (Force Protection), der skal beskytte de informationer og aktiviteter, som chefen vurderer vitale, og som kan indikere, at en operation planlægges, forberedes eller iværksættes.

Styrkebeskyttelse defineres som alle de forholdsregler og foranstaltninger, der iværksættes for at minimere sårbarheden fra alle trusler og i alle situationer mod personel, anlæg, materiel og operationer og aktiviteter for at sikre styrkens handlefrihed og operative effektivitet (AAP-6).

En operation er en militær aktivitet eller gennemførelse af en strategisk -, taktisk -, støtte -, trænings - eller administrativ opgave herunder processen at føre en kamp inklusiv nødvendige bevægelser, forsyninger, angreb, forsvar og manøvrer for at løse opgaven (AAP-6).

Operationssikkerhed anvendes i forbindelse med operationer, der har et specifikt mål og et tidsmæssigt begrænset forløb. Som eksempler på planlagte operationer kan nævnes deployeringer af styrker fra Danmark til et missions-, operations- eller baseområde, indsættelse af en styrke i et missionsområde mod et specifikt mål eller støtte til allieredes operationer. Endvidere kan opgaver som modtagelse af VIP besøg i lejren, særlige transportopgaver, personelrotationer og modtagelse af forstærkninger betragtes som operationer, der kræver en plan for operationssikkerhed.

2. FORMÅL

Operationssikkerhed har til formål¹ at opretholde en effektiv beskyttelse af planlægning, forberedelse og udførelse af militære operationer² og de dertil knyttede aktiviteter under alle forhold ved at hindre modstanderen eller en tredjepart indsigt i operationen.

Operationssikkerhed skal

- identificere de aktiviteter, der kan observeres af modstanderens indhentningskapaciteter
- identificere de indikatorer, som modstanderens indhentningskapaciteter over tid, kan analysere og stykke sammen til kritisk information, der i rette tid kan udnyttes af en modstander, og

¹ Jf. ACO DIR (AD) 080-025.

² Militære operationer dækker også operationer og opgaver, der udføres i fredsskabende og fredsbevarende missioner.

- udvælge og iværksætte passive og/eller aktive modtiltag, som eliminerer eller reducerer sårbarheden overfor modstanderens indhentningskapaciteter til et acceptabelt risikoniveau (risikostyring).

3. ANSVAR

Operationssikkerhed er en operativ funktion, der er omfattet af chefansvaret.

4. GENERELT

Operationssikkerhed er som personel-, materiel-, dokument-, informationssikkerhed og fysisk sikkerhed en del af sikkerhedssøjlen³ i styrkebeskyttelsen. Planen for operationssikkerhed skal beskrive de særlige tiltag, der eventuelt iværksættes før, under og efter en operation for at begrænse modstanderens mulighed for at skaffe sig vital viden om enhedens dispositioner, kapaciteter, intentioner og sårbarheder.

Operationssikkerhed skal ikke bare fokusere på de aktiviteter, der vedrører operationen men også på de ændringer i aktiviteter og rutiner, som operationen medfører i såvel støttestrukturen som i de daglige arbejdsrutiner og patruljemønstre. Der skal være fokus på de ændringer, der kan observeres af en modstander, og dermed giver ham indikationer på forberedelser til specielle operationer.

Operationssikkerhed er tæt forbundet med sløring og vildledning. Hvor operationssikkerhed skal forhindre modstanderen eller en tredjepart i at skaffe sig reel viden, sigter sløring og vildledning på at give et falsk eller forvrænget billede af egne styrkers aktuelle og fremtidige dispositioner, kapaciteter, intentioner og sårbarheder. Sløring og vildledning kan anvendes både som et passivt og et aktivt tiltag.

De kilder, som en modstander kan anvende til at skaffe informationer om egne og allierede styrker, kan være direkte forbundet med enhederne; men kritiske informationer kan også skaffes fra kilder, der ligger udenfor enhedernes kontrol, så som observationer mod civile og militære logistiske leverancer, politiske beslutninger, medieomtale, forsvaret samt forsvarets ansattes brug af internet og sociale medier. Effekten af operationssikkerhedsmæssige tiltag er tæt forbundet med personellet generelle sikkerhedsforståelse.

5. PRINCIPPER FOR OPERATIONSSIKKERHED

Operationssikkerhed er en proces som analyserer sikkerheden ved en operation ud fra modstanderens efterretningsbehov og indhentningskapaciteter. Enhver operation skal vurderes som en helhed ud fra modstanderens synspunkt, og alle aktiviteter relateret til operation skal medtages, herunder også øvelser, støtte operationer, kommunikations- og informationssystemer samt de logistiske netværk og andre baglands- eller lejraktiviteter. Da det ikke er muligt at skjule alle aktiviteter, skal operationssikkerhed koncentreres om de aktiviteter, der kan indikere, at en operation er forestående og de aktiviteter, der kan afsløre sårbarheder⁴. Hvor kritiske aktiviteter kan observeres, skal det overvejes at bruge sløring eller vildledning.

³ Jf. ACO DIR (AD) 080-025 baseres styrkebeskyttelse på 8 kapacitetsområder.

⁴ Disse indikatorer omtales som: "Essential Elements of Friendly Information (EEFI).

5.1. MODSTANDEREN ELLER TREDJEPARTS SYNSVINKEL.

Operationssikkerhed bør grundlæggende vurderes fra modstanderens side. For at identificere kritisk information må det vurderes, hvad modstanderen ved, og hvilke informationer, han kan udlede af specifikke hændelser og informationer. I den forbindelse kan såvel faste rutiner som ændringer af faste rutiner afsløre en operation.

5.2. KRITISKE OPLYSNINGER.

Operationssikkerhed omfatter en vurdering af hvilke informationer om en operation og de dertil knyttede aktiviteter, der er kritiske. Vurderingen omfatter endvidere hvilke informationer om kapaciteter, materiel og logistiske forhold, der er kritiske. Operationssikkerhed skal identificere de kritiske informationer, som en modstander kan anvende til at forudsige en operation. Operationssikkerhed skal forhindre, at en modstander får kritisk viden, der sætter ham i stand til at angribe og sabotere vitale elementer eller til at imødegå og bekæmpe den indsatte styrke, således at målet for den planlagte operation ikke opnås. Målet for operationssikkerhed er således at beskytte kritisk information for at sikre en operation.

5.3. KOORDINATION.

Planlægning af operationssikkerhed skal koordineres på alle niveauer såvel internt i staben og enheden som eksternt med overordnede og underlagte myndigheder, herunder internationale og allierede partnere på "need to know" basis, således at operationssikkerheden opretholdes på alle niveauer.

5.4. OMFANG OG RETTIDIGHED.

Operationssikkerhed omfatter alle aspekter i en operation herunder overordnede og detaljerede tidsplaner, administrative tiltag, logistiske planer og forhold, kommunikationsplaner og –trafik samt bevægelser for alle elementer i den pågældende styrke. Identifikation af kritiske oplysninger skal gennemføres tidligst muligt i planlægningen af en operation. Manglende operationssikkerhed kan nødvendiggøre aflysning af en operation, hvis planen er blevet kompromitteret.

5.5. TILPASNING AF TILTAG.

De tiltag, der iværksættes med henblik på at opretholde operationssikkerhed, skal afstemmes efter modstanderens efterretningskapaciteter. En overvurderet trussel kan således fjerne egne ressourcer fra operationen. De iværksatte tiltag skal accepteres af modstanderen som en del af normalbilledet, og de må i sig selv ikke indikere, at en operation er under forberedelse.

5.6. FLEKSIBILITET.

Planen for operationssikkerhed skal løbende tilpasses ændringer i situationen, herunder såvel ændringer i planlægningsfasen som ændringer i forbindelse med mulige kompromitteringer af kritiske oplysninger. Ved en mulig kompromittering af dele af planen skal den operative leder vurdere, om planen kan gennemføres, om den kan ændres eller om operationen skal aflyses.

6. TILTAG

De tiltag, der iværksættes med henblik på at opretholde operationssikkerhed, kan bestå af generelle tiltag for hele styrken og specifikke, eventuelt tidsbegrænsede tiltag for enkelte

enheder, udstyr, installationer eller områder. Tiltag iværksættes ud fra en risikovurdering og afstemmes efter modstanderens efterretningskapaciteter, herunder modstanderens indhentningsmidler i området så som rekognoscering, overvågning, specialstyrker, sympatisører eller agenter. De iværksatte tiltag kan være passive med skærpede sikkerhedstiltag eller aktive i form af øget bevogtning, patruljering samt angreb på eller eliminering af modstanderens indhentningskapaciteter for at begrænse indhentning. De iværksatte tiltag kan suppleres med sløring og vildledning for at hindre indhentning og give modstanderen et ufuldstændigt eller fejlagtigt billede af egne dispositioner, kapaciteter og intentioner (se bilag: Plan for og eksempler på opretholdelse af operationssikkerhed).

7. PLANLÆGNING AF OPERATIONSSIKKERHED

Det er operationselementet og efterretningselementerne, der sammen planlægger operationssikkerhed. Tilrettelæggelsen udføres af operationselementet i tæt samarbejde med stabens øvrige elementer. I enheder, hvor der ikke er operations- eller efterretnings-elementer er chefen ansvarlig for planlægningen. I alle tilfælde inddrages SIKOF, CI-officeren og evt. andet relevant sikkerhedspersonel i nødvendigt omfang.

Operationssikkerhed er en løbende proces, der planlægges, tilrettelægges og gennemføres i fire faser, der udgør en repeterende cyklus.

7.1. ANALYSE AF TRUSLEN.

Truslen analyseres og vurderes ud fra kendskabet til modstanderens indhentningskapaciteter samt hans evne til at udnytte informationer og imødegå eller forhindre en operation i at gennemføres med succes.

7.2. IDENTIFIKATION AF KRITISKE INFORMATIONER.

På baggrund af trusselsanalysen vurderes hvilke informationer en modstander kan havekendskab til samt hvilke informationer modstanderen mangler tilstrækkeligt kendskab til for at forudsige, imødegå eller forhindre en operation.

7.3. SÅRBARHED.

I forbindelse med en operation vurderes hvilke aktiviteter og forhold, der i planlægnings-forberedelses- iværksættelses- og afslutningsfasen kan give en modstander kritisk information. Ud fra en vurdering af modstanderens indhentningskapacitet og viden analyseres og fastlægges hvilke oplysninger om egne forestående og igangværende aktiviteter, der skal betragtes som vitale eller sensitive for aktivitetens gennemførelse.

7.4. VALG AF MIDLER FOR OPERATIONSSIKKERHED.

Den operative chef skal ud fra en analyse og vurdering af trusler og sårbarheder udgive et direktiv for hvilke særlige beskyttelsestiltag, der skal effektueres i forbindelse med planlægning og gennemførelse af en operation. Planen bør fastlægge hvilke informationer/områder, der vurderes som vitale eller sensitive for operationen i den givne situation, og som derfor bør være belagt med særlige restriktioner. Planen bør ligeledes indeholde tidsplan for, hvornår og i hvilket omfang delplaner og detaljer vedr. operationen kan meddeles til de deltagende enheder.

Planen for operationssikkerhed bør udgives som et bilag eller et tillæg til operationsplanen for en specifik operation for at sætte fokus på de kritiske elementer i operationen. De enkelte tiltag for operationssikkerhed kan efter den operative chefs vurdering indgå i de

relevante dele af operationsplanen. Planen for operationssikkerhed skal nøje koordineres med eventuelle planer for sløring og vildledning.

8. TILTAG TIL GENNEMFØRELSE AF OPERATIONSSIKKERHED

Tiltag til opretholdelse af operationssikkerhed er primært tilknyttet en specifik operation, men tiltagene kan have relation til de daglige aktiviteter f.eks. i en lejr. Eventuelle tiltag bør kun sættes i værk, hvis det vurderes, at effekten står mål med indsatsen.

De daglige rutiner og stereotype procedurer bør varieres således at forberedelse af større operationer ikke afsløres ved ændringer i hverdagen. Personellets generelle sikkerhedsforståelse i hverdagen er en forudsætning for at opretholde operationssikkerhed.

9. KONTROL

Kontrol af operationssikkerhed forudsætter, at der i forbindelse med operationer udgives særlige direktiver med skærpede tiltag vedr. enkeltdele af planen. Selve kontrollen vil herefter være fokuseret på, om de udgivne direktiver og sikkerhedsbestemmelser efterleves, herunder en vurdering af det involverede personels sikkerhedsforståelse. Kontrol af operationssikkerhed er ikke et sikkerhedseftersyn af hele sikkerhedsområdet jf. FKOBST 358-1.

PLAN FOR OG EKSEMPLER PÅ OPRETHOLDELSE AF OPERATIONSSIKKERHED

1. GENERELT.

Planen for operationssikkerhed skal baseres på brug af de muligheder, der er i bestemmelserne for personel -, materiel -, dokument -, informations - og fysisk sikkerhed men bør dog ikke begrænses til disse. Mange af de indikatorer, der kan observeres af en modstander, så som daglige rutiner og procedurer, patruljeringsmønstre, øvelser og aktiviteter forud for en operation er ikke nødvendigvis klassificerede, men de kan dog være med til at afsløre den forestående operation. I forbindelse med operationssikkerhed skal det overvejes at bruge sløring og vildledning for at forhindre modstanderen i at opnå det fulde billede af operationen.

2. PLANEN.

Det er en operativ vurdering hvilke operationer, der kræver en særskilt plan for operationssikkerhed. Planen kan udgives som en selvstændig plan i form af bilag eller tillæg til en operationsplan, eller den kan indarbejdes i delplanerne for operationen som f. eks kommunikationsplan, logistikplan etc.

3. TILTAG.

Planen skal beskrive de tiltag, der skal iværksættes for at begrænse modstanderens mulighed for at få kendskab til de vitale informationer, der kan give ham mulighed for at standse en operation eller forhindre succes. Tiltag skal iværksættes i hele forløbet fra planlægning, forberedelse, gennemførelse og til afslutning af operationen. Alle iværksatte tiltag bør være en del af normalbilledet og gennemføres indenfor styrkens faste rutiner og procedurerne. I planlægningen skal det overvejes, i hvilket omfang særlige tiltag på nedenstående sikkerhedsområder skal iværksættes til brug for operationssikkerhed.

3.1. Personelsikkerhed.

Det personel, som skal arbejde med operationen, skal være sikkerhedsgodkendt til de dele af planen, som de skal arbejde med. Det gælder både nøglepersoner og teknik- og støttepersonel som f.eks. it supportere, sekretærer, tolke, arkiv personale m.fl. med adgang til informationerne. I planlægnings- og forberedelsesfasen bør kun nøglepersoner, der har et behov kende til og arbejde med operationen i alle dens faser, have adgang efter "Need to Know" princippet. Planen bør endvidere beskrive, hvornår det involverede personel orienteres om hele eller for dem, relevante dele af operationen.

Operationssikkerhed kan udgøre et særligt problem i relation til allierede partnere, som enten skal deltage i eller være vidende om operationen, hvis disse partnere ikke behandler informationerne på det samme sikkerhedsniveau.

I missioner, hvor egne styrker skal samarbejde med nationale og lokale militære eller civile sikkerhedsstyrker (Embedded Partnering), skal der være særligt fokus på operationssikkerhed i fælles operationer.

3.2. Materielsikkerhed.

I missioner, hvor det materiel, der er til rådighed til opbevaring og aflåsning, ikke er tilstrækkeligt til at sikre vitale informationer, skal chefen iværksætte tiltag til at sikre vitale informationer ved bevogtning, opbevaring i døgnbemande rum eller ved andre tiltag, der i situationen giver tilstrækkelig sikkerhed mod kompromittering.

3.3. Dokumentsikkerhed.

Planen for operationssikkerhed skal beskrive om og i hvilket omfang, der for hele eller dele af planlægningen skal anvendes særlige restriktioner på dokumenter som beskrevet i kapitel 1 til FKOBST 358-1 med særlige mærkninger. Det bør overvejes at anvende "Need to Know" mærkning, suppleret med angivelse af den personelgruppe, der har adgang til informationerne. Der kan endvidere iværksættes særlige procedurer for opbevaring, fordeling og makulering af disse dokumenter.

3.4. Informationssikkerhed.

Planen for operationssikkerhed skal angive hvilke restriktioner, der evt. skal iværksættes ved behandling i informatiksystemer. Planen skal beskrive brugen af netværk (missions-netværk, nationalt eller stand alone). Endvidere skal planen beskrive evt. restriktioner så som behandling i lukkede brugergrupper og adgangsbegrænsninger til mapper og filer, samt evt. brug af password. Endvidere skal eventuelle begrænsninger i brugen af USB stik og andre lagermedier, dedikerede printere og behandling af udskrifter beskrives. Ligeledes skal der udarbejdes en policy for brug af e-mail vedr. operationen for at undgå spredning af informationer. Operationssikkerhed i forbindelse med brug af it-systemer i en operation kan med fordel udarbejdes som en standardinstruks, der kan iværksættes, når der er behov for ekstra sikkerhed.

3.5. Fysisk sikkerhed.

Planen skal indeholde eventuelle restriktioner for adgang til områder, hvor operationen planlægges og forberedes. Der kan således være restriktioner for enkelte kontorer, operationsrum, briefingrum og lignende, men det skal også overvejes om der skal være restriktioner for adgang til logistikområder, klargøringsområder og lignende, idet såvel ændringer i forsyningsmængde og type samt klargøringsaktiviteter kan være med til at give indikationer på en forestående operation. Hvor de fysiske forhold vurderes at være utilstrækkelige til at sikre informationer, kan der efter den operative leders vurdering iværksættes yderligere tiltag så som samlet opbevaring under bevogtning, alarmer eller alternativ opbevaring i arkiv eller andet sikret sted. Endvidere kan fysisk sikkerhed suppleres med slørings- og vildledningsaktiviteter.

3.6. Informations – og presse politik.

Planen skal indeholde en tidsplan for, hvornår nødvendige informationer til brug for forbedelser kan formidles til berørte enheder og evt. til pressen. Tidsplanen skal endvidere beskrive, hvornår involveret personel og støttefunktioner informeres. Tidsplanen skal koordineres med kommandomyndigheder og allierede enheder, der deltager i operationen eller opererer i området. Der kan i forbindelse med særlige operationer i missionsområdet, forøget indsats i området, VIP besøg m.fl. fra allierede, fra kommandomyndigheder eller af politisk interesse være ønske om pressedækning af enhedens indsats. Der bør i disse tilfælde aftales med medierne, hvornår informationerne kan offentliggøres f.eks. i forbindelse med VIP besøg. Soldaterne skal ligeledes informeres om på hvilket tidspunkt, de kan informere pårørende m.fl. om operationer eller besøg i lejren.

3.7. Andre forhold.

Den operative leder og alle, der arbejder med operationssikkerhed, bør løbende identificere aktiviteter og forhold, der for en modstander afslører forestående operationer. En modstander vil dels se på faste rutiner i operationsmønstre og dels på ændringer i disse for at forudsige en operation.

3.7.1. Faste rutiner.

Faste rutiner kan afsløre at en operation er på vej. Det kan f.eks. være forløbet op til en operation, hvor der udføres intensiveret rekognoscering i et område, evt. med fly eller UAV'er fulgt af en operation, radiotavshed før en særlig vigtig operation, afbestilling af kost før en operation, aflysning af planlagte CIMIC opgaver eller besøg, som alle kan være faktorer, der kan være tegn på en kommende operation.

3.7.2. Ændrede rutiner.

Forberedelse af en større operation kan være svær at skjule i de daglige rutiner. Planen skal tage hensyn til de vitale aktiviteter, der ikke kan skjules i de daglige rutiner, og vurdere, hvordan man med fordel kan anvende sløring eller vildledning til gradvis at ændre de faste rutiner mod de ønskede tiltag. Løbende ændringer og uregelmæssigheder i dagligdagen vil være med til at sløre eller vildlede en modstander om, at en operation er under forberedelse.

3.7.3. Kritiske faktorer.

Kritisk materiel er ikke i sig selv en del af operationssikkerheden for en operation. Operationssikkerhedsmæssigt er det nogle af de faktorer, som en modstander over tid kan observere og identificere som kritiske, og dermed kan modstanderen ved aktioner i rette tid forhindre en forestående operation. Modstanderens viden om kritiske områder har kun betydning, hvis angreb på eller sabotage af materiellet kan forhindre den forestående operation. Et angreb på styrkens drivmiddel depot behøver f.eks. ikke være kritisk for operationen, hvis alle køretøjer er tanket.

4. DIREKTIVER

Selv om operationssikkerhed knytter sig til en specifik operation, kan chefen udarbejde standard direktiver for tiltag, der kan iværksættes i operationsplanen eller være gældende i hverdagen f. eks. for adgang til operationsområder og brug af informatiksystemer i planlægningsfasen.

5. FORUDSEENHED

Ved planlægning af operationssikkerhed skal chefen og de øvrige planlæggere vurdere hvilke forhold i missionen, der kan være med til at afsløre informationer. Det bør løbende vurderes, hvordan forholdene i lejrindretningen, planlægning af de daglige rutiner og procedurer løbende kan bruges til at sløre eller vildlede modstanderens indhentningskapaciteter. Mange rutiner er forårsaget eller styret af støttefunktioner så som faste tider for levering af forsyninger, rotationsflyvninger, kostforplejning, morgenbriefinger og ordredgivelser. Hvor rutiner ikke kan ændres, bør de udnyttes til at skjule operationsforberedelser. Hvor der er mulighed for fleksibilitet, bør denne fleksibilitet anvendes bedst muligt til at skjule andre dele af forberedelserne.

INTRODUKTION OG VEJLEDNING TILSTØTTEVÆRKTØJ FOR ETABLERING AF MILITÆR SIKKERHED I INTERNATIONALE MISSIONER.

1. BAGGRUND

Støtteværktøjet er initieret af Forsvarsministeriets Sikkerhedsudvalg efter ønske fra de operative kommandoer.

2. FORMÅL

Støtteværktøjet skal hjælpe såvel sikkerhedsofficerer som chefer og planlæggere i forbindelse med vurdering og etablering af militær sikkerhed i forbindelse med nye missioner, således at sikkerheden kan indarbejdes i den operative planlægning gennem alle faser fra missionens start til missionens afvikling.

I initialfasen (hold 0/1) af en ny mission, samt i større længerevarende missioner, anbefales det at sikkerhedsofficersfunktionen er en fuldtidsstilling.

3. AFGRÆNSNING

Støtteværktøjet fokuserer på militær sikkerhed som beskrevet i FKO BST 358-1, Bestemmelser for Den Militære Sikkerhedstjeneste, og dermed på beskyttelse af klassificerede informationer og vitalt eller sensitivt materiel. Værktøjet omfatter kun de dele af styrkebeskyttelsen, der relaterer sig til militær sikkerhed,

4. ANVENDELSE

Støtteværktøjet skal støtte brugeren ved at skabe et overblik over de sikkerhedstiltag, der er nødvendige for at etablere og opretholde et tilstrækkeligt sikkerhedsniveau og dermed skabe grundlaget for militær sikkerhed i internationale missioner. Støtteværktøjet, der referer til de enkelte kapitler i FKO BST 358, skal lede og inspirere brugeren gennem en række sikkerhedsmæssige overvejelser, der er nødvendige i opbygningen af missionens militære sikkerhed. Støtteværktøjet er ikke en tjekliste, der kan dække alle missioner og situationer, men et dynamisk værktøj, der giver brugeren mulighed for at tilføje og fjerne punkter tilpasset den aktuelle mission.

5. STØTTEVÆRKTØJ

[Støtteværktøjet](#) med tilhørende vejledning kan hentes på FE sikkerhedsportal på FIIN eller rekvireres ved FE. Værktøjet kan endvidere hentes via skrivbare skabeloner i FKOBST 358-1. Støtteværktøjet er inddelt i 8 dele med hver deres emneområde:

5.1. Del 1 - sikkerhedsmæssige overvejelser

Værktøjet skal støtte brugerens sikkerhedsmæssige og operative overvejelser i forbindelse med indretning af lejrområdet, herunder placering af operative og sikrede områder. Indretningen af lejren skal således reducere effekten af truslen fra spionage og indhentning rettet mod styrken i lejrområdet. Endvidere fokuserer operationssikkerhed på adgangs- og opholdkontrol til såvel lejr som bygninger allerede fra etableringsfasen, herunder også ved etablering af nye anlæg og nyt byggeri. Støtteværktøjet fokuserer på militær sikkerhed, men brugeren kan medtage andre dele af styrkebeskyttelsen ved sin brug af værktøjet.

5.2. Del 2 - generel sikkerhed

Værktøjet skal støtte brugeren igennem overvejelser omkring sikkerhedsorganisationen og dennes samspil med den evt. internationale sikkerhedsorganisation i lejren. Hvis den etablerede lejr er dansk, da støttes vurderingen af egen organisation og samspillet med øvrige enheder i området. Endvidere behandles samarbejde med lokale myndigheder, f.eks. i forbindelse med "embedded partnering".

5.3. Del 3 - personelsikkerhed

Værktøjet skal støtte brugeren i overvejelser omkring sikkerhedsgodkendelser for eget personel, herunder behovet for sikkerhedstjek (vetting) af lokalt ansatte. Endvidere inddrages sikkerhedsgodkendelser og sikkerhedsuddannelser for personel i særlige funktioner og generelle sikkerhedsuddannelser for alt personel før og under udsendelsen. Del tre omfatter endvidere regler for omgang med udenlandsk personel.

5.4 Del 4 - materielsikkerhed

Værktøjet skal støtte brugeren ved vurderingen af behovet for opbevaring af vitalt, sensitivt eller klassificeret materiel og informationer for at etablere områdeinddelinger og fastlægge sikringsniveauer for de enkelte lejrområder. Del fire skal endvidere afdække behovet for opbevaringsmidler for klassificerede informationer og opbevaringsfaciliteter for klassificeret, vitalt eller sensitivt materiel.

5.5. Del 5 - dokumentssikkerhed

Værktøjet skal støtte brugeren i vurderinger omkring dokumenthåndtering, herunder nødvendige funktioner samt organisation og faciliteter til registrering, opbevaring, forsendelse og destruktion af klassificeret materiale. Vurderingen skal afdække hvilke faciliteter, der er i missionen, og hvilke der et nationalt ansvar.

5.6. Del 6 - operationssikkerhed

Værktøjet skal støtte brugeren i såvel sikkerhedsmæssige som operative overvejelser i forbindelse med etablering af lejren. Del seks omhandler adgang til informationer og indsigt til operative aktiviteter i missionen. For begge forholds vedkommende kan der forebygges ved en hensigtsmæssig indretning af lejrområdet. Der fokuseres endvidere på fremmedes adgang til klassificerede områder og deres bevægelser i hverdagen. Operationssikkerhed fokuserer på rutiner og sikkerhedsforståelse.

5.7. Del 7 - informationssikkerhed

Værktøjet skal støtte brugeren med at afdække behovet for kommunikationsmidler og IT systemer til behandling af klassificerede informationer, herunder afdækning af hvilke systemer, der er til rådighed i missionen, og hvilke der skal etableres. Støtteværktøjet beskæftiger sig ikke med sikkerhedsmæssige tiltag omkring de klassificerede systemer, da dette er en del af installationsgodkendelsen.

5.8. Del 8 - fysisk sikkerhed

Værktøjet skal støtte brugeren ved vurderingen af den fysiske sikring af et dansk lejrområde. Der fokuseres på, hvad der skal sikres og dermed behovet for sikre og overvågede områder. Del otte skal endvidere støtte brugerens overvejelser i forbindelse med sikring af lejren, herunder fastlæggelse af ansvar og behov for sikkerhed i lejrområdet. Værktøjet skal endvidere støtte ved en vurdering af hvilke opgaver, der løses af andre, og hvilke opgaver og tiltag den danske enhed selv skal varetage. Det skal i den forbindelse overvejes, om der skal etableres særlige adgangsbegrænsninger til dele af det danske lejrområde samt om der er behov for adgangs- og opholdskontrol i hele eller dele af det danske område.

KAPITEL 6

INFORMATIONSSIKKERHED

AFSNIT I

INDLEDNING

1. FORMÅL OG ANVENDELSESOMRÅDE

Formålet med dette kapitel er at fastlægge krav til beskyttelsen af informationer, der lagres, behandles eller transmitteres ved hjælp af informations- og kommunikationsteknologi, herunder også OT¹ og IOT². Disse informationer skal beskyttes mod trusler om tab af fortrolighed, integritet og tilgængelighed. Formålet er desuden at fastlægge krav til beskyttelsen af ikke-informationsbærende systemer, der understøtter vigtige forretningsprocesser i koncernen, som eksempelvis visse militære, operative systemer samt alarmeringssystemer.

Kapitlet er henvendt til medarbejdere der arbejder med risikostyring inden for informationssikkerhed herunder persondatabeskyttelse (navnlig risikorådgivere, databeskyttelsespecialister, forretningsrepræsentanter og forretningsansvarlige for systemer samt system-sikkerhedsofficerer) og medarbejdere i øvrigt i informationssikkerhedsorganisationen, forretningen og ved de koncerninterne leverandører, der arbejder med implementering af informationssikkerhedsforanstaltninger.

Medarbejderne forudsættes at have kompetencer inden for informationssikkerhed, herunder i relevant omfang it-sikkerhed og persondatabeskyttelse, samt viden om FMNBST 358-2 om risikostyring inden for informationssikkerhed. Medarbejderne skal desuden have viden om og kunne anvende ISO 27002 og ISO 27701 som vejledning til implementering af foranstaltninger.

2. KRAV TIL FORANSTALTNINGER

Informationssikkerheden skal baseres på risikostyring i henhold til FMNBST 358-2 om risikostyring inden for informationssikkerhed. Risikostyringen skal sikre etablering og opretholdelse af et informationssikkerhedsniveau, der er afstemt i forhold til risikobilledet, og som understøtter varetagelsen af koncernens kerneopgaver. Det kan f.eks. gælde i forhold til operationssikkerhed, jf. kapitel 5, hvor der kan være et behov for at skærpe informationssikkerhedsforanstaltningerne.

Forsvarsministeriet og FE har, jf. afsnit II nedenfor, fastlagt minimumskrav til informationssikkerheden, herunder til persondatabeskyttelse, ved at forhåndsudvælge en række henholdsvis organisatoriske, adfærdsmæssige, fysiske og tekniske foranstaltninger, der som udgangspunkt alle skal implementeres.

¹ Operational Technology.

² Internet of Things.

I bilag 5 til kapitel 6 findes en oversigt over de forhåndsudvalgte foranstaltninger, herunder delforanstaltninger, med anførsel af om de er obligatoriske, eller om de eventuelt kan fraviges på baggrund af risikovurdering. For profil B og C klassificerede systemer, jf. afsnit II, pkt. 2 nedenfor, er de angivne foranstaltninger obligatoriske og kan ikke fravælges på baggrund af risikovurdering. Det fremgår desuden af bilag 5, hvem der typisk skal implementere foranstaltningerne.

Myndighederne skal være opmærksomme på eventuelle yderligere krav til foranstaltninger, end de der fremgår af kapitel 6. Det kan f.eks. være yderligere krav i forhold til persondataskyttelse, de af Digitaliserings-styrelsen udmeldte "tekniske minimumskrav" samt krav fastsat i relation til akkreditering af systemer og installationer.

3. ROLLER OG ANSVAR FOR FORANSTALTNINGER

Den overordnede organisering på informationssikkerhedsområdet er beskrevet i FMNPOL 358-1, Koncern Cyber- og Informationssikkerhedspolitik.

Styrelses- og myndighedschefer i koncernen har ansvaret for informationssikkerheden inden for eget område i forhold til forretningsprocesserne og anvendelsen herunder afhængigheden af understøttende it-services og systemer.

Myndighederne skal dokumentere og implementere informationssikkerhedsforanstaltninger, herunder hvad angår persondataskyttelse i henhold til kravene i dette kapitel med bilag. Det gælder også koncerninterne leverandører med driftsansvar for systemer uanset, om der måtte foreligge et aftalegrundlag med myndighederne med specifikke krav til informationssikkerheden for de leverede it-services og systemer.

Forsvarsministeriets koncern Chief Information Security Officer (CISO) kan til koncernens myndigheder anvise, herunder påbyde konkrete foranstaltninger, der skal implementeres, på alle områder inden for informationssikkerhed, der er behandlet i dette kapitel med bilag. Det vil typisk kunne ske på baggrund af enten Forsvarsministeriets tilsyn med informationssikkerheden herunder persondataskyttelsen, rapportering om risikovurderinger i koncernen, eller læring efter hændelser.

FE's Center for Cybersikkerhed rådgiver og vejleder som national it-sikkerhedsmyndighed om Danmarks nationale og internationale forpligtelser i relation til sikkerhedsbeskyttelse af klassificeret, elektronisk information, herunder om NATO og EU's konkrete krav på området. Se herunder bilag 3 til dette kapitel, Vejledning om informationssikkerhed ved håndtering af klassificeret information. Center for Cybersikkerhed anviser desuden som national it-sikkerhedsmyndighed konkrete informationssikkerhedsforanstaltninger, der skal implementeres, som led i sikkerhedsakkreditering af systemer og kryptoudstyr m.v. samt som led i tilsyn med sikkerhedsbeskyttelsen af klassificeret, elektronisk information. I det omfang Center for Cybersikkerhed derudover som national it-sikkerhedsmyndighed måtte udmelde krav til informationssikkerhedsforanstaltninger, vil disse blive anvist i koncernen gennem Forsvarsministeriets koncern CISO.

4. DISPENSATION

Forsvarsministeriets koncern CISO kan dispensere fra kravene til informationssikkerhedsforanstaltninger herunder foranstaltninger til persondataskyttelse i dette kapitel.

Center for Cybersikkerhed kan dispensere fra yderligere krav til sikkerhedsforanstaltninger, der måtte være fastlagt som led i Center for Cybersikkerheds akkrediteringer herunder af systemer og på baggrund af centerets tilsyn.

Dispensationer derudover fra krav udmeldt af Center for Cybersikkerhed, håndteres i et samarbejde med Forsvarsministeriets koncern CISO.

Hvis der er tale om obligatoriske krav, der følger af internationale eller nationale regelsæt, kan der alene og kun undtagelsesvist i visse tilfælde gives en tidsbegrænset dispensation. Dette kan kun ske på baggrund af en dokumenteret risikovurdering, hvorved der samtidig er taget stilling til kompenserende foranstaltninger med henblik på at minimere risici.

AFSNIT II

INFORMATIONSSIKKERHEDSFORANSTALTNINGER

1. OM FORANSTALTNINGERNE

Informationssikkerhedsforanstaltningerne i afsnit II er udvalgt, struktureret og nummereret med afsæt i ISO/IEC 27001:2022, Annex A, og ISO/IEC 27002:2022. Sidstnævnte skal alene anvendes som vejledende i forhold til implementering af foranstaltningerne. Der er desuden tilføjet foranstaltninger til persondatabeskyttelse fra ISO/IEC 27701:2021, som ligeledes skal anvendes som implementeringsvejledning, i sammenhæng med GDPR³.

Hvis en foranstaltning er dækket af andre kapitler end kapitel 6 i denne bestemmelse, vil det være anført med henvisning til det relevante kapitel.

2. SIKKERHEDSPROFILER

Kravene til informationssikkerhedsforanstaltninger er yderligere inddelt ud fra sikkerhedsprofilerne A, B og C på baggrund af krav til henholdsvis forretnings- og samfundskritiske systemer samt til beskyttelse af klassificeret, elektronisk information. Sikkerhedsprofilerne er et værktøj til implementering af informationssikkerhedsforanstaltninger som led i myndighedernes risikostyring.

I bilag 5 findes en oversigt over, hvilke foranstaltninger der er knyttet til profil A, B og/eller C. Foranstaltninger tilknyttet de enkelte profiler kan omhandle såvel fortrolighed som integritet og tilgængelighed af information samt persondatabeskyttelse. Foranstaltninger tilknyttet profil A er basisforanstaltninger for alle it-services og systemer, koncernen anvender. Profil B og C indeholder skærpede krav til informationssikkerhedsforanstaltninger.

Sikkerhedsprofilerne fastlægges dels på baggrund af den højeste klassifikationsgrad for information, et system skal kunne håndtere, dels på baggrund af en vurdering af forretnings- og samfundskritikalitet. Hvis en forretningsmæssig konsekvensvurdering viser, at et system er forretningskritisk, vælges som minimum profil B. Hvis en konsekvensvurdering (PIA⁴) viser høje konsekvenser for de registrerede ved brud på persondatabeskyttelsen, skal et system behandles som forretningskritisk. Hvis et system er samfundskritisk, vælges

³ General Data Protection Regulation.

⁴ Privacy Impact Assessment.

profil C. Det skal således vurderes, om et systems kritikalitet fordrer, at det skal sikres efter en mere sikker profil.

- **Profil A:** Profil med basisforanstaltninger for alle it-services og systemer, koncernen anvender.
- **Profil B:** Anvendes som minimum hvor et system er vurderet forretningskritisk. Profilen anvendes også altid ved systemer, der skal lagre, behandle og/eller transmittere informationer klassificeret TIL TJENESTEBRUG/NATO RESTRICTED/EU RESTRICTED.
- **Profil C:** Anvendes hvor et system er vurderet samfundskritisk. Profilen anvendes også altid ved systemer, der skal lagre, behandle og/eller transmittere informationer klassificeret FORTROLIGT/NATO CONFIDENTIAL/EU CONFIDENTIAL og HEMMELIGT/NATO SECRET/EU SECRET.

Den forretningsansvarlige for et system har opgaven med fastlæggelse af sikkerhedsprofilen for systemet på baggrund af en konsolidering af input fra risikoejere i forretningen. Hvis der er tale om et koncernfælles system, indhenter den forretningsansvarlige input via de udpegede forretningsrepræsentanter, jf. FMIDIR 380-01.

3. FORANSTALTNINGER

ORGANISATORISKE FORANSTALTNINGER

Nr.	Område
5.1	Politikker for informationssikkerhed

Der skal fastlægges, dokumenteres og kommunikeres en ledelsesgodkendt informationssikkerhedspolitik samt emnespecifikke politikker inden for informationssikkerhed.

Se Koncern Cyber- og Informationssikkerhedspolitikken i FMNPOL 358-1, der stiller krav til en styrelsesspecifik politik med målsætninger for informationssikkerheden, herunder beskyttelse af personoplysninger.

Kravene til emnespecifikke politikker samt til processer, procedurer og instrukser fremgår af beskrivelsen af foranstaltningerne i kapitel 6. Myndighederne kan vælge andre betegnelser for dokumenterne, eksempelvis "bestemmelser". Der findes en oversigt i bilag 5 til kapitel 6 over, hvor der er et dokumentationskrav for en foranstaltning. Myndighederne kan vælge at samle dokumentationen i et eller flere dokumenter. De lokale, brugerrettede informationssikkerhedsinstrukser kan eventuelt indgå i sikkerhedsinstrukserne for militærsikkerhed, jf. kapitel 9.

Nr.	Område
5.2	Roller og ansvar for informationssikkerhed

Alt ansvar for informationssikkerhed herunder persondataskyttelse, skal defineres og fordeles, og der skal være etableret en informationssikkerhedsorganisation. Informationssikkerhedsorganisationen skal være tilpasset de lokale forretningsmæssige og operative forhold, organisationen, behandlingen af personoplysninger, den geografiske udbredelse

samt antal og type af systemer, myndigheden anvender. Informationssikkerhedsorganisationen skal desuden være kendt af alle ansatte, ledelsen såvel som medarbejderne.

Der er i FMNBST 358-1 om informationssikkerhedsledelse fastlagt roller og ansvar i forhold til styrelsernes informationssikkerhedsledelse i henhold til ISO/IEC 27001. Der er i FMNBST 358-2 om risikostyring inden for informationssikkerhed fastlagt roller og ansvar i forhold til risikostyring i regi af ledelsessystemerne for informationssikkerhed.

Se desuden kapitel 1 (samt bilag 2 hertil), hvad angår rollerne informationssikkerhedsofficer (ISOF), kryptosikkerhedsofficer (KRYSO) og Terminal Area Security Officer (TASO).

Ved it-ansvarlige i koncernen, jf. FMIDIR 380-01 om it-styring, skal der for følgende systemer udpeges en systemsikkerhedsofficer (SYSO):

- Profil C klassificerede systemer
- Systemer der anvendes ved mere end én myndighed
- Systemer der er besluttet forretnings- og/eller samfundskritiske, herunder også systemer der håndterer TTJ eller ikke klassificerede informationer.

I forbindelse med indkøb, udvikling og eventuel akkreditering af nye systemer skal SYSO, jf. ovenstående kriterier for udpegning, udpeges så tidligt som muligt i projektførelsen.

SYSO' opgaver fremgår af bilag 4 til kapitel 6.

Myndigheder med ansvar for OT- og IOT-systemer skal tilsvarende vurdere behovet for udpegning af en SYSO eller tilsvarende funktion for systemerne. Opgaver som nævnt i bilag 4 omfatter i relevant omfang en sådan funktion.

Nr.	Område
5.3	Funktionsadskillelse

Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret, utilsigtet eller tilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.

Det bør ikke være den samme person, som henholdsvis godkender, udfører eller kontrollerer væsentlige aktiviteter. Der skal som minimum gennemføres en sådan funktionsadskillelse på områderne:

- Ændringsstyring for systemer og netværk
- Styring af adgangsrettigheder, herunder privilegerede (udvidede) adgangsrettigheder
- Design, implementering og gennemgang af kode
- Udvikling og test af software samt systemadministration.

Anden funktionsadskillelse skal overvejes som led i risikovurdering. Se også kravene til funktionsadskillelse i FMNBST 358-1 om informationssikkerhedsledelse, kapitel 3, for så vidt angår funktioner omfattet af denne bestemmelse.

Hvor relevant adskillelse af ansvarsområder og/eller funktionsadskillelse ikke er mulig, skal der implementeres risikomitigerende (risikoreducerende) foranstaltninger, f.eks. kontrolprocedurer eller et øget uafhængigt tilsyn.

Nr.	Område
5.4	Ledelsesansvar

Ledelsen skal som rollemodel med dens beslutninger og handlinger understøtte, at medarbejderne er opmærksomme på og har mulighed for at efterleve målsætninger og krav til informationssikkerhed herunder persondatabeskyttelse.

Ledelsen skal i den forbindelse sikre, at:

- Der er tilstrækkelige ressourcer og kompetencer.
- Der gives de nødvendige sikkerhedsinstruktioner.
- Der udfærdiges relevante procedurer samt lokale informationssikkerheds- og systemsikkerhedsinstrukser.

Ledelsen skal desuden sikre, at kravene til informationssikkerhed herunder persondatabeskyttelse håndhæves.

Alle brugere skal som minimum årligt gives en sikkerhedsinstruktion om gældende informationssikkerheds- og systemsikkerhedsinstrukser m.v. Det skal dokumenteres, hvilke medarbejdere der har modtaget instruktionen, og dokumentationen skal gemmes, indtil der gives en ny instruktion.

Nr.	Område
5.5	Kontakt med myndigheder

Der skal opretholdes passende kontakt med relevante internationale og nationale myndigheder. Det kan f.eks. være revisions- og tilsynsmyndigheder, sikkerhedsmyndigheder (herunder den nationale it-sikkerhedsmyndighed), eller myndigheder der i visse tilfælde skal modtage rapportering om hændelser (herunder Datatilsynet).

Informationssikkerheden herunder persondatabeskyttelsen skal iagttages ved udvekslingen af information med sådanne myndigheder, se 5.14.

Nr.	Område
5.6	Kontakt med særlige interessegrupper

Der skal opretholdes passende kontakt med særlige interessegrupper og andre relevante sikkerhedsfora o.l. Det kan f.eks. være i forhold til at opnå og dele viden om informationsikkerhed og persondatabeskyttelse samt modtage rådgivning.

Der skal abonneres på varsler og tweets fra den nationale it-sikkerhedsmyndighed.

Informationssikkerheden herunder persondatabeskyttelsen skal iagttages ved udvekslingen af information med disse, se 5.14.

Myndighederne skal løbende gennemgå og forholde sig til vejledninger og anbefalinger om informationssikkerhed fra Center for Cybersikkerhed.

Myndighederne skal desuden vurdere, hvilke vejledninger fra eksempelvis Datatilsynet, Politiet, PET, Digitaliseringsstyrelsen og Erhvervsstyrelsen, myndighederne vil anvende, se Sikkerdigital.dk.

Nr.	Område
5.7	Trusselsefterretning

FE herunder Center for Cybersikkerhed analyserer trusler og udsender trusselsvurderinger samt varsler. Myndighederne skal anvende disse som led i risikostyring, jf. FMNBST 358-2 om risikostyring inden for informationssikkerhed.

Nr.	Område
5.8	Informationssikkerhed ved projektstyring

Informationssikkerhed herunder persondatabeskyttelse skal uanset projekttype indgå ved projektstyring. Risikostyring i forhold til informationssikkerhed herunder persondatabeskyttelse skal således indgå i projektstyringen fra projektinitiering, gennem projektets livscyklus til overgang til drift.

Hvis der skal behandles personoplysninger, skal der udarbejdes en PIA forud for enhver behandlingsaktivitet.

Krav til informationssikkerhed herunder persondatabeskyttelse skal være specificerede og dokumenterede.

Hvad angår it-projekter, skal krav til informationssikkerhed herunder persondatabeskyttelse indgå ved såvel nye systemer som ved forbedringer af eksisterende systemer.

Krav til informationssikkerhed herunder persondatabeskyttelse skal udarbejdes samtidig med brugerkrav og skal indgå som en styrende parameter i designet af systemet.

Sikkerhedsprofilen herunder klassifikationsgraden for et system skal fastsættes så tidligt som muligt i projektfasen.

Sikkerhedsprofilen herunder klassifikationsgraden skal revurderes i forbindelse med genudbud af systemet og ved større ændringer i forretningen, der kan medføre en ændret anvendelse af systemet. Der skal dog som minimum ske en årlig revurdering. Myndighederne skal i den forbindelse være opmærksomme på bestemmelser om klassifikation samt på behovet for en eventuel akkreditering eller re-akkreditering af systemet, jf. 8.20. Forud for en ændring af klassifikationen skal der i alle tilfælde foretages en fornyet, dokumenteret risikovurdering med en revurdering af informationssikkerhedsforanstaltningerne.

For profil B og C gælder desuden: Det skal vurderes, om der er services eller systemer, der ikke behøver internetadgang.

Sikkerhedskrav skal fremgå af sikkerhedsdokumentationen for systemet, herunder hvordan sikkerhedskravene er implementerede.

Nr.	Område
5.9	Fortegnelse over aktiver

I kapitel 2.1 i FMNBST 358-1 om informationssikkerhedsledelse og kapitel 5 i FMNBST 358-2 om risikostyring inden for informationssikkerhed er der stillet krav til kortlægning af it-services og systemer med afsæt i forretningsprocesser.

Koncerninterne leverandører af it-services og systemer skal vedligeholde en detaljeret fortegnelse over aktiver, der understøtter disse it-services og systemer, herunder over den

tekniske infrastruktur. Det skal vurderes, om informationen skal klassificeres, hvordan den opbevares sikkert, og hvem der skal have adgang til den. Adgang skal begrænses til et funktionsbetinget behov.

Krav til fortegnelse over aktiver hvad angår behandling af personoplysninger, findes i bilag 1 til FMNBST 358-1 om informationssikkerhedsledelse.

Nr.	Område
5.10	Accepteret brug af aktiver

Der skal fastlægges, dokumenteres og implementeres regler for accepteret brug samt procedurer for håndtering af information og understøttende aktiver.

Der skal i den forbindelse udarbejdes og kommunikeres instrukser for brug af systemer og netværk, herunder om brugernes ansvar og om undtagelsesvis brug af privat udstyr. Disse skal i relevant omfang også omhandle brug af internettet. Instrukserne skal omfatte såvel ansatte i koncernen som andre brugere af koncernens systemer og netværk. Reglerne for accepteret brug af netværk og systemer kan indgå i informationssikkerhedsinstrukser og/eller i systemsikkerhedsinstrukser.

Se også 8.1. For profil B og C klassificerede systemer gælder desuden: Koncernens aktiver skal behandles i overensstemmelse med den højeste klassifikationsgrad af de informationer, der er eller har været på det pågældende aktiv.

Sikkerhedsdokumentationen for systemerne skal indeholde et regelsæt om accepteret brug af systemerne.

Tilslutning af privat udstyr til klassificerede systemer er ikke tilladt.

For profil C klassificerede systemer gælder også: Brugere skal have læst og underskrevet en erklæring om overholdelse af regelsættet for brug af systemerne.

Nr.	Område
5.11	Tilbagelevering af aktiver

Medarbejdere og eksterne brugere skal aflevere alle organisationens aktiver i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.

Der skal i den forbindelse foreligge en procedure for tilbagelevering af aktiver, herunder hvor medarbejdere og eksterne brugere ved modtagelsen af aktiver forpligtes til tilbagelevering af disse ved fratrædelse, eller hvor der ikke længere er et arbejdsbetinget behov for aktiverne. Proceduren skal omfatte, hvilken funktion der skal modtage aktiverne.

Se også 7.14 om sikker bortskaffelse eller genbrug af udstyr.

Proceduren skal også omfatte krav i forhold til at sikre, at myndigheden fortsat har adgang til den for myndigheden vigtige information, der er lagret på aktiverne, herunder hvad angår journalisering.

For profil B og C gælder også: Proceduren skal omfatte kontrol af og dokumentation for, at alt udstyr er tilbageleveret.

Proceduren skal omfatte kontrol af, at der ikke sker uautoriseret informationsoverførsel i opsigelsesperioden.

Nr.	Område
5.12	Klassifikation af information

Foranstaltningen implementeres gennem bestemmelserne i kapitel 1 og 4.

Nr.	Område
5.13	Mærkning af information

Informationer skal mærkes og klassificeres efter regelsættet i kapitel 1 og 4.

Se desuden FMNBST 400-1 Mærkning og håndtering af personoplysninger, der skal mærkes "PERSONOPLYSNING, FORTROLIG – POF".

Nr.	Område
5.14	Informationsoverførsel

Der skal foreligge politikker og procedurer for informationsoverførsel samt være implementeret passende foranstaltninger med henblik på at opretholde og håndhæve informations-sikkerheden herunder persondatabeskyttelsen.

Der skal således for hvert system være fastsat regler og procedurer for, hvordan man flytter information til og fra andre systemer. Reglerne skal fremgå af det enkelte systems sikkerhedsdokumentation.

Kravet omhandler såvel informationsoverførsel internt ved en myndighed eller enhed som informationsoverførsel til og fra eksterne parter. Der skal indgås aftaler med eksterne parter om passende sikker informationsoverførsel.

Myndighederne skal vurdere behovet for klassifikation af information og anvendelse af klassificerede kommunikationsmidler, eller i øvrigt brug af TLP (Traffic light Protocol) eller tilsvarende til mærkning af information.

Hvad angår administrative systemer med e-mail programmer som eksempelvis Outlook, skal der foreligge en vurdering af, om dette skal implementeres sådan, at en e-mail ikke kan afsendes før mærkning og klassifikationsgrad er angivet i e-mailen.

For profil B og C klassificerede systemer gælder desuden: Hvad angår administrative systemer med e-mail programmer som eksempelvis Outlook, skal systemerne implementeres sådan, at en e-mail ikke kan afsendes før mærkning og klassifikationsgrad er angivet i e-mailen. Automatiserede løsninger må kun implementeres efter godkendelse fra den nationale it-sikkerhedsmyndighed.

Nr.	Område
5.15	Adgangsstyring

Der skal på grundlag af forretnings- og informationssikkerhedskrav fastlægges regler for adgangsstyring for vigtige aktiver omfattet af de enkelte ledelsessystemer for informationssikkerhed.

Adgangsstyringen skal tage højde for informationers klassifikationsgrad og for kravene til sikkerhedsgodkendelse samt følge principperne om need-to-know og need-to-use. Der skal således være overensstemmelse mellem tildeling af adgangsrettigheder og arbejdsmæssigt behov.

Krav til fysisk adgangskontrol følger af kap. 7.

Se også 5.16-5.18 samt 8.2 og 8.3 i dette kapitel.

Nr.	Område
5.16	Brugerregistrering og –afmelding

Der skal med henblik på styring af adgangsrettigheder være en til- og fratrædelsesprocedure, der omfatter identifikation, registrering og afmelding af brugere. Proceduren skal herunder omhandle nedlæggelse af brugerkonti, der ikke længere anvendes, samt ubrugte og ukendte brugerkonti. Proceduren skal også omhandle de-aktivering (pausering) af brugerkonti, der midlertidigt ikke anvendes (f.eks. hvis en medarbejder har orlov eller andet langtidsfravær).

Der skal desuden vedligeholdes en oversigt over brugere og brugerkonti.

For profil B og C gælder også: Der skal være en procedure for kontrol af eventuel uretmæssig anvendelse af konti:

- I perioden fra en opsigelse til en fratrædelse.
- Hvis en brugerkonto ikke er afmeldt umiddelbart efter en fratrædelse.

For profil C gælder desuden: Der skal som minimum halvårligt ske en kontrol af, om til- og fratrædelsesproceduren er fulgt, jf. ovennævnte krav til proceduren.

Nr.	Område
5.17	Autentifikationsinformation

Tildeling og styring af autentifikationsinformation, herunder passwords, skal ske ved en formel, dokumenteret procedure, som også skal omfatte rådgivning af brugerne om håndtering af informationen. Det skal være et krav i proceduren, at brugere følger koncernens bestemmelser og praksis ved anvendelse af hemmelig autentifikationsinformation.

For password gælder følgende minimumskrav:

- Mindst 12 karakterer i en blanding af små og store bogstaver samt specialtegn. Kravet kan fraviges på baggrund af en teknisk risikovurdering alene, hvor en implementering ikke er teknisk mulig, eller hvor anden tilstrækkelig sikkerhedsfunktionalitet er etableret, f.eks. for mobile enheder.
- Mobiltelefoner og tablets (selve enheden) må kun kunne tilgås af brugeren med en minimum 6 cifret kode eller ved biometrisk identifikation af brugeren.
- Password må ikke kunne ses på skærmen under indtastning.
- Grænsen for forsøg på log-on skal vurderes for hvert enkelt system. Brugerens adgang skal dog som minimum spærres efter 10 forsøg på log-on. Fornytt adgang skal kræve assistance fra en person med administrative rettigheder, eller hvor dette ikke vurderes nødvendigt eller muligt, anden sikker identifikation af brugerne.
- Der skal fra centralt hold kunne gennemtvinges ændring af passwords for alle konti.
- Password skal udløbe efter maksimalt 180 dage. Det nye password skal være væsentligt forskellig fra tidligere anvendte passwords.
- De 10 senest benyttede password må ikke anvendes.
- Det må ikke være muligt for en almindelig bruger selv at skifte password hyppigere end hver 24 time.

- Ved oprettelse af en bruger skal brugeren selv indtaste sit password. Alternativt skal en mekanisme tvinge brugeren til at ændre password i forbindelse med første log-on, så kun brugeren kender sit password.
- Standard passwords som eksempelvis udleveres med it-udstyr skal ændres med det samme.
- Password skal beskyttes efter reglerne for den højeste klassifikationsgrad, det giver adgang til.
- Oplåsning af en konto og udstedelse af password skal følge en dokumenteret proces, og medarbejderne skal gøres bekendt med, hvordan der kan ske oplåsning.
- Oplåsning af en brugerkonto kræver forudgående sikker identifikation af brugeren.

Der kan for profil A etableres en automatiseret password reset-proces eksempelvis vha. tilsending af engangspassword med kort gyldighed til mobiltelefon eller lignende.

Se 8.5 om brugerautentifikationsteknologier og -procedurer.

Myndigheden skal give instruks til brugerne på baggrund af ovennævnte minimumskrav til passwords og Center for Cybersikkerheds vejledning om passwords.

For profil B og C gælder også: Oplåsning af en brugerkonto må kun foretages af en person med administrative rettigheder.

For profil C gælder desuden: Hvad angår samfundskritiske systemer, må ofte anvendte eller lækede passwords ikke tillades.

Nr.	Område
5.18	Adgangsrettigheder

Der skal for alle brugertyper tildeles, gennemgås, ændres og inddrages adgangsrettigheder i henhold til kravene til adgangsstyring, se 5.15.

Der skal føres en oversigt over alle tildelte adgangsrettigheder til systemer med anførsel af unikt brugeradgangs-ID, og de forretningsansvarlige for aktiverne skal sikre, at brugernes adgangsrettigheder gennemgås med jævne mellemrum.

Der skal periodisk gennemføres stikprøvevis kontrol af brugernes faktiske adgang til systemerne i forhold til rettighederne.

Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og systemer skal inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter ændringer, herunder eksempelvis organisationsændringer eller ændringer i øvrigt i en jobfunktion. Rettigheder skal også inddrages, hvis de midlertidigt ikke anvendes.

Procedure for inddragelse af rettigheder skal indgå i den dokumenterede til- og fratrædelsesprocedure, se 5.16.

Alle aktiviteter vedrørende ændring af rettigheder skal logges.

Nr.	Område
5.19	Informationssikkerhed i leverandørforhold

Der skal implementeres en politik samt procedurer med henblik på risikostyring i relation til anvendelsen af leverandører.

Politikken kan indgå i myndighedens informationssikkerhedspolitik, jf. 5.1.

Myndigheden skal sikre, at der er en proces for risikovurdering af leverandører og disses leverancer af it-services og systemer forud for en aftaleindgåelse, samt for fastlæggelse af krav til informationssikkerhed herunder persondatabeskyttelse i leverandøraftaler, jf. 5.20. Processen skal dokumenteres og skal indgå som en del af myndighedens udbuds- og indkøbsprocedurer. Det skal overvejes, om processen skal indeholde krav, hvad angår andre typer leverancer af betydning for informationssikkerheden.

Der skal derudover implementeres relevante procedurer og passende foranstaltninger i forhold til løbende at styre risici i relation til leverandører og leverandørydelser.

Der skal herunder implementeres passende foranstaltninger i forhold til leverandørers adgang til myndighedens informationer uanset karakteren af leverandørydelser. Det gælder for hele aftaleperioden og i forhold til afvikling af samarbejdet.

Om governance hvad angår interne leverandører af it-services, se også FMIDIR 380-01 og FMIBST 380-02.

Om proceduren for opfølgning på aftalte krav se 5.22. Hvis leverandøren ikke opfylder krav til informationssikkerheden herunder persondatabeskyttelsen, skal der implementeres passende kompenserende foranstaltninger. Det gælder også, hvis der ikke i tilstrækkelig grad er aftalt krav til informationssikkerheden.

For profil C gælder også: Myndighederne skal ved indkøb og udbud af samfundskritiske systemer vurdere behovet for rådgivning fra den nationale it-sikkerhedsmyndighed.

Nr.	Område
5.20	Håndtering af informationssikkerhed i leverandøraftaler

For hver enkelt leverandør skal der på baggrund af risikovurdering fastlægges og aftales de, i forhold til karakteren af leverandørydelser, relevante krav til informationssikkerhed herunder persondatabeskyttelse. Kravene skal i relevant omfang vedrøre hele livscyklussen for netværk, systemer og andre aktiver.

Myndighederne skal i den forbindelse gennemgå og stille specifikke informationssikkerhedskrav til leverandørerne med afsæt i foranstaltningerne i kapitel 6. Kravene i kapitel 6 kan, hvad angår eksterne leverandører, fraviges på baggrund af en risikovurdering godkendt af risikoejerne i forretningen. Dette bør kun ske, hvis der kun er identificeret en ubetydelig risiko eller, hvis der enten implementeres eller stilles krav til leverandøren om implementering af passende tilsvarende og/eller kompenserende, risikoreducerende foranstaltninger.

Hvis aftaleforholdet medfører behandling af personoplysninger, skal dette fremgå af leverandøraftalen, og der skal i tillæg til aftalen indgås en databehandleraftale. Denne skal omhandle de særskilte foranstaltninger med henblik på beskyttelse af personoplysninger, som henholdsvis myndigheden, leverandøren, eventuelle underleverandører og andre relevante tredjeparter skal implementere.

Der skal som en del af leverandøraftalerne og databehandleraftalerne stilles krav til leverandøren om hurtig og sikker rapportering af hændelser og mistanke om hændelser, der har, eller kan have påvirket, eller vil kunne påvirke informationssikkerheden ift. de aftalte

ydelse. Myndighederne skal i den forbindelse være opmærksomme på eventuelle eksterne krav til rapportering, herunder hvad angår brud på persondatasikkerheden.

Det skal også aftales, hvordan hændelser håndteres af leverandøren i beredskabssituationer.

Der skal desuden stilles krav om, at leverandørerne informerer om væsentlige sårbarheder, der ikke er håndteret af leverandøren, herunder i forhold til de aftalte informationssikkerhedsforanstaltninger.

Det skal for internetvendte systemer vurderes, om der skal stilles krav til monitorering af netværkstrafik, i givet fald så vidt muligt via netsikkerhedstjenesten ved Center for Cybersikkerhed. Hvis der stilles et sådan krav, skal rapportering om hændelser også ske til Center for Cybersikkerhed.

Det skal for hvert enkelt aftaleforhold overvejes, om der, udover specifikke krav til informationssikkerhed, skal stilles et generelt krav til leverandøren om risikostyring og implementering af yderligere, passende foranstaltninger jf. best practise for informationssikkerhed herunder persondatabeskyttelse.

Hvor koncernen er ansvarlig for at stille informationssikkerhedskrav direkte til leverandører af it-drift, skal der altid udarbejdes en Service Level Agreement (SLA) eller en Operational Level Agreement (OLA) med en sikkerhedskravsspecifikation (SKS).

Der skal opretholdes et overblik over leverandører og leverandøraftaler samt over, om der er aftalt passende krav til informationssikkerhed herunder persondatabeskyttelse. Leverandørydelserne skal, herunder med henblik på risikostyring, så vidt muligt listes ud fra en prioritering i forhold til kritikalitet for forretningen.

Kravene til informationssikkerhed herunder persondatabeskyttelse i de indgåede leverandøraftaler skal gennemgås og, i overensstemmelse med gældende udbudsregler, opdateres med passende mellemrum for at sikre, at de fortsat er relevante og tilstrækkelige. Hvis en aftale ikke kan genforhandles, skal der overvejes kompenserende foranstaltninger i forhold til identificerede risici, leverandøren ikke kan forpligtes til at håndtere.

For profil B og C gælder også: Der skal for relevante typer leverandørydelser stilles et krav til leverandøren om monitorering af netværkstrafik, så vidt muligt via netsikkerhedstjenesten ved Center for Cybersikkerhed. Rapportering om hændelser skal i givet fald også ske til Center for Cybersikkerhed.

Der skal fastsættes specifikke krav i forhold til informationssikkerhedskontinuitet og it-beredskab, se også 5.29 og 5.30, herunder i forhold til at der skal foreligge reetableringsplaner for systemer, der skal holdes opdaterede, og som skal testes (såvel i forhold til restore som disaster recovery).

Det skal i forbindelse med udbudsforretningen og/eller aftaleindgåelsen påses, at leverandøren kan dokumentere overholdelsen af de fastsatte sikkerhedskrav.

Nr.	Område
5.21	Informationssikkerhed i forsyningskæden for leverandørydelser

Der skal implementeres processer og procedurer samt indgås aftaler i forhold til håndtering af informationssikkerhedsrisici forbundet med forsyningskæden for leverandørydelser.

Informationssikkerhed herunder persondatabeskyttelse forbundet med forsyningskæden for leverandørydelser skal adresseres såvel i alle procedurer som i aftaler med leverandører, jf. 5.19, 5.20 og 5.22. Det skal fremgå af leverandøraftalerne, hvilke forpligtelser leverandøren har i forhold til krav til informationssikkerhed, der skal gælde for eventuelle underleverandører.

Samarbejdet med leverandører og deres underleverandører skal i øvrigt ske i overensstemmelse med kravene i kapitel 8.

Hvad angår leverancer fra koncerninterne underleverandører, der ikke medfører driftsansvar, men alene udlevering af udstyr og/eller opsætning eller opkobling til netværk og systemer, skal forhold vedrørende informationssikkerheden håndteres i aftaler mellem leverandør og underleverandør samt på baggrund af eventuelle krav direkte fra den eller de forretningsansvarlige for de understøttende aktiver. Underleverandørerne er således ikke automatisk forpligtet til at implementere samtlige obligatoriske krav i kapitel 6. De koncerninterne underleverandører skal dog som led i deres egne forretningsmæssige risikovurderinger gennemgå og forholde sig til foranstaltningerne i dette kapitel, uagtet om der foreligger krav til informationssikkerhed fra forretningssiden eller den driftsansvarlige leverandør.

Nr.	Område
5.22	Leverandørstyring

Der skal ske en i forhold til karakteren af leverandørydelser passende overvågning, gennemgang og håndtering af ændringer i leverandørydelser samt et tilsyn med efterlevelsen af de aftalte krav.

Myndigheden skal således have en procedure for leverandørstyring med henblik på at sikre efterlevelsen af informationssikkerhedskrav og opretholdelse af informationssikkerheden herunder persondatabeskyttelsen i relation til leverandørydelserne.

Leverandøraftalerne, jf. 5.20, skal beskrive myndighedens rettigheder samt leverandører og underleverandørers forpligtelser i forhold til sikring af, at krav til informationssikkerheden herunder persondatabeskyttelsen efterleves. Der skal i den forbindelse også være stillet passende krav til leverandørers løbende sikkerhedsrapportering i forhold til leverandørydelser og de fastsatte krav til informationssikkerhed herunder persondatabeskyttelse.

For profil C gælder også: Der skal, hvad angår samfundskritiske systemer, som minimum stilles krav om systemspecifikke revisorerklæringer.

Nr.	Område
5.23	Informationssikkerhed ved brug af cloud services

Der skal etableres og dokumenteres processer for indkøb, anvendelse, styring af og exit fra cloud services i overensstemmelse med informationssikkerhedskrav og koncernfælles retningslinjer for anvendelse af cloud services.

Der skal gennemføres dokumenteret risikovurdering af cloud services inden aftaleindgåelse med cloud leverandøren. Informationssikkerhedskrav herunder krav til persondatabeskyttelse specificeres på baggrund af risikovurderingen.

Myndighederne skal være opmærksomme på eksterne krav herunder i GDPR i forhold til overførsel af personoplysninger til tredjeland.

Se også krav til informationssikkerhed herunder persondatabeskyttelse i leverandørforhold i 5.19-5.22.

Exitplan og -processer skal testes, inden cloud services ibrugtages.

Nr.	Område
5.24-5.28	Hændelsesstyring

Implementeres gennem bestemmelserne i kapitel 10 og FMNBST 280-2 Håndtering af brud på persondatasikkerheden i Forsvarsministeriets koncern.

Nr.	Område
5.29	Informationssikkerhedskontinuitet

Myndighederne skal planlægge for at kunne opretholde informationssikkerheden for forretningskritiske processer samt persondatabeskyttelsen på et passende niveau ved større hændelser.

Der skal planlægges *forebyggende* foranstaltninger for at kunne opretholde eller genoprette informationssikkerheden herunder persondatabeskyttelsen. Planlægningen skal tage afsæt i myndighedens forretningsoverblik og aktivfortegnelser. På baggrund heraf udvælges de kritiske forretningsprocesser, herunder i forhold til behandling af personoplysninger, samt understøttende it-services og systemer hertil. Kritikaliteten vurderes med udgangspunkt i en konsekvensanalyse.

Myndigheden skal herefter fastlægge kravene til:

- Tilpasning af de informationssikkerhedsforanstaltninger, der er implementeret i relation til normal drift.
- Kompenserende foranstaltninger for foranstaltninger, der ikke kan opretholdes ved større hændelser.

Foranstaltningerne med henblik på informationssikkerhedskontinuitet vil typisk først skulle implementeres eller gennemføres ved et forhøjet trusselsniveau, i forbindelse med større hændelser, eller hvor myndighedens og/eller leverandørernes beredskab er aktiveret. Der kan afhængigt af trusselsbilledet eller karakteren og omfanget af en hændelse være behov for at tilpasse såvel organisatoriske som adfærdsmæssige, fysiske og tekniske foranstaltninger.

Myndighederne skal, jf. 5.20, stille krav til leverandørers håndtering af informationssikkerhedskontinuitet.

Koncerninterne leverandører skal planlægge for samt implementere og gennemføre alle passende processer, procedurer og foranstaltninger for at sikre informationssikkerhedskontinuitet, uagtet om forretningen har stillet krav hertil. Det gælder herunder hvad angår nøddrift, retablering af systemer og data samt genoptagelse af normal drift. Krav til procedurer for hændelseshåndtering fremgår af kap. 10.

De koncerninterne leverandører skal desuden have udpeget og instrueret personale med ansvar, bemyndigelse og kompetence til at sikre den nødvendige informationssikkerhedskontinuitet.

Planer og procedurer for informationssikkerhedskontinuitet skal afprøves med jævne mellemrum for at sikre, at foranstaltningerne kan gennemføres. Afprøvningen skal som minimum ske årligt.

For profil B og C gælder også: Frekvensen for afprøvning af planer og procedurer skal fremgå af sikkerhedsdokumentationen for systemerne.

For profil C gælder desuden: Myndighederne skal, for så vidt angår samfundskritiske systemer, som led i planlægningen af forebyggende foranstaltninger til at sikre informationssikkerhedskontinuitet, gennemgå og sikre efterlevelsen af alle krav udmeldt af den nationale it-sikkerhedsmyndighed om et styrket cyberforsvar.

Nr.	Område
5.30	It-beredskab for business continuity

Myndigheden skal planlægge, implementere, vedligeholde og øve et it-beredskab. Beredskabet, som skal baseres på mål for og krav til forretnings- og informationssikkerhedskontinuitet, har fokus på tilgængelighed af understøttende it-services og systemer i beredskabssituationer. It-beredskabet skal således understøtte, at myndigheden så vidt muligt fortsat kan varetage sine opgaver i beredskabssituationer.

It-beredskabet udgør herved en vigtig del af myndighedens planlægning for forretningskontinuitet generelt, og det skal sikres, at relevant koordination med denne indsats finder sted. Relevante chefer og medarbejdere på informationssikkerhedsområdet bør i den forbindelse indgå i myndighedens beredskabs- og krisestyringsorganisation.

Konkret skal der som en del af it-beredskabet foreligge følgende beredskabsplaner:

- En plan for aktivering af myndighedens interne kriseberedskab og krisestyring i beredskabssituationer (krisestyringsplan), der involverer større it-nedbrud af de it-services og systemer, myndigheden anvender. Planen kan udgøre en del af myndighedens generelle beredskabsplan for forretningskontinuitet.
- Reetableringsplaner i forhold til den tekniske reetablering af systemer i beredskabssituationer. Dette krav gælder kun profil B og C, jf. nedenfor.

Foranstaltninger for informationssikkerhedskontinuitet, jf. 5.29, indgår i it-beredskabsplanlægningen.

Beredskabsplaner skal være tilgængelige for relevante medarbejdere, herunder offline for medarbejdere der, jf. beredskabsplanerne, har en rolle i beredskabet. Dette skal kontrolleres årligt.

Ledelsen skal sikre, jf. 6.2 og 6.3, at medarbejderne er bekendte med beredskabsplanerne, herunder at personer med en rolle i beredskabet er gjort bekendt med deres ansvar og opgaver i beredskabet. Der skal følges op på dette som minimum halvårligt.

Ledelsen skal også sikre, at beredskabsplanerne gennemgås og opdateres som minimum årligt, herunder på baggrund af øvelser og tests, samt ved større organisatoriske og/eller it-relaterede ændringer.

Der skal være en proces for, at lister med kontaktoplysninger vedligeholdes løbende og som minimum halvårligt.

For profil B og C gælder også:

Myndighedens krisestyringsplan skal indbefatte konkrete procedurer for, hvordan myndigheden vil håndtere betydelig nedsat eller manglende tilgængelighed for it-services og systemer, der understøtter forretnings- og samfundskritiske processer.

Myndigheden skal herunder også planlægge for brug af alternative, særligt sikrede kommunikationsmidler og forbindelser, herunder eksempelvis REGNEM, SINE og kredsløb til beredskabsmæssige formål samt for abonnementer på prioritet i mobilnettet. Der skal som minimum årligt følges op på planlægningen, og det skal sikres, at kommunikationsmidlerne fungerer.

Reetableringsplaner for systemer skal som minimum indeholde følgende elementer:

- Aktiviteter med henblik på reetablering af systemet.
- Sammenhæng med reetablering af øvrige it-systemer i myndighedens infrastruktur.
- Konkrete forretningskrav til maksimal reetableringstid og datatab.
- Rolle- og ansvarsfordeling.
- Beskrivelse af forholdene vedrørende aktivering og de-aktivering af reetableringsplaner.
- Kontaktoplysninger hos myndighed og leverandøren.

Der skal som minimum årligt gennemføres både tests af reetablering af data i systemerne (data restore test) og fuld reetableringstest af systemerne og data (disaster recovery test). Hvis en koncernintern leverandør af it-services og systemer ikke kan garantere tilgængelighedskravet fra forretningen med den eksisterende systemarkitektur, bør reservekomponenter- eller arkitekturer være overvejet. Der skal desuden tages stilling til forsyningssikkerhed i form af eventuel brug af alternative mobil- og internetudbydere. Se også 7.11 om forsyningssikkerhed generelt.

Nr.	Område
5.31	Identifikation af lov-, myndigheds- og kontraktkrav

Implementeres gennem kapitel 2.1 i FMNBST 358-1 om informationssikkerhedsledelse.

Nr.	Område
5.32	Immaterielle rettigheder

Der skal implementeres passende procedurer til at sikre, at der er overensstemmelse med lov-, myndigheds- og kontraktkrav i relation til immaterielle rettigheder og anvendelse af beskyttede softwareprodukter.

Immaterielle rettigheder kan f.eks. være kildekode licenser, copyrights, patenter og varemærker.

Nr.	Område
5.33	Beskyttelse af fortegnelser

Fortegnelser skal beskyttes mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse i overensstemmelse med lov-, myndigheds-, kontrakt- samt forretningsmæssige krav.

Der skal i relevant omfang fastlægges regler og gives retningslinjer for opbevaring, lagring, håndtering samt sletning af fortegnelser. Hensynet til eventuel klassifikation af samling af ellers ikke-klassificeret information i fortegnelser, herunder i databaser, skal iagttages.

Nr.	Område
5.34	Privatlivets fred og beskyttelse af personoplysninger

Privatlivets fred og personoplysninger skal beskyttes i overensstemmelse med lov-, myndigheds-, kontrakt- samt forretningsmæssige krav.

Krav til en informationssikkerhedspolitik med målsætninger for persondatabeskyttelsen, se 5.1, følger af FMNPOL 358-1.

Der skal fastlægges, dokumenteres, kommunikeres og implementeres alle nødvendige procedurer og foranstaltninger til beskyttelse af personoplysninger og udøvelse af de registreredes rettigheder.

Nr.	Område
5.35	Uafhængig gennemgang af informationssikkerhed

Foranstaltningen er implementeret gennem:

- Forsvarsministeriets tilsyn med informationssikkerhed herunder persondatabeskyttelsen.
- FE's tilsyn med militær sikkerhed.
- Den nationale it-sikkerhedsmyndigheds tilsyn.

Om styrelseres tilsyn med underliggende myndigheder og enheder se kapitel 6 i FMNBST 358-1 om informationssikkerhedsledelse.

Se også "Vejledning om databeskyttelsesrådgivere i Forsvarsministeriets koncern" om databeskyttelsesrådgiverens uafhængige tilsyn i forhold til persondatabeskyttelse.

Nr.	Område
5.36	Compliance med politikker og standarder for informationssikkerhed

Foranstaltningen om egenkontrol er implementeret gennem kapitel 5 i FMNBST 358-1 om informationssikkerhedsledelse.

Nr.	Område
5.37	Dokumenterede driftsprocedurer

Driftsprocedurer for informationsbehandlingsfaciliteter skal dokumenteres og gøres tilgængelige for alle brugere, der har brug for dem.

Der skal i relation til informationssikkerhed som minimum udarbejdes driftsprocedurer for systemer, når:

- En aktivitet skal udføres på samme måde af mange personer.
- En aktivitet skal udføres sjældent, og der er risiko for, at proceduren glemmes.
- En aktivitet er ny, og der er risiko for, at den ikke udføres korrekt.

Dokumentationen skal ledelsesgodkendes på passende niveau og holdes opdateret.

ADFÆRDSMÆSSIGE FORANSTALTNINGER

Nr.	Område
6.1	Screening

Implementeres gennem bestemmelserne i kapitel 2.

Nr.	Område
6.2	Ansættelsesvilkår og -betingelser

Kontrakter med medarbejdere skal beskrive medarbejdernes og myndighedens overordnede ansvar og forpligtelser inden for informationssikkerhed, herunder persondatabeskyttelse, og eksempelvis hvad angår tavshedspligt.

Ansvar og forpligtelser vil typisk også fremgå ved sikkerhedsgodkendelser, eller kan følge af hemmeligholdelses- og non-disclosure aftaler, se 6.6.

Den nærmeste ledelse skal sikre, at medarbejdere og eventuelle samarbejdsparter (f.eks. eksterne konsulenter) i forbindelse med tiltrædelsen af en stilling eller ny funktion orienteres nærmere om myndighedens ansvar for informationssikkerhed, herunder persondatabeskyttelse, og om de pågældendes egen rolle og ansvar på området.

For profil B og C gælder også: Udenlandsk personel, som samarbejder med typisk Forsvaret, må ikke gives adgang til nationalt klassificerede systemer. Med udenlandsk personel menes her personel ansat af udenlandske myndigheder eller virksomheder og i andre lande. Den nationale it-sikkerhedsmyndighed kan dog i helt særlige tilfælde udstede en tidsbegrænset tilladelse. En sådan tilladelse vil normalt være betinget af, at den pågældende medarbejder er sikkerhedsgodkendt af hjemlandets myndigheder, og at der eventuelt iværksættes særlige sikkerhedsforanstaltninger.

Nr.	Område
6.3	Awareness, uddannelse og træning

Ledelsen skal sikre, at al informationssikkerheds- herunder persondatasikkerhedspersonel, jf. 5.4, løbende modtager passende uddannelse og træning. Det skal ske med afsæt i dokumenterede og individuelle uddannelsesprogrammer for de enkelte medarbejdere, der varetager specifikke roller og funktioner inden for informationssikkerhed herunder persondatabeskyttelse, f.eks. informationssikkerhedsofficerer og databeskyttelsesspecialister. Det kan ske i relation til koncernens medarbejderudviklingskoncept. Uddannelsesprogrammet skal inkludere indføring i koncernens forvaltningsgrundlag for informationssikkerhed og persondatabeskyttelse.

Uddannelse og træning kan bestå i deltagelse i såvel eksterne som interne kurser og seminarer, selvstudier, øvelsesaktivitet, sidemandsoplæring etc.

Ledelsen skal derudover sikre, at alle medarbejdere (og samarbejdsparter) ved deres tiltrædelse, og herefter med passende mellemrum, modtager instruktion om informationssikkerhed herunder persondatabeskyttelse med afsæt i forvaltningsgrundlaget men med vægt på informationssikkerheds- og systemsikkerhedsinstrukser relevante for deres jobfunktion.

Forsvarsministeriet gennemfører løbende koncernfælles awareness-aktiviteter og udvikler materiale, som myndighederne kan tage afsæt i ved myndighedernes egne awareness-

aktiviteter. Awareness kan ske i form af aktiviteter som f.eks. kampagner, nyhedsmails, plakater, pop-up meddelelser, quiz eller netværksmøder. Aktiviteterne skal omhandle truselvurderinger og konsekvenser ved sikkerhedsbrud for både myndighederne og de registrerede, hvad angår personoplysninger, samt risikoreducerende foranstaltninger.

Awareness-aktiviteterne skal også omhandle information om hændelsesrapportering i relation til informationssikkerhed, herunder i forhold til mistanke om phishingmail, samtbrud på persondatasikkerheden. Der skal gennemføres awareness aktiviteter om dette som minimum årligt.

Awareness-aktiviteter skal også, når det er aktuelt, inkludere forhold om beskyttelse af klassificeret information samt klassificerede systemer og klassificeret udstyr.

Ledelsen skal sikre, at alle ansatte (herunder også ledelsen) og i relevant omfang samarbejdspartner deltager i eventuel obligatorisk koncernintern undervisning i informationssikkerhed herunder persondatabeskyttelse. Ledelsen skal ligeledes understøtte deltagelsen i awareness-aktiviteter.

Myndighederne skal følge op på deltagelsen i koncernfælles og myndighedsspecifikke awareness-aktiviteter, f.eks. ved måling, test og stikprøvekontrol om sikkerhedsbevidsthed og viden om informationssikkerhed herunder persondatabeskyttelse. Forsvarsministeriet vejleder herom og anviser i relevant omfang metodik og værktøjer hertil.

Myndighederne skal periodisk kontrollere, om medarbejderne ved, hvordan de skal rapportere om sikkerhedshændelser og mistanke om hændelser, jf. kap. 10 og myndighedens lokale informationssikkerhedsinstrukser.

For profil B og C klassificerede systemer se også krav til uddannelse inden for kryptosikkerhed og kryptoforvaltning i bilag 3 til kapitel 6.

Nr.	Område
6.4	Disciplinær processer (sanktioner)

Det skal kommunikeres til medarbejdere og andre relevante parter, at en overtrædelse af informationssikkerhedsbestemmelser herunder om persondatabeskyttelse, efter omstændighederne kan medføre strafferetslig forfølgelse. Herunder kan en overtrædelse medføre disciplinære sanktioner, ligesom det kan have betydning for sikkerhedsgodkendelsen.

Kommunikationen indgår ved sikkerhedsgodkendelse og typisk også i hemmeligholdelses- og non-disclosure aftaler, se 6.6, men skal også ske i myndighedernes interne forvaltningsgrundlag og i forbindelse med tiltrædelse, se 6.2.

Nr.	Område
6.5	Ansættelsesforholdets ophør eller ændring

Krav om ansvar og forpligtelser vedrørende informationssikkerhed efter ansættelsens ophør, herunder hvad angår tavshedspligt, vil typisk være defineret og kommunikeret i forbindelse med medarbejders og samarbejdspartners tiltrædelse, se 6.2. Ledelsen skal dog overveje at kommunikere kravene ved fratrædelsessamtaler.

Ved ændringer til en ansættelse eller en funktion, herunder navnlig en informationssikkerhedsfunktion, skal ledelsen kommunikere eventuelle ændrede informationssikkerhedsforpligtelser.

For profil C klassificerede systemer gælder også: Hvis en medarbejder eller samarbejdspart, der skal fratræde, har adgang til klassificerede profil C systemer, skal ledelsen gennemføre en fratrædelsessamtale, og herunder i den forbindelse indskærpe tavshedspligten.

Nr.	Område
6.6	Fortroligheds- og non-disclosure aftaler

Krav til eventuelle fortroligheds- eller hemmeligholdelsesaftaler, der afspejler myndigheds behov for at beskytte information, herunder personoplysninger, skal identificeres og gennemgås regelmæssigt, og aftalerne skal dokumenteres.

Fortroligheds- eller hemmeligholdelsesaftaler kan være relevante, hvor der ikke måtte være krav til en sikkerhedsgodkendelse, eller hvor denne endnu ikke er givet. Kravene i kapitel 2 og 8 skal i den forbindelse iagttages.

Nr.	Område
6.7	Fjernarbejde

Der skal gennemføres en risikovurdering af fjernadgang til et givent netværk med henblik på, at der kan implementeres passende sikkerhedsforanstaltninger for at beskytte information, herunder personoplysninger, der er adgang til, og som behandles eller lagres via fjernarbejde.

Ved fjernarbejde forstås her, at en pc kobles til et koncernnetværk fra en lokalitet uden for koncernens arbejdssteder.

I forhold til eventuel fjernadgang fra udlandet, skal der overvejes skærpede sikkerhedsforanstaltninger.

Der gælder følgende minimumsforanstaltninger:

- Fjernadgang skal ske over krypterede forbindelser, og lagrede informationer skal være krypterede. Koncernens VPN-løsninger til internetadgang skal anvendes.
- Adgang til systemet skal ske via multifaktorautentifikation.
- Udstyr skal være beskyttet mod malware.
- De systemer, der kan tilgås, skal være opdaterede.

For profil B og C gælder også: Hvor der er et krav til sikkerhedsgodkendelse af systemer og netværk, se 8.20, skal der som led i sikkerhedsgodkendelsen ske en godkendelse af fjernadgangen til klassificerede systemer af den nationale it-sikkerhedsmyndighed.

Nr.	Område
6.8	Hændelsesrapportering

Implementeres gennem bestemmelserne i kapitel 10 og FMNBST 280-2 Håndtering af brud på persondatasikkerheden i Forsvarsministeriets koncern.

FYSISKE FORANSTALTNINGER

Hvor der i det følgende er henvist til, at en foranstaltning implementeres gennem bestemmelserne i kapitel 7, gælder:

Fysiske foranstaltninger i relation til klassificerede systemer implementeres som foreskrevet i kapitel 7 samt bilag 1 og 2 til kapitel 6, afhængigt af klassifikationsgraden af de informationer, systemerne håndterer.

Hvad angår ikke-klassificerede systemer gælder:

- Profil B og C systemer beskyttes som udgangspunkt i henhold til kravene i kapitel 7 med samme fysiske foranstaltninger som - eller tilsvarende - for systemer klassificeret FTR eller højere.
- Profil A systemer beskyttes som udgangspunkt i henhold til kravene i kapitel 7 med samme fysiske foranstaltninger som - eller tilsvarende - for systemer klassificeret TTJ.

Nr.	Område
7.1	Fysisk perimetersikring

Implementeres gennem bestemmelserne i kapitel 7.

Nr.	Område
7.2	Fysisk adgangskontrol

Implementeres gennem bestemmelserne i kapitel 7.

Nr.	Område
7.3	Sikring af kontorer, lokaler og faciliteter

Implementeres gennem bestemmelserne i kapitel 7.

Nr.	Område
7.4	Overvågning af fysisk adgang

Der skal som udgangspunkt være etableret overvågning af fysisk adgang til lokaliteter. Graden og karakteren af den overvågning, der skal etableres, afhænger af kritikaliteten af de systemer, der kan tilgås på lokaliteten, og af klassifikationsgraden for systemerne. Minimumskrav til overvågning fremgår af kapitel 7.

Overvågningen skal også afhænge af omfanget af systemer samt understøttende netværk og infrastruktur på lokaliteten. Den skal desuden afhænge af omfanget og karakteren af erkendte sårbarheder for disse aktiver. F.eks. utilstrækkelig sikring mod uautoriseret adgang til systemer og netværk.

Nr.	Område
7.5	Fysiske og miljømæssige trusler

Der skal tilrettelægges og etableres beskyttelse mod naturkatastrofer og andre hændelige eller bevidste fysiske trusler mod infrastrukturen. Myndighedernes risikovurderinger i forhold til fysiske lokaliteter skal inkludere fysiske og miljømæssige trusler mod infrastruktur, og der skal implementeres passende risikoreducerende foranstaltninger.

Nr.	Område
7.6	Arbejde i sikre områder

Implementeres gennem bestemmelserne i kapitel 7 og lokale instrukser for militær sikkerhed.

Nr.	Område
7.7	Ryddeligt skrivebord og blank skærm

Skriveborde skal holdes ryddet for klassificerede og mærkede dokumenter samt flytbare lagermedier, når de forlades.

Myndighedernes informationssikkerhedsinstruks skal desuden oplyse medarbejderne om krav til brug af skærmlås, automatisk skærmlås samt mulig frakobling af pop-ups om f.eks. e-mails under præsentationer og skærmdeling etc.

Se også kapitel 1, bilag 7, om kontorsikkerhed.

Nr.	Område
7.8	Placering og beskyttelse af udstyr

Udstyr skal placeres sikkert og beskyttes. Udstyr skal således placeres og beskyttes, så risikoen for miljømæssige trusler og farer samt muligheden for uautoriseret adgang reduceres.

Informationsbehandlingsfaciliteter som myndigheden er ansvarlig for, skal så vidt muligt placeres fysisk adskilt fra faciliteter, som håndteres af andre, eksterne myndigheder eller leverandører. Hvordan det skal ske, skal afhænge af en risikovurdering.

For profil B og C klassificerede systemer se også kravene i bilag 1 og 2 samt kapitel 16 i bilag 3, Vejledning om informationssikkerhed ved håndtering af klassificeret information.

Nr.	Område
7.9	Udstyr og aktiver uden for organisationen

Anvendelsen af en myndigheds aktiver uden for koncernens lokaliteter forudsætter fastlæggelse af ansvarsforholdene i relation hertil, herunder brugernes ansvar, samt ledelsesgodkendelse på passende niveau.

Der skal fastlægges og implementeres passende sikkerhedsforanstaltninger, herunder instrukser til brugerne om sikker anvendelse af aktiverne. Instrukserne skal herunder omfatte brugernes ansvar for at skærme information mod uautoriseret indsigts. Der skal så vidt muligt anvendes privacy skærmfilter.

Kravet gælder alt koncernens udstyr og enheder, herunder mobile enheder og antenner, som lagrer eller behandler information.

Se også 6.7 om fjernarbejdspladser.

For profil C klassificerede systemer gælder også: Områder, hvor der behandles informationer klassificeret FTR eller højere, må kun indrettes efter forudgående tilladelse fra FE.

Nr.	Område
7.10	Håndtering af lagermedier

Lagermedier skal håndteres gennem hele deres livscyklus i forhold til anskaffelse, anvendelse, transport og bortskaffelse i overensstemmelse med deres klassifikation og krav til informationssikkerhed herunder persondatabeskyttelse.

Der skal udarbejdes og kommunikeres procedurer for håndtering af lagermedier til beskyttelse af lagermedier mod uautoriseret adgang, misbrug og ødelæggelse.

Lagermedier skal destrueres, når de ikke længere skal anvendes (herunder genanvendes). De skal beholde deres eventuelle mærkning og/eller klassifikation, indtil de er destrueret.

Procedurerne på området skal håndteres i overensstemmelse med bestemmelserne i kapitel 3 og 4.

Se også 7.14.

For profil B gælder også: Harddiske, der indeholder klassificeret TTJ-information, kan efter regenerering også genanvendes i ikke-klassificerede systemer. Inden genanvendelse skal der gennemføres sletning af informationer med en, af den nationale it-sikkerhedsmyndighed godkendt metode. For profil B og C klassificerede systemer gælder desuden: Alt udstyr skal mærkes i forhold til anvendelsen, f.eks. FIIN, samt klassifikation. Kryptomateriel mærkes CRYPTO jf. DAMSG 205. Harddiske og andre lagermedier skal mærkes med:

- "Forsvarets Ejendom" eller "< > ejendom"
- Klassifikationsgrad.

Den anvendte klassifikationsgrad skal svare til den højeste klassifikation af information, som er eller har været lagret på mediet.

Mærkning skal tilstræbes at ske på en sådan måde, at den ikke kan ændres uden, det er umiddelbart synligt.

Flytbare medier skal være krypteret med et, af den nationale it-sikkerhedsmyndighed godkendt produkt, når de forlader tjenestestedet.

For profil C klassificerede systemer gælder tillige: Medier skal mærkes med individuelt nummer. Nummeret skal indgå i myndighedens mønstringsgrundlag.

Et klassificeret lagermedie kan genbruges inden for samme system uden særlige forholdsregler. Et klassificeret lagermedie kan genbruges i et andet sikkerhedsgodkendt system med samme klassifikationsgrad eller højere.

Lagermedier klassificeret FTR/NC eller højere må ikke nedklassificeres.

Lagermedier klassificeret FTR/NC eller højere, der ikke længere skal anvendes, skal uanset type fremsendes til Kryptofordelingscenter Danmark med henblik på tilintetgørelse.

Der skal i forbindelse med tilintetgørelsen føres relevante journaler, og der skal udstedes et tilintetgørelsesbevis i henhold til bestemmelserne for dokumentsikkerhed.

Nr.	Område
7.11	Forsyningssikkerhed

Systemer og infrastruktur skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger. Der skal herunder implementeres passende foranstaltninger i forhold til navnlig svigt af el-, tele- og vandforsyning samt køling.

Foranstaltningerne skal i relevant omfang testes med jævne mellemrum og om nødvendigt tilpasses.

Se underbilag 2 til bilag 3 til kapitel 7 om krav til forsyningssikkerhed for Sikkerhedsnettet.

For profil B og C gælder også: Der skal overvejes etableret redundante netværksforbindelser i form af forbindelser fra mere end én udbyder på forskellige netværk samt redundant kabelføring.

Se også 5.30, idet forsyningssikkerhed skal indgå i planlægningen af et beredskab for at kunne tilgå it-services og systemer, herunder kommunikationssystemer i beredskabssituationer.

Nr.	Område
7.12	Sikring af kabler

Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, skal beskyttes mod indgreb, interferens og skader.

Indendørs kabelinstallationer:

Lokale netværk med klassifikationsniveau op til TTJ må inden for *kontrolleret område* føres i almindelige kabelbakker, når det fysiske sikringsniveau er 3-10 eller derover.

Kabelkanaler skal generelt være tilgængelige for inspektion, eller kunne forsegles for derved at beskytte kabler mod indtrængen.

Der bør uanset klassifikationsniveau anvendes fiberoptiske kabler, når der skal tages hensyn til støj- og interferensfænomener samt transmissionshastighed og rækkevidde.

Lokale netværk med klassifikationsniveau FTR og HEM må kun etableres inden for *sikret område*, jf. kap. 7. Kabler må føres i almindelige kabelkanaler, når det fysiske sikringsniveau er 2-30 eller højere. Kabler skal føres i stålrør, hvis det fysiske sikringsniveau er under 2-30.

Installation af lokale netværk med klassifikationsniveau FTR og derover skal følge vejledningen i bilag 3, Vejledning om informationssikkerhed ved håndtering af klassificeret information, kapitel 16.

Lokale netværk med klassifikationsniveau FTR og derover skal godkendes af den nationale it-sikkerhedsmyndighed som del af en installationsakkreditering.

Lokale netværk med klassifikationsniveau YHM må ikke etableres uden særlig tilladelse fra den nationale it-sikkerhedsmyndighed.

Udendørs kabelinstallationer mellem bygninger:

Føringsveje for kabler skal etableres således, at risiko for indtrængen, interferens og skader/afbrydelser minimeres. Der bør anvendes fiberoptiske kabler ved store afstande, og når der skal tages hensyn til støj- og interferensfænomener samt transmissionshastighed og rækkevidde.

Føringsvejen skal beskyttes til det sikringsniveau, der matcher den højeste klassifikation af information, der løber i kabler i føringsvejen, jf. nedenstående retningslinjer.

IKL og TTJ kan føres u-krypteret i kabelføringsveje inden for kontrolleret område.

FTR og HEM kan føres u-krypteret i kabelføringsveje inden for kontrolleret område, når der tillige er indført følgende sikringstiltag:

- Kabelbrønde skal være aflåst med låseblik og sikkerhedsgodkendt lås samt skal være overvåget med alarm jf. sikringsniveau 2-30. Se krav til alarmer og gennembrydningstid m.v. i kapitel 7.
- Kabelbrønde kan alternativt være nedgravet så brønddækslet er min. 40 cm under terræn. Da bortfalder ovenstående krav om lås og alarm.
- Trækrør skal være nedgravet minimum 75 cm under terræn og kan være lavet af plastik eller metal.
- Føringsvejen må ikke gå gennem tæt bevoksning (buskads, såt eller skov), hvor der ikke umiddelbart kan erkendes et forsøg på indtrængen.
- Indføring i bygning bør ske min. 75 cm under terræn.
- Kabel skal føres i stålrør op langs facaden nede fra min. 75 cm under terræn, hvis indføring i bygningen sker over terræn.

Der må ikke etableres udendørs endepunkter/tilslutningsmuligheder til u-krypterede FTR/HEM netværksforbindelser.

FTR og HEM informationer må aldrig fremføres u-krypteret i kabler uden for kontrolleret område.

Nr.	Område
7.13	Vedligeholdelse af udstyr

Koncernens udstyr skal vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet. Vedligeholdelsen skal som udgangspunkt ske i henhold til leverandørens anbefalinger.

Under vedligeholdelse skal der være en særlig opmærksomhed på ikke at introducere nye sårbarheder.

Inden udstyr idriftsættes efter vedligeholdelse, skal det så vidt muligt kontrolleres, at det virker efter hensigten, og at det ikke er manipuleret.

Hvis koncernens lagermedier skal bortskaffes af en leverandør eller reparatør, skal denne instrueres om sikker destruktion, se 7.10.

For profil B og C gælder også:

Hvis en vedligeholdelse finder sted på tjenestestedet af en udefrakommende reparatør, skal myndigheden sikre sig, at vedkommende er sikkerhedsgodkendt. Hvis vedkommende ikke har den fornødne sikkerhedsgodkendelse, skal arbejdet overvåges af en af myndigheden udpeget person. Den udpegede person bør så vidt muligt have fornøden indsigt i indgrebet.

Koncernens elektroniske udstyr, der behandler klassificeret information, må som udgangspunkt ikke vedligeholdes af en civil leverandør uden for tjenestestedet.

I givet fald skal leverandøren enten være fornødent sikkerhedsgodkendt eller overvåges under vedligeholdelsen. Alle lagermedier skal desuden være fjernet. Hvis vedligeholdelsen vedrører et lagermedie, skal det kontrolleres, at alle klassificerede informationer er slettet eller forsvarligt overskrevet. Det samme gælder for andet elektronisk udstyr, der skal vedligeholdes uden for tjenestestedet.

Kravene under 7.13 er at betragte som særkrav for leverandørers vedligeholdelse af udstyr, i forhold til kravene i bilag 5 til kapitel 7 om adgangs-, opholds- og udgangskontrol. Se bilag 5 hvad angår krav i øvrigt til ledsaget adgang.

Nr.	Område
7.14	Sikker bortskaffelse eller genbrug af udstyr

Inden bortskaffelse eller genbrug af udstyr med lagringsmedier, skal det verificeres, at personoplysninger og andre følsomme data samt licensbeskyttet software er slettet eller forsvarligt overskrevet. Hvis der er usikkerhed, om lagringsmedier indeholder personoplysninger, skal de håndteres, som var dette tilfældet.

Se også 7.10 hvad angår selve bortskaffelsen af lagermedier.

TEKNISKE FORANSTALTNINGER

Nr.	Område
8.1	Slutbrugerudstyr

Information og data herunder personoplysninger lagret på, behandlet af, eller som kan tilgås via slutbrugerudstyr, skal beskyttes.

Der skal fastlægges og dokumenteres regler om sikker konfiguration og håndtering af alle typer af slutbrugerudstyr, som bruges af almindelige brugere uden administratorrettigheder.

Se 8.9 om konfigurationsstyring.

Systemsikkerhedsinstrukser skal indeholde regler om brugernes adgang til at installere software på udstyret.

Lagret information på mobilt udstyr skal være krypteret. Udstyret skal være beskyttet mod malware.

Ved indkøb af nyt slutbrugerudstyr skal der, så vidt teknisk muligt, være etableret indbygget privacy skærmfilter i udstyret.

Der må på koncernens it-infrastruktur (netværk og systemer) udelukkende anvendes slutbrugerudstyr, der er udleveret i tjenstligt medfør. Dette omfatter alt slutbrugerudstyr såsom stationære og bærbare pc'er, mobiltelefoner, USB, mus og høretelefoner m.v.

Hvad angår gæstenetværk eller andre internetvendte tjenester, skal der, når der anvendes privat slutbrugerudstyr, implementeres passende sikkerhedsforanstaltninger for at reducere risici, udstyret kan introducere. Herunder om nødvendigt instrukser til brugerne.

Mobilt slutbrugerudstyr, hvori der behandles klassificeret information, skal opfylde tilsvarende krav, som gælder for mærkning, registrering, opbevaring og transport af klassificerede dokumenter, jf. kap. 4.

For profil B og C gælder også: Mobilt, klassificeret udstyr skal være godkendt af den nationale it-sikkerhedsmyndighed. Det gælder, hvor der, se 8.20, er et krav om sikkerhedsgod-

kendelse af systemer og netværk, og godkendelsen af udstyret vil som udgangspunkt ske som led i en sådan sikkerhedsgodkendelse.

Nr.	Område
8.2	Privilegerede adgangsrettigheder

Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.

Tildelingen og anvendelsen af privilegerede adgangsrettigheder skal i øvrigt ske i overensstemmelse med kravene til adgangsstyring, se 5.15, og på baggrund af en dokumenteret proces. I det følgende er der fastsat krav til processen og til foranstaltninger.

Tildelingen af privilegerede adgangsrettigheder kræver chefgodkendelse og skal så vidt muligt ske for en tidsbegrænset periode i forhold til formålet.

Privilegerede adgangsrettigheder må udelukkende tildeles dedikerede, særskilte oprettede konti, og skal kunne henføres til en sikkerhedsgodkendt person. Sikkerhedsgodkendelse af systemadministratorer skal ske til som minimum en klassifikationsgrad højere end for det system, der gives privilegerede adgangsrettigheder til.

Arbejdet med privilegerede adgangsrettigheder må kun ske med udstyr udleveret i tjenstligt medfør.

Servicekonti må kun oprettes på baggrund af godkendt sikkerhedsdokumentation (sikkerhedsmodel) og skal, hvor det er teknisk muligt, være de-aktiveret for log-on.

Passwords på privilegerede konti skal udløbe efter maksimalt 30 dage. Hvor teknisk muligt skal passwords til konti med privilegerede rettigheder være på minimum 25 karakterer. Øvrige krav til passwords se 5.17.

Det skal være dokumenteret, hvem der har hvilke privilegerede adgangsrettigheder.

Der skal med passende mellemrum, som minimum årligt og ved organisationsændringer, ske en gennemgang af adgangsrettighederne.

For profil B og C gælder også: Der skal som minimum halvårligt ske en gennemgang af adgangsrettighederne.

Nr.	Område
8.3	Begrænset adgang til information

Adgang til information, applikationer og systemer skal begrænses i overensstemmelse med kravene til adgangsstyring, se 5.15.

Der skal implementeres passende foranstaltninger til sikring af, at kun autoriserede brugere har adgang til aktiverne.

Implementering af logisk adgangskontrol skal afstemmes med de implementerede fysiske adgangskontroller.

Nr.	Område
8.4	Adgang til kildekode

Adgang og rettigheder til kildekode, udviklingsværktøjer og softwarebiblioteker skal begrænses og styres.

Ændringer til kildekode, udviklingsværktøjer og softwarebiblioteker skal være underlagt versions- og ændringsstyring.

For profil B og C gælder også:

Samme person må kun varetage en af følgende funktioner:

- Tildele adgang og rettigheder
- Godkende tildeling
- Føre kontrol med området.

Der skal tages stilling til hjemtagning af kildekode.

Nr.	Område
8.5	Sikker autentifikation

Der skal, baseret på kravene til adgangsstyring og adgangsbegrænsninger, implementeres sikre brugerautentifikationsteknologier og -procedurer.

Det skal for hvert profil A system overvejes og dokumenteres om og hvordan, der kan anvendes multifaktorautentifikation af brugerne. For internetvendte systemer og systemer hvor der gives adgang til følsomme personoplysninger, skal der anvendes multifaktorautentifikation af brugerne.

For privilegerede konti gælder det, at der altid skal anvendes multifaktorautentifikation. Kontrol af at dette sker, skal som minimum ske halvårligt.

Hvor det er teknisk muligt, skal systemet orientere brugeren om seneste log-on tidspunkt og antal mislykkede log-on forsøg siden seneste log-on.

Ved opsætning af systemer skal det sikres, at låseskærm aktiveres efter maksimalt 5 minutter.

For profil B og C gælder også: Der skal anvendes multifaktor autentifikation af brugerne.

Nr.	Område
8.6	Kapacitetsstyring

Anvendelsen af ressourcer skal løbende overvåges og justeres i forhold til den forventede udvikling i kapacitetsbehovet med henblik på at sikre systemers tilgængelighed. Der skal til brug herfor udarbejdes og vedligeholdes en kapacitetsplan for hvert system, herunder under hensynstagen til aftalte forretningskrav.

Planerne danner grundlag for overvågning og justering af kapaciteten, som bl.a. skal ske for at reducere risici i forhold til informationssikkerheden forbundet med begrænsede ressourcer, herunder hvad angår nøglepersoner og faciliteter.

Nr.	Område
8.7	Beskyttelse mod malware

Der skal på alle enheder, hvor det er teknisk muligt, være implementeret end-point beskyttelse mod malware med automatisk opdatering.

Malwarebeskyttelsen skal blokere for installation og forhindre eksekvering af malware, og/eller detektere og sætte detekteret malware i karantæne samt alarmere personel, der er tildelt ansvar for håndtering af malware.

Malwarebeskyttelsen skal ske kontinuerligt.

Ændringer i værktøjer til beskyttelse mod malware skal være underlagt ændringsstyring (Change Management), se 8.32.

For profil B og C gælder også: Der skal anvendes minimum to leverandører af forskellige typer af værktøjer til beskyttelse mod malware på dataoverførsler via datadioder.

Nr.	Område
8.8	Styring af tekniske sårbarheder

Der skal indsamles og analyseres information om tekniske sårbarheder i systemer, således at risici identificeres og de nødvendige tiltag til risikohåndtering kan identificeres og iværksættes.

Processer, procedurer samt roller og ansvar for styring og håndtering af tekniske sårbarheder skal være defineret, dokumenteret og implementeret.

Der skal foreligge en teknisk risikovurdering af alle systemer og tilhørende understøttende aktiver. Risikovurderingerne skal opdateres som minimum årligt. Ved et væsentligt skærpet trusselsbillede skal der ske umiddelbar opdatering af risikovurderingerne og om nødvendigt en opdatering af risikohåndteringsplanerne. Dokumentation herfor skal fremgå af sikkerhedsdokumentationen. Om sammenhængen til de forretningsmæssige risikovurderinger se FMNBST 358-2.

Informationssystemer skal gennemgås både reaktivt (logning, overvågning og analyse jf. kravene i 8.15 og 8.16) og proaktivt (sikkerhedstekniske analyser, simulerede angreb og øvelser med henblik på at efterprøve dækningsgrad og effektiviteten af de præventive tiltag), herunder også i forhold til persondatabeskyttelsen.

Der skal, hvad angår internetvendte systemer, som minimum årligt gennemføres sårbarhedsscanninger.

Der skal desuden udføres penetrationstest af internetvendte systemer, så vidt muligt af Center for Cybersikkerhed, før idriftsættelse og herefter med passende intervaller, som minimum ved væsentlige ændringer til systemer.

Der skal foreligge en politik for sikkerhedsopdatering, der skal revurderes som minimum årligt.

Alle systemer, klienter og slutbrugerudstyr skal holdes opdateret med sikkerhedsopdateringer (patches).

Sikkerhedsopdateringer og andre mitigerende tiltag skal testes og implementeres i henhold til dokumenterede procedurer (Change Management), se 8.32.

De koncerninterne leverandører skal være i dialog med forretningen, som udgangspunkt de forretningsansvarlige, om sårbarhedsstyringen, og informere om væsentlige sårbarheder, der ikke er håndteret. Hvad angår dialog med eksterne leverandører om sårbarhedsstyringen se 5.20.

For profil B og C gælder også: Der skal som minimum halvårligt gennemføres sårbarhedsscanninger af internetvendte systemer.

Der skal desuden generelt udføres penetrationstest af systemer, så vidt muligt af Center for Cybersikkerhed, før idriftsættelse og herefter med passende intervaller, som minimum ved væsentlige ændringer til systemer.

Nr.	Område
8.9	Konfigurationsstyring

Konfigurationer, herunder sikkerhedskonfigurationer, i hardware, software, services og netværk skal etableres, dokumenteres, implementeres, overvåges og løbende verificeres.

Der bør udarbejdes standard konfigurationstemplates (baseline) for infrastruktur-, platform- og softwarekomponenter. Disse bør versionsstyres. Afvigelser fra vedtagne templates skal chefgodkendes.

Dokumentationen for konfigurationer bør lagres i central Configuration Management Database (CMDB).

Ændringer til konfigurationer skal følge ændringsstyringen (Change Management), se 8.32.

For profil C systemer gælder også: Det skal, hvad angår samfundskritiske systemer, kontrolleres som minimum årligt, at netværksdokumentationen er korrekt og opdateret, herunder IP-adresser og domænenavne.

Nr.	Område
8.10	Sletning af information

Informationer og data gemt i it-systemer, lagringsmedier eller andet udstyr skal slettes i henhold til gældende lovgivning, og når det ikke længere er nødvendigt eller påkrævet at gemme dem.

Det skal fremgå af aftalegrundlaget med leverandøren, hvornår information og data i det givne system skal slettes. Det skal fremgå af sikkerhedsdokumentationen for et system, hvilken information og hvilke data der eventuelt må genskabes efter sletning.

Se også 8.13, hvad angår utilsigtet sletning.

Der skal kunne føres bevis for, at sletning er udført.

Se 7.14 om sikker bortskaffelse eller genbrug af udstyr.

For profil B og C gælder også: Der skal, hvor det er teknisk muligt, etableres mulighed for at slette informationer fra mistede enheder ved hjælp af "remote wipe".

Nr.	Område
8.11	Datamaskering

Datamaskering skal ske i henhold til gældende lovgivning og databehandleraftaler.

Hvad angår personoplysninger, skal det indgå i en risikovurdering, om der skal ske maskering af data under behandling, lagring og transmission.

Se 8.24 om kryptering.

Nr.	Område
8.12	Forebyggelse af datalækage

Det skal vurderes og dokumenteres, om der skal implementeres værktøjer til forebyggelse og/eller detektering af datalækage på systemer, netværk og udstyr.

For profil B og C gælder: Værktøjer til forebyggelse af datalækage skal være implementeret på systemer, netværk og udstyr, hvis der behandles vitale eller beskyttelsesværdige informationer.

Nr.	Område
8.13	Backup

Backup af informationer, software og systemer skal løbende vedligeholdes og testes i overensstemmelse med den mellem myndigheden og leverandøren aftalte politik for backup.

Der skal foreligge en dokumenteret procedure for backup, herunder for personoplysninger, som skal tage højde for revisionssletninger, aftalte reetableringsmål og omfanget af acceptabelt datatab for det pågældende system.

Der skal dokumenteret tages stilling til krav til opbevaring og fysisk beskyttelse af backup.

For profil C systemer gælder også: Det skal, hvad angår samfundskritiske systemer, kvartalsvist kontrolleres, at backups gennemføres korrekt, og at der opbevares en kopi offline. Det skal desuden afprøves kvartalsvist, om det er muligt at foretage reetablering af data fra backuppen.

Nr.	Område
8.14	Redundante informationsbehandlingsfaciliteter

Der skal implementeres tilstrækkelig redundans på udstyr, der understøtter behandling af information og data, til at opretholde den aftalte tilgængelighed.

Se også 5.30.

Nr.	Område
8.15	Logning

Alle sikkerhedsbetydende aktiviteter (for systemer, brugere og ændringer), afvigelser og hændelser skal logges. Logs skal gemmes og beskyttes, herunder integritetssikres, i henhold til gældende lovgivning.

Se også 8.16.

Det specifikke omfang af logningen, periode, roller, proces for opsætning og behandling af logs, opbevaring, sletning af information samt adgang til logs skal fastlægges og dokumenteres i de enkelte systemers sikkerhedsdokumentation.

For internetvendte tjenester og centrale interne systemer skal logs opbevares i minimum 12 måneder, medmindre lovgivning på området tilsiger andet.

Det skal med afsæt i en risikovurdering besluttes, om logning skal indbefatte registrering af adgangen til personoplysninger. Herunder i forhold til oprettelse, læsning, ændringer og sletning samt i den forbindelse, hvilken registreret persons personoplysninger, der er blevet tilgået. Ved behandling af følsomme og fortrolige personoplysninger skal der altid ske en sådan logning med registrering af adgangen til personoplysninger.

For profil C gælder også: Det skal som minimum årligt kontrolleres, at logningen fungerer korrekt.

Nr.	Område
8.16	Monitorering

Netværk, systemer og software skal monitoreres med henblik på at opdage, standse og/eller reducere følgevirkningerne af sikkerhedshændelser.

Der skal dokumenteret tages stilling til, hvad der skal indgå i en 24/7 sikkerhedsmonitorering, og i hvilket omfang der skal etableres driftsmonitorering.

Logs, se 8.15, skal analyseres.

For profil C gælder også: Hvis ikke logs sikkerhedsmonitoreres 24/7, skal det, hvad angår samfundskritiske systemer, løbende og som minimum årligt kontrolleres, at logs gennemgås jævnligt for sikkerhedshændelser.

Nr.	Område
8.17	Tidssynkronisering

Tiden i de anvendte systemer skal være synkroniseret til en enkelt, pålidelig og robust referencetidskilde for det gældende miljø. Der skal på baggrund af en risikovurdering overvejes, om der skal tilføjes en redundant referencetidskilde.

Nr.	Område
8.18	Anvendelse af værktøjer til styring af privilegerede adgange

Brugen af værktøjer, der kan omgå system- og applikationsforanstaltninger, skal begrænses og styres.

Formål og proces for tildeling af privilegerede rettigheder via værktøjerne skal fastlægges og dokumenteres. Hvor der forefindes et sådan værktøj, skal det altid anvendes på det pågældende miljø.

Ændringer skal være underlagt ændringsstyring (Change Management), se 8.32.

Nr.	Område
8.19	Installation af software

Der skal forelægge dokumenterede procedurer til styring og godkendelse af softwareinstallationer på produktionssystemer med det formål at sikre integriteten af systemerne og undgå udnyttelse af tekniske sårbarheder.

Installationer af software skal være underlagt ændringsstyring (Change Management), se 8.32.

Nr.	Område
8.20	Netværkssikkerhed

Netværk skal styres og kontrolleres for at beskytte information og data i systemer og applikationer.

Der skal foreligge opdaterede system- og netværksdiagrammer. Netværk skal segmenteres med henblik på at beskytte information og data, se 8.22. Alle services og porte, der ikke anvendes, skal lukkes.

Ved ændringer i konfigurationer i netværket skal processen for ændringer følges, og ændringerne skal dokumenteres, se krav til konfigurationsstyring i 8.9.

For profil B og C klassificerede systemer gælder også:
Klassificerede systemer må ikke forbindes til andre systemer uden godkendelse af sammenkoblingen fra den nationale it-sikkerhedsmyndighed. Ejerskabet i forhold til grænsefladen mellem systemerne skal være fastlagt og dokumenteret.

Den nationale it-sikkerhedsmyndighed skal involveres med henblik på udarbejdelse af en akkrediteringsplan og sikkerhedsgodkendelse af:

- Alle former for systemer og netværk, der skal frembringe, bearbejde, transmittere eller lagre information klassificeret FORTROLIG eller derover.
- Systemer der skal transmittere information klassificeret TIL TJENESTEBRUG over internettet og/eller mellem flere myndigheder i staten.
- Kommunikationssystemer i øvrigt til kommunikation af information klassificeret TIL TJENESTEBRUG eller højere.

Der må kun tilsluttes udstyr/enheder, der er godkendt af den nationale it-sikkerhedsmyndighed.

Nr.	Område
8.21	Sikkerhed i netværksservices

Sikkerhedsmekanismer (så som Firewalls og Intrusion Detection Systems m.v.), serviceniveauer og servicekrav på netværk skal identificeres, implementeres og monitoreres.

Ovenstående skal fremgå af alle aftaler, der omhandler netværksservices, uanset om disse leveres af en intern eller ekstern leverandør.

For profil C gælder også: Det skal, hvad angår samfundskritiske systemer som minimum årligt kontrolleres, at firewallregler er konfigureret i overensstemmelse med det aktuelle behov for nødvendig netværkstrafik.

Nr.	Område
8.22	Netværkssegmentering

Brugervendte services, back-end services, klienter og privilegerede services skal opdeles i selvstændige segmenter.

Det skal som led i en dokumenteret risikovurdering overvejes, hvor det er teknisk og funktionelt muligt, at flytte systemer og/eller brugere til eget segment for at separere kritiske eller sårbare systemer fra andre segmenter.

Management aktiviteter på infrastrukturkomponenter og services skal altid ligge i eget segment. Det vil sige, at tilgangen til særlige management services/porte ikke må kunne tilgås fra det normale, brugervendte netværk.

Se også foranstaltningerne under 8.20.

Nr.	Område
8.23	Webfiltrering

Adgang til eksterne websites fra slutbrugerudstyr skal styres for at begrænse eksponering fra ondsindet indhold.

Der skal således ske manuel eller automatiseret blokering af adgangen til hjemmesider med kendt ulovligt indhold, virus eller phishing materiale.

Der skal derudover i relation til blokering af adgange, fastlægges og anvendes dynamiske, skalerbare eksponeringskriterier. Håndtering af afvigelser fra kriterierne skal ske iht. dokumenterede procedurer.

Nr.	Område
8.24	Anvendelse af kryptografi

Der skal fastlægges og implementeres regler for anvendelse af kryptografi til beskyttelse af information, herunder personoplysninger, i henhold til gældende lovgivning samt rets- og myndighedspraksis.

Der skal være fastlagt og dokumenteret procedurer for administration af kryptonøgler i hele deres livscyklus (inkl. opbevaring og bortskaffelse).

For profil B og C klassificerede systemer gælder også: Transmission af information må kun finde sted under anvendelse af en kryptografisk metode godkendt af den nationale it-sikkerhedsmyndighed.

Se også kravene til kryptosikkerhed i bilag 3, Vejledning om informationssikkerhed ved håndtering af klassificeret information.

Nr.	Område
8.25	Sikker udviklingscyklus (model/-proces)

Der skal fastlægges, dokumenteres og anvendes regler for udvikling, herunder nyudvikling og forbedringer, af software og systemer, herunder i relation til persondatabeskyttelse. Se kravene i 5.8, 5.32 og 8.26-8.31.

Udvikling af systemer og software skal således generelt ske i overensstemmelse med best practice for sikker udvikling herunder under hensyntagen til Security & Privacy by Design and by Default principperne.

Nr.	Område
8.26	Applikationssikkerhed

Der skal identificeres, specificeres og godkendes krav til informationssikkerhed herunder persondatabeskyttelse inden udvikling eller indkøb af applikationer.

Sikkerhedskrav skal indgå i kravene til nye applikationer og forbedringer af eksisterende.

For profil B og C klassificerede systemer gælder også: Software til brug for sikkerhedsgodkendte systemer skal være godkendt af den nationale it-sikkerhedsmyndighed. Dette omfatter sikkerhedssoftware og større opdateringer af software, der indgår i sikkerhedsgodkendelsen for systemet.

Nr.	Område
8.27	Sikkerhed i arkitekturudvikling

Der skal anvendes principper, jf. 8.25, for udvikling af sikre løsninger. Principperne skal omfatte alle udviklingsaktiviteter og arkitekturlag.

De anvendte teknologier skal risikovurderes, og risici skal håndteres efter en risikohåndteringsplan.

Nr.	Område
8.28	Principper for sikkerhed i softwareudvikling (Sikker kodning)

Der skal anvendes og dokumenteres principper for sikker kodning ved softwareudvikling. Principperne skal anvendes såvel i planlægningsfasen og før kodning, som i forbindelse med kodning og efter kodningen er idriftsat.

Nr.	Område
8.29	Sikkerhedstest

Der skal være fastlagt, dokumenteret og implementeret processer for sikkerhedstests i arbejdet med udvikling.

Sikkerhedstestene skal sikre, at informationssikkerhedsforanstaltninger og foranstaltninger til persondatabeskyttelse er effektivt implementeret i produktionsmiljøet. De skal gennemføres såvel ved nyetablering af systemer som ved opgradering og installation af nye versioner af software.

Der skal som minimum foretages en sårbarhedsscanning før idriftsættelse af systemer. Hvad angår internetvendte systemer, skal sårbarhedsscanninger følges op med penetrationstests, der så vidt muligt skal foretages af Center for Cybersikkerhed.

Resultater af tests skal kommunikeres til den forretningsansvarlige myndighed til brug for eventuel opdatering af risikobilledet og risikohåndteringsplanen.

For profil B og C gælder også: Sårbarhedsscanninger skal følges op med penetrationstests, der så vidt muligt skal foretages af Center for Cybersikkerhed.

For profil C klassificerede systemer gælder også: Der skal fastlægges krav til sikkerhedstest i akkrediteringsprocessen.

Nr.	Område
8.30	Outsourcet udvikling

Outsourcet udvikling skal styres, monitoreres og gennemgås. Der skal således føres tilsyn med og ske overvågning af systemudviklingsaktiviteter, der er outsourcet. Dette skal ske med afsæt i en sikkerhedskravspecifikation (SKS), hvor der er et krav om en sådan.

For profil C klassificerede systemer gælder også: Der skal fastlægges sikkerhedskrav til udviklingsmiljøet i akkrediteringsplanen.

Nr.	Område
8.31	Adskillelse af udviklings-, test- og produktionsmiljø

Miljøer for henholdsvis udvikling, test og produktion skal være adskilte og sikrede, for at beskytte produktionsmiljøet mod uautoriserede ændringer forårsaget af udviklings- og testaktiviteter.

Nr.	Område
8.32	Change Management (Ændringshåndtering)

Alle ændringer til informationsbehandlingsfaciliteter og systemer skal være underlagt en dokumenteret Change Management proces.

Change Management processen skal omhandle niveau for godkendelse af ændringer, dokumentation af ændringer, forudgående test og kvalitetskontrol.

Der skal desuden fastlægges og dokumenteres understøttende procedurer for håndtering af ændringer, herunder for eventuel godkendelse af konkrete ændringer.

Der skal gennemføres idriftsættelsestest af væsentlige ændringer, herunder test af fall-back.

Nr.	Område
8.33	Testdata

Testdata skal udvælges omhyggeligt og skal beskyttes og styres.

Personoplysninger bør som udgangspunkt ikke anvendes til testformål.

Testdata, der tager afsæt i produktionsdata, skal beskyttes på samme måde som produktionsdata. Anvendelse af testdata fra produktionsmiljøet kræver særskilt ledelsesgodkendelse hver gang.

Sensitive data, herunder følsomme personoplysninger, skal maskeres.

For profil C klassificerede systemer gælder også: Der skal fastlægges krav til testdata i akkrediteringsplanen.

Nr.	Område
8.34	Beskyttelse af systemer under audit

Test som led i tilsyn samt lignende kvalitetstest og undersøgelser af systemer skal være planlagt og aftalt med den relevante ledelse i såvel it-organisationen som forretningen.

Aftalen skal indbefatte et eventuelt behov for logning og overvågning af adgange samt oprydning (herunder sletning af adgange).

OVERSIGT OVER KRAV TIL FYSISK SIKRING AF IT-HARDWARE¹

Klassifikation	Områdekategori / Sikringsniveau	Bemærkninger	Henvi- sning i FKOBST 358-1, underbilag 1 til bilag 1 til kapitel 7
Aktive stik i væg og IP-telefoner			
TTJ	3-10		Figur 2.3.
TTJ	4-30	Krav til reaktion 30 min.	Figur 2.1.
FTR/HEM	2-30		Figur 2.5.
IT-arbejdsstationer inkl. USB og CD-rom			
TTJ	3-10	Harddisk kan være monteret i pc	Figur 2.3.
TTJ	4-30	Harddisk kan være monteret i pc, krav til reaktion 30 min.	Figur 2.1.
FTR/HEM	2-30	Udtagelig harddisk skal opbevares i opbevaringsmiddel klasse A, jf. EN1143-1 Grade 1	Figur 2.5.
FTR/HEM	2-40	Udtagelig harddisk skal opbevares i opbevaringsmiddel klasse B eller tilsvarende	Figur 2.6.
FTR/HEM	1-50	Harddisk kan være monteret i pc	Figur 2.7.
VTC-udstyr			
TTJ	3-10		Figur 2.3.
TTJ	4-30	Krav til reaktion 30 min.	Figur 2.1.
FTR/HEM	2-30	Kun autoriseret adgang til mødelokale. Mødelokale holdes aflåst i arbejdstiden og styres med ADK med mindre alle ved myndigheden er adgangsberettiget, og der i øvrigt er etableret en 2-30 løsning som skalsikring.	Figur 2.5.
Printere			
TTJ	3-10		Figur 2.3.
TTJ	4-30	Krav til reaktion 30 min.	Figur 2.1.
FTR/HEM	2-40	Store printere placeret på gulvet	Figur 2.6.
FTR/HEM	1-50	Bordprintere med hukommelse	Figur 2.7.
Servere			
IKL	3-10	Såfremt systemet er karakteriseret som kritisk eller vitalt for enheden, skal det opbevares som minimum TTJ (En risikovurdering må vise om det skal opbevares højere).	Figur 2.3.
TTJ	2-30	Skal låses i rackskab	Figur 2.5.
FTR/HEM	2-30	Server skal opbevares i opbevaringsmiddel klasse A (Serversafe), jf. EN1143-1 Grade 1. Krav til reaktionstid 5 min.	Figur 2.5.
FTR/HEM	2-40	Server skal opbevares i opbevaringsmiddel klasse A (Serversafe), jf. EN1143-1 Grade 1	Figur 2.6.
FTR/HEM	1-50	Server skal opbevares i aflåst rackskab	Figur 2.7.

¹ CFCS kan dispensere for kravene i skemaet efter en konkret vurdering af aktivets fortrolighed

Klassifikation	Områdekategori / Sikringsniveau	Bemærkninger	Henvisning i FKOBST 358-1, underbilag 1 til bilag 1 til kapitel 7
Datacenter²	1-60	Server skal opbevares i aflåst rackskab. Redundant datacenter skal etableres.	Figur 2.8.
Krydsfelter og netværksudstyr (routere, switche m.v.)			
TTJ	3-10	Gælder for unmanaged (dumb) udstyr (ældre udstyr som ikke længere bør anvendes)	Figur 2.3.
TTJ	2-30	Gælder for managed (intelligent) udstyr. Såfremt alle er medarbejdere er sikkerhedsgodkendt til minimum FTR, kan 2-30 løsningen etableres i skalsikringen. Krav til reaktion 30 min.	Figur 2.5.
FTR/HEM	2-30	Udstyr skal opbevares i opbevaringsmiddel klasse A (Serversafe), jf. EN1143-1 Grade 1	Figur 2.5.
FTR/HEM	2-40	Udstyr skal opbevares i opbevaringsmiddel klasse B eller tilsvarende	Figur 2.6.
FTR/HEM	1-50	Udstyr skal opbevares i aflåst rackskab	Figur 2.7.
Nøglet eller tidligere nøglet kryptoudstyr			
TTJ	2-30	Bør placeres i opbevaringsmiddel klasse B eller tilsvarende. Krav til reaktion 30 min.	Figur 2.5.
TTJ	4-30	SVN skibe i havn og HJV enheder. Krav til reaktion 15 min.	Figur 2.1.
FTR/HEM	2-40	Udstyr skal opbevares i opbevaringsmiddel klasse A (Serversafe), jf. EN1143-1 Grade 1	Figur 2.6.
Kryptonøglemateriel (Nøgler/koder)			
TTJ	2-30	Koder skal opbevares i opbevaringsmiddel klasse A, jf. EN1143-1 Grade 1	Figur 2.5.
FTR/HEM	2-40	Koder skal opbevares i opbevaringsmiddel klasse A, jf. EN1143-1 Grade 1	Figur 2.6.
CCI³ og Sensitivt udstyr			
	2-30	Komponenter skal placeres i opbevaringsmiddel klasse B eller tilsvarende. Krav til reaktion 15 min.	Figur 2.5.
	2-40	Komponenter kan placeres direkte i rummet. Krav til reaktion 15 min.	Figur 2.6.
TEMPEST udstyr			
	2-30	Komponenter kan placeres direkte i rummet. Krav til reaktion 30 min. Ibrugtaget TEMPEST-udstyr skal som minimum overholde opbevaringskrav til gældende klassifikation.	Figur 2.5.
Note: Såfremt der er it-aktiver, der bruger køleanlæg, skal der udarbejdes en risikovurdering for om tab af tilgængeligheden af data kan accepteres.			

² Datacenter med flere HEM-systemer³ CCI-materiel (Controlled Cryptographic Item eller Controlled Comsec Item). Til denne kategori hører kryptoudstyr, komponenter, tilbehør og reservedele hertil, der i stedet for klassifikationsmærkning er mærket CCI.

ELEKTRONISKE INFORMATIONSSYSTEMER OG ANDET ELEKTRONISK UDS- STYR I OMRÅDER, HVOR DER BEHANDLES KLASIFICERET INFORMATION

Dette bilag uddyber kravene i afsnit II om benyttelse af udstyr.

I dette bilag bruges RØDT område om et område, der er godkendt til alle former for behandling af information ikke klassificerede og klassificeret op og med HEMMELIGT.

RØDE områder skal være:

- fysisk sikret område kategori 1 eller 2, dvs. som minimum kategori 2¹,
- TEMPEST-zonet² således, at der elektronisk kan behandles information klassificeret til FORTROLIGT og HEMMELIGT.

GENERELT

RØDE områder er inddelt i tre klasser og kan etableres med deraf følgende forskellige muligheder for anvendelse af elektroniske informationssystemer og andet elektronisk udstyr.

Nedenstående krav til de tre klasser er minimumskrav, som afspejler tre niveauer af krav til fortrolighed. På grundlag af en konkret risikovurdering kan den informationssikkerhedsansvarlige chef fastsætte højere krav.

Den informationssikkerhedsansvarlige chefs fastsættelse af klasse og anvendelse af elektroniske informationssystemer og andet elektronisk udstyr skal i hvert enkelt tilfælde godkendes af it-sikkerhedsmyndigheden.

Områderne skal være synligt mærket i overensstemmelse med den pågældende klasse. Områder og deres anvendelse skal være beskrevet i styrelsen eller myndighedens sikkerhedsinstruks.

Flytning af godkendt elektronisk udstyr inden for området kan kun ske med godkendelse fra SIKOF eller IT-SIKOF.

RØDT område klasse A

Klasse A etableres, hvor behandling af information klassificeret til FORTROLIGT og HEMMELIGT er stærkt begrænset, og hvor der ikke er identificeret særlige beskyttelsesbehov på baggrund af it-risikovurderingen.

1. Der må ikke tales om forhold, der er klassificeret højere end TIL TJENESTEBRUG i klasse A.
2. Der må fremvises visuelle informationer klassificeret op til og med HEMMELIGT.
3. Alle former for elektroniske informationssystemer og andet elektronisk udstyr i klasse A til behandling af information klassificeret til FORTROLIGT og HEMMELIGT skal være faste installationer og sikkerhedsgodkendt af it-sikkerhedsmyndigheden.

¹ Der henvises til FKOBST 358-1, kapitel 7, afsnit 6.1.2 for krav til kategori 2 område og til kapitel 7, afsnit 6.1.1 for krav til kategori 1.

² Et sådan område skal forstås som det tredimensionelle rum, som er udpeget anvendt til installation af informationsudstyr til behandling af **ikke-krypteret klassificeret information**, klassificeret til FORTROLIGT og HEMMELIGT. Udstyret omfatter tilhørende faciliteter til alle former for drift af dette særlige informationsbehandlingsudstyr.

4. Informationssystemer og andet elektronisk udstyr til behandling af højere klassificeret information skal være afskærmet mod utilsigtet indblik fra ikke-sikkerhedsgodkendte enheder i området.
5. Der må medbringes mobile enheder som f.eks. mobiltelefoner, tablets og bærbare computere, der ikke er sikkerhedsgodkendt.
6. Respektafstande i henhold til den til enhver tid gældende SDIP-29 mellem udstyr, herunder mobilt udstyr, kabler mv. skal overholdes.

RØDT område klasse B

Klasse B etableres, hvor behandling af højere klassificeret information som udgangspunktet er begrænset, og hvor der er behov for et differentieret sikkerhedsniveau.

1. Den tilstedeværende leder i klasse B kan tillade, at der medbringes mobile enheder som f.eks. mobiltelefoner, tablets og bærbare computere, der ikke er sikkerhedsgodkendt. Når det ikke-sikkerhedsgodkendte udstyr befinder sig i området, må der ikke tales om forhold, der er klassificeret højere end TIL TJENESTEBRUG. Det skal ved tydelig markering fremgå, hvornår der kan tales om forhold der er højere klassificeret.
2. Der må samtidig fremvises visuelle informationer klassificeret op til og med HEMMELIGT.
3. Alle former for elektroniske informationssystemer og andet elektronisk udstyr i klasse B til behandling af information klassificeret til FORTROLIGT og HEMMELIGT skal være faste installationer og sikkerhedsgodkendt af it-sikkerhedsmyndigheden.
4. Informationssystemer og andet elektronisk udstyr til behandling af højere klassificeret information skal være afskærmet mod utilsigtet indblik fra ikke-sikkerhedsgodkendte enheder i området.
5. Respektafstande i henhold til den til enhver tid gældende SDIP-29 mellem udstyr, herunder mobilt udstyr, kabler mv. skal overholdes.
6. Hvis lederen forlader området skal dette sikkerhedsansvar formelt overdrages til en anden.

RØDT område klasse C

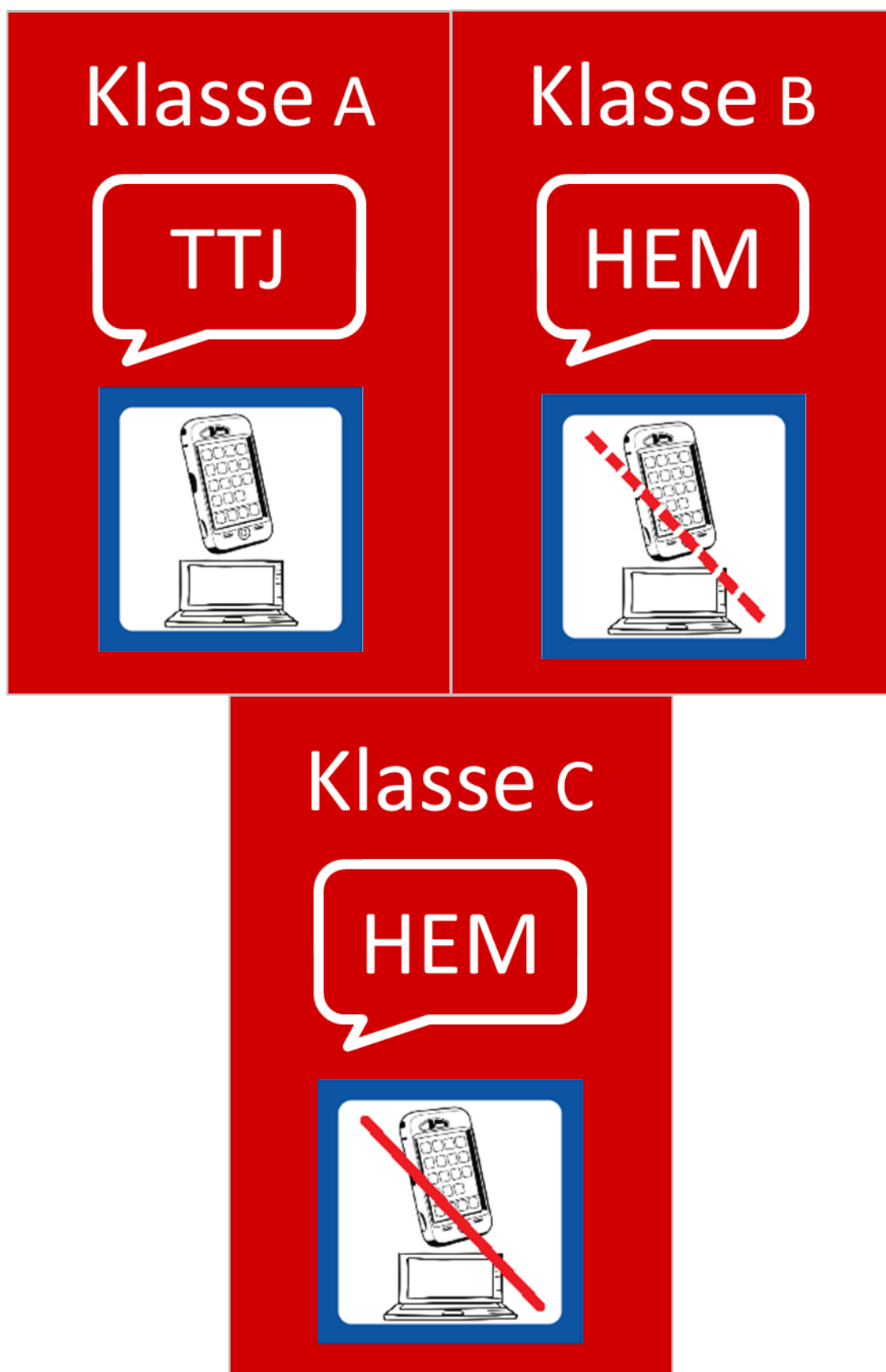
Klasse C etableres, hvor der er behov for behandling af højere klassificeret information i alle former, og hvor risikovurderingen viser behov for et højt sikkerhedsniveau.

1. Der må tales og fremvises audiovisuelle informationer der er klassificeret op til og med HEMMELIGT.
2. Alle former for elektroniske informationssystemer og andet elektronisk udstyr, der befinder sig i klasse C, - uanset om der behandles klassificeret eller ikke-klassificeret information - skal sikkerhedsgodkendes af it-sikkerhedsmyndigheden.
3. Respektafstande i henhold til den til enhver tid gældende SDIP-29 mellem udstyr, kabler mv. skal overholdes, med mindre området er godkendt som en "TEMPEST RØD Ø".

Overblik over RØDE områdeklasser

Klas- se	Fysisk sikring	Faste installa- tioner	Tilstedevæ- rende leder	Der må tales op til og med		Af- skærm- ning mod indsigt	Der må vises	
A	Kategori 1 og 2	Godken- des af FE	N/A	TTJ		Ja	På udstyr der ikke er afskær- met mod indblik	TTJ
							På udstyr der er afskærmet imod indblik	HEM
B	Kategori 1 og 2	Godken- des af FE	Skal god- kende brug af udstyr, som ikke er sikkerheds- godkendt	Hvis mobile enheder	TTJ	Ja	På udstyr der ikke er afskær- met mod indblik	TTJ
				Hvis ingen mobile en- heder	HEM		På udstyr der er afskærmet imod indblik	HEM
C	Kategori 1 og 2	Godken- des af FE	N/A	HEM		N/A	HEM	

Eksempler på skiltning



VEJLEDNING OM INFORMATIONSSIKKERHED VED HÅNDTERING AF KLASIFICERET INFORMATION

Kapitel 1

Formål og anvendelsesområde

1. I henhold til aftaler indgået mellem Danmark og internationale organisationer, er Danmark forpligtet til at sikkerhedsbeskytte klassificerede informationer efter disse organisationers regelsæt og udøve den til regelsættene hørende kontrolfunktion. Danmarks forpligtelser er overordnet beskrevet i "Cirkulære om sikkerhedsmæssig beskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt"¹ ([sikkerhedscirkulæret](#)).

Denne vejledning supplerer sikkerhedscirkulæret, og er således underlagt cirkulæret i relation til sikkerhedsforanstaltninger til beskyttelse af klassificeret information og bør anvendes i sammenhæng med cirkulæret.

Vejledningen giver nærmere anvisninger til de informationssikkerhedsforanstaltninger, som skal gennemføres for at efterleve Danmarks internationale forpligtelser med henblik på at sikkerhedsbeskytte klassificeret information. Vejledningen kan også anvendes i relation til beskyttelse af andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt.

2. Vejledningen beskriver konkret NATO og EU's krav til sikkerhedsforanstaltninger i relation til håndtering af kryptoudstyr, kryptografiske nøgler og andet kryptomateriale samt krav til TEMPEST-foranstaltninger, der skal nedsætte risikoen for kompromittering af klassificeret information som følge af elektromagnetisk udstråling eller bortledning. Vejledningen beskriver desuden krav og anbefalinger vedrørende tekniske sikkerhedseftersyn og lyddæmpning for at undgå aflytning af tale og anden akustisk formidling af klassificeret information.

Vejledningen beskriver også Forsvarets Efterretningstjenestes Center for Cybersikkerheds (CFCS) opgaver og anbefalinger på områderne som national it-sikkerhedsmyndighed, kryptosikkerhedsmyndighed og TEMPEST-myndighed.

3. Vejledningen henvender sig til alle offentlige myndigheder samt alle offentlige og private institutioner og virksomheder, som behandler klassificerede informationer i henhold til sikkerhedscirkulæret og modtager kryptoudstyr og andet kryptomateriale og/eller TEMPEST-udstyr fra Kryptofordelingscenter Danmark (NDA DNK). Vejledningen indeholder endvidere procesbeskrivelser og kontaktoplysninger til CFCS i relation til de enkelte emner.

¹ Cirkulære nr. 10338 af 17/12/2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt.

Kapitel 2

Organisering på kryptoområdet

4. CFCS har som national it-sikkerhedsmyndighed og national kryptosikkerhedsmyndighed bl.a. til opgave at:

- Godkende og underskrive bilaterale eller multinationale aftaler, der involverer nationalt kryptoudstyr og kryptonøgler.
- Indarbejde NATO og EU's kryptosikkerheds- og forvaltningsmæssige forskrifter i nationale sikkerheds- og forvaltningsmæssige bestemmelser.
- På vegne af NATO og EU føre tilsyn med, at NDA DNK overholder NATO og EU's bestemmelser om kryptosikkerhed og kryptoforvaltning, idet NATO's Office of Security også fører et vist tilsyn.
- Autorisere og godkende nationalt fremstillede high-grade kryptonøgler.
- Godkende placering af elektroniske kryptonøglefordelingscentre og produktionscentre.
- Godkende installationer af kryptoudstyr.
- Godkende kryptoplaner for nationale kryptonet.
- Godkende anvendelse af krypteringssoftware, der ønskes implementeret i nationale kryptosystemer og kryptonet.
- Sikre, at der i forbindelse med godkendelser opnås interoperabilitet mellem nationale samt NATO- og EU-systemer, hvor det er nødvendigt.
- Godkende kryptoudstyr/-systemer, der omfatter alle nationale klassifikationsgrader under forudsætning af, at de kun skal kryptere informationer med nationale klassifikationsgrader.
- Godkende kryptoudstyr/-systemer, der omfatter NATO-klassifikationsgrader til og med NATO CONFIDENTIAL.
- Godkende kryptoudstyr/-systemer, der omfatter EU-klassifikationsgrader til og med EU CONFIDENTIAL.
- Føre tilsyn i relation til de it- og kryptosikkerhedsmæssige foranstaltninger, Danmark skal gennemføre for at efterleve internationale forpligtelser med henblik på at sikkerhedsbeskytte klassificeret information.
- Rådgive om kryptosikkerhed og evaluere rapporterede brud på kryptosikkerheden.

5. Forsvarsministeriets Materiel- og Indkøbsstyrelse (FMI) varetager følgende opgaver:

- Indstiller til CFCS om sikkerhedsgodkendelse af værksteder og laboratorier, der skal kontrollere og reparere kryptoudstyr.
- Teknisk og økonomisk rådgivning i forbindelse med projektering, anskaffelse, installation og drift af kryptoudstyr.
- Indkøb af kryptoudstyr og software i samarbejde med CFCS. Førstegangsanskaffelse af kryptoudstyr skal være godkendt af CFCS inden aftaleindgåelse med leverandøren. Når udstyret er indkøbt, fordeles det via NDA DNK efter en kryptoplan, som CFCS har godkendt.
- Udgivelse af betjeningsvejledninger for kryptoudstyr i samarbejde med relevante uddannelsesinstitutioner. Det sikkerhedsmæssige indhold koordineres med CFCS.
- Udfærdigelse og vedligeholdelse af den nationale kryptoforvaltningsbestemmelse (DAMSG 205), som CFCS skal godkende efter indstilling fra FMI.

6. NDA DNK indgår organisatorisk i FMI. NDA DNK varetager Danmarks funktion som National Distribution Authority over for NATO og EU. NDA DNK har følgende

hovedopgaver, som varetages i overensstemmelse med DAMSG 205², jf. NATO og EU's instrukser i henholdsvis SDIP-293/1 og TECH-I-01:

- Fremstilling af nationale kryptonøgler på baggrund af en af CFCS godkendt kryptoplan.
- Modtagelse og distribution af alle kryptomaterialer fra NATO, EU og bilaterale partnere til nationale kryptoforvaltninger.
- Central regnskabsførelse (Central Office of Record) med alle kryptonøgler og kryptoudstyr ved nationale kryptoforvaltninger.
- Uddannelse af kryptokustodepersonale i nationalt Electronic Key Management System (EKMS). Uddannelse skal ske i koordination med Føringsstøtteregimentet.
- Årlig revision af alle kryptoforvaltninger.
- Bortskaffelse/destruktion af alt nationalt ejet kryptoudstyr. Destruktionssystem og processer skal godkendes af CFCS.
- Returnering eller destruktion af NATO og EU ejet kryptoudstyr på instruktion fra NATO eller EU.
- Destruktion af alle bærbare lagermedier, der er klassificerede FORTROLIGT/NATO CONFIDENTIAL/EU CONFIDENTIAL eller højere. Destruktionssystem og processer skal godkendes af CFCS.

Kapitel 3

Etablering af en kryptoforvaltning

7. Myndigheder m.fl., jf. pkt. 3, der skal tildeles kryptoudstyr og andet kryptomateriale, skal etablere en lokal kryptoforvaltning. Inden etableringen skal følgende iværksættes og implementeres:

- Udpegning, sikkerhedsgodkendelse og uddannelse af kryptopersonalet, jf. kap. 4 nedenfor.
- Udarbejdelse af en lokal, skriftlig kryptosikkerhedsinstruks, herunder som minimum med en beskrivelse af sikkerhedsorganisation og ansvarsforhold samt procedurer for modtagelse, afsendelse, opbevaring, transport, destruktion og nødfaldsdestruktion af kryptomateriale.
- Eventuelt nødvendige bygningsmæssige foranstaltninger samt anskaffelse af opbevaringsmidler, jf. kap. 7 nedenfor.
- Anskaffelse af destruktionsmidler, jf. kap. 13 nedenfor.
- Etablering af kontakt til en kurertjeneste, jf. kap. 10 nedenfor.

8. Herefter skal CFCS anmodes om tilladelse til etablering af kryptoforvaltningen, og NDA DNK skal underrettes. Anmodningen skal indeholde oplysninger om:

- Sikkerhedsgodkendt, uddannet kryptopersonale.
- Bekræftelse af, at procedurer for kryptotjenesten, jf. den lokale kryptosikkerhedsinstruks, er implementeret.
- Bekræftelse af, at de nødvendige bygningsmæssige sikringsforanstaltninger er implementeret.

² Forkortelsen DAMS står for Danish Allied Military Security, hvilket betyder, at den pågældende kode er produceret og kontrolleres af en dansk myndighed. DAMS skal altid følges op af et eller flere bogstaver, som indikerer, hvilket anvendelsesområde koden har. Den efterfølgende talrække er kodens identitet og identificerer samtidig, hvilken kryptoplan koden tilhører. NATO-nøgler er altid mærket med AMS.

- Bekræftelse af, at de nødvendige opbevaringsmidler til kryptoudstyr og -nøgler er til rådighed.
- Bekræftelse af, at de nødvendige destruktionsmidler er til rådighed.
- Underskriftskort, der rekvireres fra og sendes eller afleveres til NDA DNK i udfyldt stand.

Anmodningen med ovennævnte informationer bør som minimum klassificeres TIL TJENESTEBRUG.

9. Inden CFCS kan godkende anmodningen, skal der foretages et eftersyn af den fysiske sikkerhed, jf. kap. 7 nedenfor.

10. Når CFCS har godkendt anmodningen, sender NDA DNK de nødvendige hjælpemidler til vedkommende myndighed, institution eller virksomhed og meddeler CFCS det tildelte kryptoforvaltningsnummer. Herefter modtager organisationen kryptoudstyr og -materiel i henhold til de kryptoplaner, organisationen indgår i.

11. Når kryptoudstyret er modtaget, skal CFCS udstede en installationsgodkendelse, jf. kap. 8 nedenfor, for så vidt angår anvendelsen af stationært udstyr ved permanente installationer.

12. Opretholdelse af tilladelsen fra CFCS til kryptoforvaltning samt modtagelse af kryptoudstyr og andet kryptomateriel fra NDA DNK forudsætter overholdelse af NATO og EU's bestemmelser om kryptosikkerhed, som i det væsentligste er indeholdt i denne vejledning, samt de sikkerheds- og forvaltningskrav, der er fastsat i DAMSG 205.

13. Nedlæggelse af en kryptoforvaltning skal ske i henhold til DAMSG 205, jf. kap. 3.

Kapitel 4

Kryptopersonalet

14. Ved myndigheder m.fl., jf. pkt. 3, hvor der skal oprettes en kryptoforvaltning og føres kryptoregnskab, skal der udpeges en kryptokustode, der som minimum skal være enten oversergent eller civil af mellemlidergruppen (C-200).

Der skal også udpeges en alternativ kryptokustode på samme niveau, der bistår kryptokustoden med de daglige kryptoforvaltningsmæssige opgaver. Den alternative kryptokustode har ikke ansvaret for kryptoforvaltningen, men skal til enhver tid kunne overtage de forpligtelser og det ansvar, der påhviler kryptokustoden.

Der skal udpeges kryptokustodepersonale, der kan varetage kryptoforvaltningen på daglig basis. De må ikke tildeles andre opgaver, der gør, at de ikke kan varetage kryptoforvaltningen. Der bør udpeges personale, der kan bestride funktionerne i minimum et år.

15. Kryptokustoden har følgende forvaltningsmæssige ansvar, der skal udføres i henhold til DAMSG 205:

- At føre et retvisende kryptoregnskab, der indeholder alle oplysninger om alt kryptoudstyr og kryptonøgler, der er i kryptoforvaltningen.
- At ilægge kryptonøgler i kryptoudstyr. Dette kan dog også gøres af andet personale med et gyldigt kryptocertifikat og relevant uddannelse på udstyret.

- At forestå modtagelse/forsendelse/opbevaring/udlån af organisationens kryptobeholdning i samarbejde med den alternative kryptokustode.
- At forestå destruktion af organisationens kryptonøgler.
- At fremsende halvårlig rapportering til NDA DNK om status på kryptobeholdningen.

16. Personale, som tidligere er fjernet fra funktionen kryptokustode eller alternativ kryptokustode som følge af forsømmelse, af disciplinære eller sikkerhedsmæssige årsager, må ikke igen udpeges som kustode.

17. Der skal desuden udpeges en kryptosikkerhedsofficer. Kryptosikkerhedsofficeren skal som minimum være seniorsergent eller civil C-300. CFCS anbefaler, at der ikke er sammenfald mellem kryptosikkerhedsofficeren og kryptokustoden. Ved tvivl om forholdet skal CFCS inddrages.

18. Kryptosikkerhedsofficeren har følgende opgaver, der skal udføres i henhold til DAMSG 205:

- Rådgivning af chefen vedrørende kryptotjenesten.
- Sikring af, at kryptopersonalet har gennemgået relevant uddannelse og besidder korrekt sikkerhedsgodkendelse samt har et gyldigt kryptocertifikat.
- Årlig kryptosikkerhedsbelæring af personale med kryptocertifikat. Kryptosikkerhedsbelæringen påføres kryptocertifikatet.
- Sikring af, at CFCS har godkendt kryptoinstallationer for elektroniske informationssystemer, der behandler informationer klassificeret FORTROLIGT og højere, før systemerne tages i brug.
- Udarbejde og vedligeholde en detaljeret instruks til kryptopersonalet om kryptotjenesten (opbevaring, udlevering, adgang, fysisk sikkerhed, forsendelse, destruktion og nødfaldsplan). Det anbefales, at instruksens udfærdigelse i samarbejde med kryptokustoden.
- Forelæggelse af optællingsresultater (inventory og ved overdragelser) af kryptobeholdningen for chefen.
- Årlig udfærdigelse af kryptokontrolrapport, som arkiveres i minimum et år.

19. Der kan udpeges en kryptooperatør, som har kryptonøgler i sin varetægt, og som har til opgave at ilægge kryptonøgler i kryptoudstyr. Kryptooperatøren skal have et gyldigt kryptocertifikat, jf. nedenfor, og er ansvarlig over for kryptokustoden for, at alle kryptosikkerhedsmæssige bestemmelser bliver overholdt for udleverede kryptonøgler og -materiale.

20. Kryptopersonale sikkerhedsgodkendes i henhold til sikkerhedscirkulæret. Kryptokustoder skal som minimum være sikkerhedsgodkendt til HEMMELIGT. Personale, der forvalter kryptonøgler, skal dog som minimum altid have den samme sikkerhedsgodkendelse som den højeste klassifikation på det udstyr eller nøglemateriale, som myndigheden forvalter. En eventuel kryptooperatør skal være sikkerhedsgodkendt til minimum samme klassifikation som de kryptonøgler og udstyr, der er i vedkommendes varetægt.

Hvis kryptokustodepersonalet forvalter ti eller flere kryptonøgler, der er klassificeret HEMMELIGT/NATO SECRET, skal kryptokustodepersonalet være sikkerhedsgodkendt til YDERST HEMMELIGT/COSMIC TOP SECRET.

21. Kryptokustodepersonalet skal have gennemført en kryptokustodeuddannelse inden tiltrædelse i funktionen. Kryptosikkerhedsofficeren skal have gennemført kryptokustodeuddannelse og/eller kursus for kryptosikkerhedsofficerer inden tiltrædelse i funktionen.

22. For personale på Forsvarsministeriets område giver et "Q" i DeMars om gennemgået kryptokustodeuddannelse mulighed for at være kryptokustode. Personale uden for Forsvarsministeriets område skal have et fysisk kryptocertifikat for at kunne varetage denne funktion.

En kryptosikkerhedsofficer behøver ikke et kryptocertifikat for at bestride funktionen som kryptosikkerhedsofficer.

23. Et "Q" og et kryptocertifikat er gyldigt i ét år, hvorefter det skal opdateres én gang årligt. For myndigheder, der ikke har adgang til FIIN (civile myndigheder og firmaer), skal der udstedes et kryptocertifikat af den myndighed, der har forestået uddannelsen. Kryptocertifikatet opdateres og opbevares ved den lokale kryptoforvaltning indtil endt tjeneste.

24. En kryptokustode- og kryptosikkerhedsofficersuddannelse er gyldig i op til seks år efter gennemførelsen. Uddannelsen skal for kryptokustodens vedkommende én gang om året følges op med en kryptosikkerhedsbelæring, for at kryptocertifikatet er gyldigt. Opstår der et tidsrum på mere end 3 år mellem uddannelsestidspunktet og en sikkerhedsbelæring, skal kryptokustode-uddannelse gennemføres på ny.

25. Kryptooperatører, der skal have et kryptocertifikat, men ikke have et forvaltningsansvar, skal gennemføre relevant operatøruddannelse. Uddannelsen giver ikke adgang til at udføre funktionen som kryptokustode.

26. Føringsstøtteregimentet og Søværnets Center for Taktik gennemfører de nødvendige nationale uddannelser på kryptoområdet for alt personale, som skal arbejde med kryptoforvaltning og kryptosikkerhed nationalt, i NATO eller EU.

Kapitel 5

Godkendelsesprocedurer for kryptoudstyr

27. Kryptoudstyr er alt udstyr eller mekanismer, som involverer en kryptologisk proces, der har til formål at beskytte mod tab af fortrolighed, integritet og tilgængelighed af nationale, NATO, EU og andre partnerinformationer.

28. CFCS skal godkende alt kryptoudstyr til brug for klassifikationsgraden TIL TJENESTEBRUG eller højere. Før der tages beslutning om anskaffelse eller implementering af en ny type kryptoudstyr, skal der tages kontakt til CFCS. Ved behov for indgåelse af en bilateral eller multilateral aftale mellem Danmark og et kryptoproducerende land er det altid CFCS, som foretager en nærmere vurdering af udmøntningen af den konkrete aftale og koordinerer og underskriver aftalen.

29. Kryptoudstyr til brug for klassifikationsgraden NATO SECRET skal altid godkendes ved SECAN Washington DC (SECAN). Alt kryptoudstyr til brug for NATO eller systemer

med forbindelse til NATO skal godkendes af SECAN. CFCS kan anmode SECAN om godkendelse af et givent udstyr.

CFCS kan godkende kryptoudstyr til klassifikationsgraden NATO CONFIDENTIAL og lavere til brug for nationale systemer/netværk uden forbindelse til NATO systemer. Herudover er det en betingelse, at alt kryptoudstyr, som benyttes til at beskytte informationer klassificeret NATO RESTRICTED og højere, er produceret i et NATO medlemsland. Udstyr, der allerede er NATO-godkendt, kan findes på NATO Information Assurance Product Catalogue på NATO's hjemmeside.³

30. Godkendelsesproceduren for kryptoudstyr til brug for klassifikationsgraden EU SECRET er, at den kryptoproducerende nation og mindst én af de seks kryptogodkendende nationer i EU⁴ kan godkende det givne udstyr til den ønskede klassifikationsgrad.

CFCS kan godkende kryptoudstyr til EU CONFIDENTIAL og lavere til brug for nationale systemer/netværk uden forbindelse til EU systemer. Herudover er det en betingelse, at alt kryptoudstyr, som benyttes til at beskytte informationer klassificeret EU RESTRICTED og højere, er produceret i et EU-medlemsland.

Kapitel 6

Godkendelsesprocedurer for krypteringssoftware

31. CFCS godkender anvendelsen af krypteringssoftware, der ønskes implementeret i nationale informationssystemer klassificeret TIL TJENESTEBRUG eller højere. Godkendelsen skal foreligge, inden der indgås endelig aftale med en leverandør.

32. CFCS godkender krypteringssoftware til brug i NATO-informationssystemer klassificeret NATO RESTRICTED. Software til brug for NATO CONFIDENTIAL eller højere skal godkendes af SECAN efter indstilling fra CFCS.

33. De kryptogodkendende nationer i EU godkender krypteringssoftware til brug i EU-informationssystemer efter samme procedure som anført i pkt. 30.

Kapitel 7

Fysisk sikkerhed

34. Ved fysisk sikkerhed forstås de tiltag, der sikrer en bygning eller enkelte rum mod navnlig indbrud, spionage, sabotage eller tyveri.

En beskrivelse af kravene til fysisk sikkerhed for områdekategori og sikringsniveau findes i "Bestemmelser for den militære sikkerhedstjeneste" (FKOBST 358-1) kap. 7.

35. Kryptonøgler og udstyr med ilagte nøgler, der beskytter informationer klassificeret YDERST HEMMELIGT, skal opbevares i område kategori 1, sikringsniveau 50.

36. Kryptonøgler og udstyr med ilagte nøgler, der beskytter informationer klassificeret FORTROLIGT og HEMMELIGT, skal opbevares i område kategori 2, sikringsniveau 40.

³ www.la.nato.int/niapc

⁴ Godkendende nationer i EU er Tyskland, Frankrig, Østrig, Sverige, Holland og Italien.

37. Udstyr uden kryptonøgler eller udstyr mærket KRYPTO/CRYPTO eller CCI (Controlled COMSEC item/Controlled Crypto Item) skal opbevares i område kategori 2, sikringsniveau 30.

38. Udstyr, der beskytter TIL TJENESTEBRUG, og som ikke er mærket Krypto/Crypto og/eller CCI, skal som udgangspunkt beskyttes som område kategori 3, sikringsniveau 10. Der kan dog i visse tilfælde gives tilladelse til område kategori 4, sikringsniveau 30.

39. Ved opbevaring af kryptonøgler og dokumenter klassificeret HEMMELIGT skal der benyttes Klasse A (F&P)⁵ med tretals-kombinationslås. Klasse B (F&P) benyttes til operativt kryptoudstyr (radioer/mobiltelefoner) ilagt nøgler, som ikke er i brug.

40. Der kan anskaffes et særligt opbevaringsmiddel (server safe) til servere, kryptoudstyr og andet kryptomateriale, der kræver ekstra sikring som følge af, at den fysiske sikring af bygning, rum eller celle ikke er økonomisk forsvarlig.

41. Der er krav om etablering af "No-lone-zone" (NLZ) ved myndigheder, som producerer kryptonøgler, eller hvor der befinder sig et større antal kryptonøgler. Det er eksempelvis tilfældet ved kryptofordelingscentre og Key managementscentre. NLZ er et område eller rum, som er belagt med restriktioner i forhold til sikre medarbejdernes integritet. Der skal altid være mindst to behørigt sikkerhedsgodkendte og adgangsberettigede medarbejdere til stede, når der skal udføres opgaver i NLZ. Medarbejdere i NLZ kan udføre forskellige opgaver uafhængigt af hinanden. Hvor der er krav om NLZ, skal der udarbejdes og implementeres lokale procedurer for, hvordan kravene skal efterleves. Det er CFCS, som vurderer, hvor der skal etableres NLZ.

Kapitel 8

Installationer

42. Alle installationer med kryptoudstyr, der er klassificeret FORTROLIGT (NATO CONFIDENTIAL, CONFIDENTIEL UE/EU CONFIDENTIAL) eller højere, samt hvor der i øvrigt måtte være krav om en installationsgodkendelse, skal etableres, så de overholder de krav, der gælder for højere klassificerede informations- og kommunikationsteknologi-installationer (IKT-installationer).

Installationerne skal godkendes af CFCS, inden udstyret må tages i anvendelse. CFCS foretager forinden godkendelse en inspektion og yder rådgivning om NATO og EU's krav til installationerne.

CFCS gennemfører i den forbindelse TEMPEST-målinger med henblik på etablering af foranstaltninger, der skal nedsætte risikoen for kompromittering af klassificeret information som følge af elektromagnetisk udstråling eller bortledning, jf. kap. 16 nedenfor. CFCS gennemfører desuden teknisk sikkerhedseftersyn i forhold til risikoen for aflytning af tale, anden utilsigtet akustisk informationsformidling eller uautoriseret visuel indsigt, jf. kap. 17 nedenfor.

Godkendelse af installationer er i praksis relevant i to situationer:

⁵ Forsikring og Pension.

- Som led i godkendelsen af højere klassificerede, stationære systemer, jf. sikkerhedscirkulæret, § 27, hvor den anmodende part også selv skal drive eller anvende det pågældende system ved en permanent installation.
- Hvor der allerede foreligger en systemsikkerhedsgodkendelse, og det stationære system skal installeres permanent ved myndigheder, institutioner eller virksomheder, der skal anvende systemet.

43. I følgende situationer vil der skulle indhentes en ny installationsgodkendelse fra CFCS:

- Ved væsentlige ændringer i installationen.
- Ved flytning af en permanent installation.
- Ved genindflytning efter at lokaliteten har været forladt midlertidigt, hvis der har været adgang for uvedkommende.
- I tilfælde af indbrud og/eller konstateret indgreb.

Kapitel 9

Kryptonøgler

44. Alle nationale kryptonøgler produceres ved NDA DNK i henhold til kryptoplaner, der er godkendt af CFCS.

45. Fysiske nøgler i kanisterform kan stadig produceres og bestilles i Danmark. Materialer i bogform kan ligeledes produceres og bestilles ved NDA DNK.

46. Elektroniske kryptonøgler skal forvaltes på samme måde som de fysiske kryptonøgler. Produktion og distribution sker via NDA DNK. Distributionen til brugeren kan enten være ved elektronisk kommunikation eller ved brug af et Data Transfer Device (DTD). Ved kurerdistribution af u-krypterede (røde) kryptonøgler skal der benyttes DTD med Crypto Ignition Key (CIK). Ved kryptering af nøglerne (sorte) i DTD og uden isat CIK skal data i DTD betragtes som ikke klassificeret CCI. En DTD er CCI og skal opbevares som sådan.

47. Alle nationale kryptonøgler kan i henhold til godkendt kryptoplan rekvireres hos NDA DNK. Forsvarets enheder skal rekvirere NATO og EU samt bilaterale kryptonøgler hos NDA DNK via deres værns kommando. Civile myndigheder m.fl. retter via deres kryptokustode henvendelse direkte til NDA DNK med efterretning til CFCS.

48. Alle nationale kryptonøgler bærer en betegnelse, som identificerer nøglen. I Danmark er betegnelsen altid DAMS efterfulgt af mindst et bogstav og en talrække. Alle nøgler skal desuden tydeligt afmærkes med en klassifikationsgrad.

49. Udgavebetegnelsen er et bogstav eller bogstavsgruppe, der følger umiddelbart efter ovenstående DAMS-mærkning. Denne mærkning angiver, hvornår en specifik kryptonøgle er gyldig. Alle kryptonøgler, kryptopublikationer og legitimationstabeller skal have en unik udgavebetegnelse. Udgavebetegnelsen er som minimum klassificeret TIL TJENESTEBRUG, men klassificeret FORTROLIGT når den sættes i forbindelse med en specifik periode.

Gyldigheden på alle danske nøgler fremgår af publikationen "Status for kryptonøgler" (DAMSG 600), som udgives af NDA DNK.

50. Kryptonøgler, der er mærket med "Krypto/Crypto", må kun behandles af uddannet personel, som har et "Q" i DeMars eller et gyldigt kryptocertifikat.

51. En diagraph indikerer antallet af nøgleindstillinger i en kanister samt gyldighedsperiode for hver indstilling. Indholdet kan aflæses ved hjælp af en bogstavkombination og et tilhørende skema i DAMSG 205.

Kapitel 10

Transport af kryptomateriale

52. Krav til emballering og mærkning ved transport er beskrevet i DAMSG 205, kap. 5.

53. Ved transport af kryptoudstyr og kryptomateriale mærket "CCI" skal der benyttes en kurer, der er sikkerhedsgodkendt til minimum samme klassifikationsgrad som forsendelsen. Kureren skal være instrueret i kurertjeneste. I Danmark kan Forsvarets kurertjeneste med fordel benyttes.

54. Hvis Forsvarets kurertjeneste ikke kan benyttes, er det tilladt at benytte en lokalt udpeget, lejlighedsvis kurer. En lejlighedsvis kurer skal være sikkerhedsgodkendt til samme klassifikationsgrad som forsendelsen og modtage en udførlig instruktion fra den afsendende myndighed, institution eller virksomhed. Kureren skal have behørig dokumentation (kurercertifikat), og bør ved transport over grænser til ikke NATO/EU lande have diplomatpas eller lignende dokument, som sikrer kurerens personlige sikkerhed.

Instruksen til en lejlighedsvis kurer skal altid indeholde:

- Forhold omkring opbevaring og kvittering ved overdragelse.
- Kurerrute og forhold ved eventuel forsinkelse i forhold til forventet ankomsttid.
- Forhold ved kontrol der udføres af toldvæsen eller sikkerhedspersonel.
- Kontaktperson ved modtagende myndighed.

Der findes et eksempel på en instruks i DAMSG 205, kapitel 12, bilag 36.

55. Kryptonøgler skal altid transporteres af en kurer. Det skal tilstræbes, at kureren ikke er tildelt andre opgaver. Hvis kureren har andre opgaver, må de ikke være en hindring i forhold til udførelse af kureropgaven. Kureren skal modtage en instruks, jf. ovenstående.

56. Kryptoudstyr og CCI-mærket kryptomateriale kan transporteres med civilt, sikkerheds-godkendt, dansk transportfirma i NATO-lande eller i lande, der grænser op til et NATO-land, der har en specifik aftale med NATO eller Danmark om transport af klassificeret udstyr.

57. Transport af kryptoudstyr og CCI-mærket kryptomateriale kan ske med karosser eller containere, der er godkendt af CFCS til ubevogtet transport, hvis transporten udføres af et nationalt sikkerhedsgodkendt transportfirma, og kryptoudstyr og CCI-mærket kryptomateriale er lukket inde i et godkendt klasse A-opbevaringsmiddel. Det er et krav, at karossen/containeren ved ankomst til bestemmelsesstedet modtages af en dansk enhed, der kontrollerer forsendelsens integritet.

Ved brug af udenlandsk civilt transportfirma (bil/skib/fly) skal der altid følge en dansk sikkerhedsgodkendt kurer med transporten, som har til opgave at sikre forsendelsen.

Kapitel 11

Forvaltning af kryptomateriale

58. DAMSG 205, kap. 5, indeholder krav til forvaltning af kryptomateriale, hvad angår journalføring, optælling af kryptobeholdning (inventory), kryptoregnskab og arkivering.

59. Kryptokustoden er beholdningsansvarlig ved sin personlige underskrift for alt krypto/CCI-mærket kryptomateriale i sin kryptoforvaltning. Kryptokustoden er først fritaget for sit beholdningsansvar, når en tiltrædende kryptokustode sammen med den afgående kryptokustode har foretaget en komplet optælling af kryptobeholdningen og kvitteret for modtagelsen, og optællingen er godkendt af NDA DNK.

60. I tilfælde af kryptokustodens fravær i en periode, der ikke må overstige 60 dage, kan den alternative kryptokustode varetage kryptoforvaltningen.

61. Hvis kryptokustoden akut og uventet afgår som kustode, skal der udpeges en ny kryptokustode. Kryptosikkerhedsofficeren og den nye kryptokustode skal herefter foretage en komplet optælling af kryptobeholdningen og fremsende en "Possession Report" til NDA DNK, hvor årsagen til optællingen påføres.

62. Det er kryptosikkerhedsofficerens ansvar at sikre, at kryptoregnskabet altid er retvisende. Kryptosikkerhedsofficeren skal efter gennemførelse af halvårlig inventory eller ved skift til ny kryptokustode forelægge resultatet af optællingen for myndighedens chef, der ved sin underskrift bekræfter resultatet. Inventory med chefens underskrift fremsendes til NDA DNK.

Kapitel 12

Tilsyn og revision

63. Umiddelbart efter godkendelsen af etablering af en kryptoforvaltning, jf. kap. 3, og senest tre måneder efter aktivering af forvaltningen, foretager CFCS et første tilsyn. Tilsynet skal som minimum omfatte en gennemgang af kryptosikkerhedsinstruksen, håndtering og opbevaring af kryptomateriale, procedurer for rutinemæssig samt nødfaldsdestruktion og en vurdering af mulige trusler i forhold til kryptosikkerheden ved kryptoforvaltningen.

64. Inden aktivering af kryptoforvaltningen og i forbindelse med en installationsgodkendelse, jf. kap. 8, foretager CFCS også et tilsyn i form af en inspektion af den påtænkte installation, herunder med TEMPEST-målinger og et teknisk sikkerhedseftersyn.

65. Hvor der er behov for en ny installationsgodkendelse, jf. pkt. 43, foretager CFCS en ny inspektion. Ved større ændringer i installationen eller til de elektriske og/eller elektroniske systemer foretages en ny vurdering af TEMPEST-forholdene og i relevant omfang nye målinger. Der foretages efter CFCS' vurdering eventuelt også et nyt teknisk sikkerhedseftersyn.

66. CFCS gennemfører herefter periodisk tilsyn med kryptosikkerheden ved kryptoforvaltningerne. Tilsynet har typisk hovedfokus på forhold inden for kryptosikkerhedsofficerens ansvarsområde og omhandler blandt andet korrekt sikkerhedsgodkendelse og uddannelse af kryptopersonalet, årlig

kryptosikkerhedsbelæring, kryptokontrolrapport, opdateret kryptosikkerhedsinstruks, nødfaldsplaner, installationsgodkendelser, opbevaringsmidler til krypto samt opfølgning på bemærkninger fra tidligere tilsyn og revisioner. CFCS efterser også kryptoinstallationerne.

Tilsynet vil kunne gennemføres i sammenhæng med et generelt tilsyn med efterlevelsen af bestemmelserne i sikkerhedscirkulæret for så vidt angår elektronisk håndtering af klassificeret information.

67. NDA DNK gennemfører årligt en revision (Annual Audit) ved alle nationale kryptoforvaltninger efter retningslinjerne i DAMSG 205, kap. 6. NDA DNK udarbejder på baggrund af revisionerne revisionsrapporter, som tilgår kryptoforvaltningerne med henblik på eventuel opfølgning. Rapporterne sendes desuden til efterretning for CFCS.

En revision adviseres altid i god tid af NDA DNK. Dato koordineres mellem NDA DNK og den enkelte kryptoforvaltning. En eventuel uanmeldt revision gennemføres efter forudgående koordination med CFCS.

Revisionen omfatter som minimum en totaloptælling af kryptobeholdningen, en gennemgang af kryptoregnskabet, gennemgang af bestemmelser for kryptoforvaltning samt en gennemgang og kontrol vedrørende bemærkninger fra seneste revision. Revisionen indbefatter rådgivning om kryptorelaterede emner, herunder også i forhold til gældende sikkerhedsbestemmelser.

Kapitel 13

Destruktion af kryptomateriale

68. Destruktion af kryptonøgler i papirform skal ske ved anvendelse af en makulator, som ifølge NATO er godkendt til sikringsniveau O6 (DIN norm 66399, max. 5 mm²) eller ved brænding til hvid aske.

Til destruktion af kryptonøgler på SMART CARDS/CD og DVD skal der anvendes en makulator, som er godkendt til sikringsniveau O6 (DIN norm 66399, max. 5 mm²).

Destruktion af kryptonøgler skal altid foretages af to personer, som er godkendt til mindst samme klassifikationsgrad som de pågældende koder. Der skal udfærdiges en destruktionsrapport, hvor begge personer med deres underskrift bevidner destruktionsrapporten. Denne destruktionsrapport skal arkiveres i minimum et år.

DAMSG 205, kap. 11, indeholder en detaljeret beskrivelse af godkendte destruktionsmetoder og krav i øvrigt til destruktion, herunder nødfaldsdestruktion af kryptomateriale.

69. Kryptosikkerhedsofficeren skal udarbejde og vedligeholde en nødfaldsplan med foranstaltninger, der skal iværksættes i nødsituationer. Planen skal godkendes af organisationens chef. Der skal periodisk gennemføres nødfaldsøvelser. Dette eller som minimum en gennemgang af nødfaldsplanen bør ske årligt for at sikre, at nødfaldsdestruktion i henhold til planen er mulig.

Kapitel 14

Rapportering af brud på kryptosikkerheden

70. Brud på kryptosikkerheden er hændelser, der har tilladt uautoriserede personer indsigt eller mulighed for indsigt i krypteringsinformation eller -teknologi. I DAMSG 205, kapitel 9, er der listet, hvilke type hændelser der som minimum kan udgøre et brud på kryptosikkerheden.

71. Brud på kryptosikkerheden skal rapporteres i henhold til kap. 9 i DAMSG 205, herunder altid til CFCS. Den indledende rapportering skal ske omgående. Det er vigtigere at rapportere hurtigt, end at rapporten overholder formalia og at foretage undersøgelse af hændelsen.

Et brud på kryptosikkerheden kan medføre et brud på informationssikkerheden, der jf. § 45 i sikkerhedscirkulæret også skal rapporteres.

72. Rapportering kan ske ved brug af skabelonen "Brud på kryptosikkerheden", der kan rekvireres ved CFCS eller findes på internettet i FKOBST 358-1 (se link i bestemmelsens kap. 10).

73. Rapporteringen skal i udfyldt form som minimum klassificeres FORTROLIGT. Forsendelse skal ske i overensstemmelse med bestemmelserne om håndtering af klassificeret information i sikkerhedscirkulæret.

Kapitel 15

Anvendelse af kryptering i udlandet

74. Inden man benytter kryptomateriale i udlandet, bør man sikre, at kryptoudstyr, kryptonøgler og andet kryptomateriel kan opbevares forsvarligt. Man bør også undersøge, om det pågældende land tillader kryptering af data.

Desuden bør man undersøge, om det er tilladt og sikkerhedsmæssigt forsvarligt at medbringe kryptomateriellet til destinationen i henhold til nationale danske sikkerhedsbestemmelser. Der kan desuden gælde særlige regler vedrørende transport af kryptomateriel.

Information om brug af kryptering i et specifikt land kan eventuelt indhentes hos den danske repræsentation i landet, ved CFCS eller den myndighed, som eventuelt skal besøges.

Kapitel 16

Udstrålingssikkerhed (TEMPEST)

75. I elektronisk udstyr genereres elektromagnetiske felter, der udstråles som radiobølger eller bortledes som elektriske strømme i kabler, ledninger og andre metalliske ledere. En del af den elektromagnetiske udstråling kan være relateret til de data, som udstyret behandler. Med passende aflytningsudstyr kan de udstrålede signaler opsamles og data genskabes, og derved kan fortroligheden af data kompromitteres. Udstrålingssikkerhed betegnes sammenfattende TEMPEST, og handler om vurdering af den uønskede udstråling af data samt de modforanstaltninger, der skal afværge eller reducere risikoen for kompromittering.

Den uønskede udstråling kan ikke elimineres, men kan reduceres til et acceptabelt niveau ved korrekt valg af udstyr og installation. TEMPEST-udstyr er specielt designet eller modificeret kommercielt udstyr (pc'er, skærme, printere, VTC m.v.), jf. pkt. 84.

76. Udstyr, herunder kabler, krydsfelter, printere m.v., der behandler informationer klassificeret FORTROLIGT eller højere, skal, jf. sikkerhedscirkulæret § 41, være installeret på en sådan måde, at informationerne ikke kompromitteres via direkte elektromagnetisk udstråling eller bortledning.

NATO har fastlagt krav på området i "CIS Security Technical and Implementation Directive on Emission Security"⁶. Der er redegjort nærmere for, hvordan kravene kan opfyldes i publikationerne (forkortet) SDIP-27, SDIP-28 og SDIP-29, som der henvises til i det følgende. Hvor der måtte være uoverensstemmelse, er det direktivets bestemmelser, der gælder. EU har fastlagt tilsvarende krav. Dokumenterne er i det væsentligste klassificerede.

77. CFCS varetager funktionen som national TEMPEST-myndighed og yder vejledning og rådgivning på området.

Hvor der er krav om installationsgodkendelse, jf. kap. 8 oven for, gennemfører CFCS en inspektion, herunder med TEMPEST-målinger med henblik på etablering af passende TEMPEST-modforanstaltninger. CFCS' inspektioner på TEMPEST-området er beskrevet i pkt. 64-66 i kapitel 12 oven for.

78. TEMPEST-installationer kan etableres som enkeltinstallationer, ø-løsninger, "Shielded area" eller mobile installationer. Installationerne skal overholde SDIP-29. Kravene til godkendelse af en installation er en kombination af de fysiske rammers muligheder for at dæmpe elektromagnetisk udstråling, det anvendte udstyr, samt kablingen.

79. En ø-løsning er et område, hvor det er sikret, at der ikke sker bortledning af kompromitterende elektriske strømme i kabler, ledninger og andre metalliske ledere samt, at sikkerheden ikke kan kompromitteres ved aflytning af den elektromagnetiske udstråling fra udstyr. Udstyr kan *i nogen grad* frit placeres i ø-løsningen uden hensyntagen til respektafstande. Det kræver dog, at hele området, der er omfattet af ø-løsningen, lever op til de øvrige krav i SDIP-29. Ø-løsninger kræver særlig dokumentation. Inden der projekteres eller planlægges med ø-løsninger, bør der søges rådgivning ved CFCS.

80. En "shielded" installation er en installation, hvor afskærmning mod kompromitterende udstråling og bortledning implementeres i den fysiske lokalitet. En sådan installation vil typisk være "shielded" i form af et skærmrum. For installationer i meget små lokaliteter kan det være et afskærmende rackskab (målt og certificeret), hvor der installeres kommercielt standardudstyr kombineret med TEMPEST-udstyr til de konkrete arbejdspladser.

Et skærmrum er specielt konstrueret og indrettet til at dæmpe elektromagnetisk udstråling. Anvendelse af et skærmrum kan være relevant, f.eks når:

- Det ikke er muligt at tilvejebringe udstyr, der lever op til TEMPEST-kravene.
- TEMPEST-udstyr vurderes ikke at yde tilstrækkelig beskyttelse mod udstråling, eller
- Der er krav om, at en installation i særlig grad TEMPEST-beskyttes.

⁶ AC/322-D(2019)0021 (INV)

- Det vurderes at være et omkostningseffektivt alternativ til at anskaffe samtlige systemkomponenter som TEMPEST-udstyr.

Der skal udføres kontrolmåling af skærmrum en gang om året for at sikre, at rummets TEMPEST-specifikationer til stadighed er opfyldt. Efter hver måling udfærdiger CFCS en målerapport, herunder med eventuelle krav om udbedring af fejl og mangler. Rapporten fordeles til FMI og brugerenheden, hvor sidstnævnte snarest muligt efter aftale med CFCS foranlediger udbedringen. Modifikation af et godkendt skærmrum må kun ske med CFCS' godkendelse.

Bunkere og tilsvarende lukkede og solide konstruktioner, placeret over eller under jord, kan på grund af deres særlige konstruktion forventes at yde en så stor grad af beskyttelse mod kompromitterende udstråling, at brug af TEMPEST-udstyr måske ikke er nødvendigt. Det skal dog sikres, at der ikke sker bortledning af elektriske strømme i kabler, ledninger og andre metalliske ledere. CFCS vurderer i hvert enkelt tilfælde, om en bunker skal kontrolmåles.

81. For mobile installationer gælder særlige installationskrav, som bl.a. er afhængige af mobiliteten, jf. SDIP-29.

82. I forbindelse med en installationsgodkendelse foretages der Facility TEMPEST zoning (FTZ) i forhold til den aktuelle bygnings eller containers evne til at dæmpe en eventuelt kompromitterende udstråling. FTZ udføres af CFCS efter SDIP-28. Målinger af udstråling og bortledning af signaler udmøntes i op til tre zoner, zone 0, 1 eller 2. Der kan tildeles flere forskellige zoner i større bygningskomplekser.

CFCS kan i visse tilfælde tildele en FTZ-zone uden måling. F.eks. hvor bygningen, som det klassificerede udstyr ønskes installeret i, har almindelige vinduer, og hvor afstanden til det sted, hvor der uforstyrret vil kunne ske aflytning (inspectable space), er så langt fra de i SDIP-28 anførte grænseafstande mellem de tre zoner, at der ikke er tvivl om udfaldet af en egentlig måling.

83. Der kan udføres en Emitter/"on-site" test "i marken" på installationer i drift. Testen har til formål at kontrollere, om de implementerede TEMPEST-foranstaltninger er tilstrækkelig effektive. Testen udføres af FMI, og resultatet godkendes CFCS.

84. TEMPEST-udstyr produceres af virksomheder, som de nationale TEMPEST myndigheder i NATO-landene har godkendt som leverandører af TEMPEST-udstyr. Virksomhederne ombygger typisk kommercielt udstyr og foretager derefter en Equipment TEMPEST Zoning (ETZ), jf. SDIP-27. TEMPEST-udstyr anskaffes via FMI, som også fører regnskab med udstyret, indtil det er udfaset. Udstyret inddeles i henhold til SDIP-27 i TEMPEST-klasserne A, B og C, hvor udstyr i klasse A har en meget lav udstråling og bortledningsstrømme og yder den højeste TEMPEST-beskyttelse.

Som alternativ til anskaffelse af TEMPEST-produceret udstyr, kan der udføres ETZ målinger på udstyr. ETZ udføres af FMI, og resultatet godkendes derefter af CFCS. Det kan i nogen tilfælde være en fordel, hvis der er tale om indkøb af et meget begrænset antal enheder, eller hvor der er tale om specialbygget udstyr.

Krav til kabling fremgår af SDIP-29.

85. Alt TEMPEST-udstyr skal forvaltes ved hjælp af serienummerstyring. Ved serienummer-styringen skal det TEMPEST-level (A, B eller C), det pågældende udstyr er godkendt til, fremgå.

Myndigheder skal som minimum en gang årligt fysisk ved hjælp serienummereringen sikre, at alt tildelt TEMPEST-udstyr er til stede ved de godkendte installationer, herunder at udstyret ikke er manipuleret med i forhold TEMPEST-beskyttelsen, samt at det er forsynet med en label, der angiver TEMPEST-level.

FMI skal sikre, at TEMPEST-udstyr, der er indkøbt af FMI, leveres tilbage fra alle brugere til Forsvarets Supply Chain Division, efter behovet for udstyret er ophørt. TEMPEST-udstyr destrueres således, at modifikationer og modforanstaltninger ikke umiddelbart kan erkendes. Destruktionen følger de procedurer, der gælder for kryptomateriale, jf. kapitel 13.

Når der skal anvendes TEMPEST-udstyr i klassificerede netværk og systemer, skal placeringen af dette være angivet i den tilhørende kryptoplan.

Kapitel 17

Tekniske sikkerhedseftersyn

86. Tekniske sikkerhedseftersyn (TSE), også kaldet sweeping, er baseret på en række tekniske målinger og fysiske undersøgelser af lokaler, faciliteter og udstyr, som har til formål at afdække, om der er risiko for aflytning af tale eller anden akustisk formidling af information. Endvidere undersøges for visuel indsigt med f.eks. minikamera (video).

87. I sikkerhedscirkulæret, § 23 er fastsat følgende krav ift. beskyttelse mod gengivelse af klassificerede informationer:

”Mundtlig eller anden auditiv gengivelse af klassificerede informationer må ikke finde sted under sådanne forhold, at gengivelsen kan aflyttes.”

88. Som led i at mindske risikoen for mundtlig eller anden auditiv gengivelse af klassificerede informationer, anbefaler CFCS, at der gennemføres TSE, hvor der dagligt, periodisk eller lejlighedsvist gennemføres klassificerede aktiviteter.

89. NATO har derudover fastsat følgende krav til gennemførelse af TSE:

- I lokaler, hvor der regelmæssigt sker omtale/drøftelse af NATO-klassificeret information med klassifikationsgraden NATO SECRET eller højere.
- I forbindelse med CFCS' godkendelse af installation af kryptoudstyr, jf. kapitel 8 oven for.
- Ved ændringer eller renovering af lokaler og faciliteter, efter at de har været forladt, besat eller optaget af uautoriseret personale samt, hvis der er mistanke om eller opdaget aflytningsudstyr på eller i nærheden af lokalerne og faciliteterne.

90. TSE udføres af CFCS. En anmodning til CFCS om gennemførelse af TSE skal som minimum være klassificeret TIL TJENESTEBRUG. Informationer vedrørende gennemførelsen af TSE må alene udveksles, herunder telefonisk, via klassificerede kommunikationsmidler.

Der bør i forbindelse med anmodningen tages højde for, at TSE efter omstændighederne kan være tidskrævende og i komplicerede tilfælde tage dage at gennemføre. CFCS

planlægger eftersynets omfang i samarbejde med den rekvirerende parts sikkerheds-, informationssikkerheds- og/eller kryptosikkerhedsofficer.

91. Planlægning og gennemførelse af TSE skal ske med inddragelse af et minimum af parter/personale. Eftersynet må ikke omtales forud for eller under gennemførelse i de omhandlede lokaliteter, da formålet derved vil kunne forspildes.

92. Der vil typisk skulle gennemføres TSE af:

- Lokaler, der kræver permanent beskyttelse mod aflytning, såsom kontorer, arbejds- og møderum, hvor visse mindstekrav til fysiske sikkerhedsforanstaltninger skal være opfyldt.
- Lokaler, der kræver midlertidig beskyttelse mod aflytning, såsom konferencerum, som normalt benyttes til flere formål og derfor befærdes af mange personalegrupper.
- Lukkede anlæg og områder, der midlertidigt har været åbnet for ikke autoriseret personale. Sådanne anlæg og områder kan være ingeniørgange og rum, der ligger tæt på beskyttede lokaler, og derfor normalt vil være aflåst og forsegled.
- Nyindrettede faciliteter og installationer, der kræver godkendelse inden ibrugtagning.
- Køretøjer, fly og skibe, der typisk for en kortere periode ønskes beskyttet mod aflytning.

Forud for et eftersyn skal alle møbler og tekniske hjælpemidler være på plads i lokalet.

93. Den rekvirerende part skal i forbindelse med et TSE kunne fremlægge beskrivelse af følgende:

- Bygningsplacering med afstande til andre bygninger, perimeterhegn mv.
- Bygningskonstruktion (indretning, byggematerialer, faste installationer mv.).
- Tegninger over særlige installationer, herunder installationer omfattet af it-sikkerhedsbestemmelser.
- Beskrivelse af sikringsforanstaltninger, herunder i forhold til adgangskontrol.
- Eventuelt udførte ombygninger, installationsændringer, ommøbleringer mv. siden det senest gennemførte TSE.

94. Efter gennemført TSE orienterer CFCS rekvirenten om resultatet heraf og rådgiver om eventuelle relevante modforanstaltninger, herunder om NATO og EU's krav til foranstaltninger. Efterfølgende vil den rekvirerende part modtage en skriftlig rapport om eftersynet.

95. CFCS kan i visse særlige tilfælde, når der er tale om møder med særlig sensitive emner, også udføre TSE, imens et møde pågår. Dette udføres for at kontrollere, om der bevidst eller ubevidst er medbragt f.eks. radiosendere på mødelokaliteten, eller om eventuelt aflytningsudstyr placeret inden mødets start bliver aktiveret under mødet.

96. Der bør efter behov udpeges et eller flere lokaler, hvori klassificeret eller anden sensitiv informationsudveksling jævnligt kan foretages med henblik på at gøre disse lokaler til genstand for rutinemæssige TSE. Disse samt tilstødende lokaliteter skal være aflåst, når de ikke er i brug.

97. Lokaler hvori der er installeret telefoner, samtaleanlæg, højtaleranlæg, fjernsyn, radio og lignende, er ikke anvendelige til drøftelse af klassificeret information. TSE af lokaler med denne type installationer vil medføre adskillelse og afkobling af installeret

udstyr. Evt. genetablering påhviler rekvirenten. Mobiltelefoner og andet radiokommunikationsudstyr (f.eks. Powerpoint Presenters) må ikke være til stede i eftersete lokaliteter under klassificerede samtaler eller møder.

98. Efter gennemførelse af TSE er det nødvendigt, at den omhandlede lokalitet mv. holdes under konstant overvågning med den nødvendige adgangskontrol og/eller bevogtning, hvis den ved TSE opnåede sikkerhedstilstand skal opretholdes. Så snart uvedkommendes færden i eller i nærheden af den undersøgte lokalitet ikke længere er under overvågning, bortfalder værdien af det gennemførte TSE.

99. CFCS kan på Forsvarsministeriets område efter egen vurdering gennemføre uvarslet TSE som kontrol af lokaler og installationer mv.

Kapitel 18

Akustisk måling

100. For at modvirke, at klassificerede samtaler i mødelokaler m.v. kan aflyttes igennem bygningsskallen, kan der være behov for at foretage en lydmåling for at kortlægge lyddæmpningen i bygningsmaterialet. Resultatet af lydmålingen medvirker til at identificere, om en samtale potentielt vil kunne aflyttes igennem bygningsskallen.

101. CFCS har fastsat en række anbefalede minimumsværdier til lyddæmpning i sikrede lokaler, fra sikringsniveau 30 til 60, hvor der må tales HEMMELIGT eller YDERST HEMMELIGT. En beskrivelse af anbefalingerne til fysisk sikkerhed for områdekategori og sikringsniveau findes i "Bestemmelser for den militære sikkerhedstjeneste" (FKOBST 358-1) kap. 7.

102. Anbefalingen til lyddæmpningsniveauet i et lokale fastsættes ud fra en vurdering af risikoen for, at en aflytning kan finde sted. Lyddæmpningen måles efter ISO 16283-1 og beregnes i dB (DnTw) efter ISO 717-1.

103. Lokaler, hvor der må tales til og med klassifikationsgraden YDERST HEMMELIGT, bør sikres til et lyddæmpningsniveau på minimum DnTw=55 dB.

Det bør sikres, at dæmpningen gælder i alle rummets retninger, inkl. gulv og loft.

Lokaler, hvor der må tales til og med klassifikationsgraden HEMMELIGT, bør sikres til et lyddæmpningsniveau på minimum DnTw=50 dB.

Det bør sikres, at dæmpningen gælder i alle rummets retninger, inkl. gulv og loft. Det er dog tilstrækkeligt med et lyddæmpningsniveau på DnTw=45 dB, såfremt lokalets placering er i et sikret område, og samtlige medarbejdere med adgang til det sikrede område, er sikkerhedsgodkendt til minimum HEMMELIGT.

104. CFCS bør inddrages ifm. etablering eller ombygning af klassificerede lokaler eller bygninger mhp. at kunne foretage lydmålinger og rådgive om anbefalinger til lyddæmpning.

105. Anmodning om akustisk måling:

Akustisk måling udføres af og rekvireres ved CFCS via telefon eller e-mail. Detaljer vedrørende udførelse af akustisk måling samt beskrivelse af lokalitet skal klassificeres TIL TJENESTEBRUG. Informationer vedrørende gennemførelsen af akustisk måling må alene udveksles, herunder telefonisk, via klassificerede kommunikationsmidler.

106. Akustisk måling rekvireres på FIIN på FE-KTP-TSE eller via REGNEM til FE-MYN-FORSVARETS EFTERRETNINGSTJENESTE. Der skal ved rekvisitionen tages højde for, at akustisk måling efter omstændighederne kan være tidskrævende. CFCS planlægger i samarbejde med rekvirentens sikkerhedsorganisation målingens omfang.

8. marts 2022

Bilag 4: Systemsikkerhedsofficerernes opgaver

Krav til udpegning af systemsikkerhedsofficer (SYSOF) fremgår af foranstaltning 5.2 i kapitel 6.

SYSOF understøtter den it-ansvarliges/systemansvarliges opgaver med hensyn til funktionalitet og kvalitet samt sikkerhed for systemet. SYSOF skal i den forbindelse understøtte implementering og effektivitet af de foranstaltninger, som der er aftalt med den forretningsansvarlige og/eller som følger af krav i internationale, nationale og interne regelsæt samt aftaleretlige forpligtelser.

SYSOF skal herunder:

- Vedligeholde sikkerhedsrelateret systemteknisk viden (konfiguration, integration med andre systemer, netværk m.v.), uanset om systemdrift varetages af interne eller eksterne leverandører.
- Indgå som en central rolle i forbindelse med indkøb og udvikling af nye systemer samt i systemakkrediteringssager, herunder ift. udarbejdelse af en teknisk risikovurdering (systemrisikovurdering) og i den forbindelse afdækning af relevante foranstaltninger.
- Rådgive forretningen ved installationer og tilkoblinger, herunder i forbindelse med eventuel akkreditering heraf.
- Rådgive den forretningsansvarlige ved dennes udarbejdelse af system-sikkerhedsinstruks, eller efter aftale med den forretningsansvarlige udarbejde systemsikkerhedsinstruksen på vegne af denne.
- Varetage eller koordinere opgaver med sårbarhedsstyring herunder teknisk risikovurdering, jf. foranstaltning 8.8 i kapitel 6, samt føre risikolog for systemet.
- Indgå i opgaven med videreudvikling af systemet med henblik på videreførelse af det fastlagte sikkerhedsniveau.
- Bistå den it-ansvarlige/systemansvarlige, når der gennemføres tilsyn eller revision ved den it-ansvarlige/systemansvarlige, der omfatter det pågældende system.
- Rådgivning om sikkerhedsrelateret systemsikkerhed i forhold til leverandørforhold.
- Indgå ved håndtering af indrapporterede informationssikkerhedshændelser, herunder med teknisk analyse og anbefaling af udbedrende foranstaltninger, samt føre risikolog for systemet.
- Overvåge sikkerhedsmæssig forsvarlig nedlæggelse af systemet samt destruktion af hardware i henhold til bestemmelsesgrundlaget.

Bilag 5: Oversigt over informationssikkerhedsforanstaltninger

Bilag 5 indeholder en oversigt over foranstaltninger og delforanstaltninger, der skal implementeres og dokumenteres i henhold til kapitel 6 i FKOBS 358-1. Bilaget skal anvendes i sammenhæng med kapitel 6, som indeholder den fulde beskrivelse af alle delforanstaltningerne.

Læsevejledning til bilag 5	
Nr. og profil	Overskriften for foranstaltningerne følger nummereringen i ISO 27002:2022, og det er angivet, for hvilke sikkerhedsprofiler de enkelte delforanstaltninger gælder.
Foranstaltninger	Foranstaltningerne er udmøntet i delforanstaltninger ud fra, hvor der i kapitel 6 kan udledes konkrete foranstaltninger, der skal implementeres, og ikke blot en nærmere beskrivelse af en foranstaltning.
Krav	Med "Ja" menes, at det er obligatorisk at implementere foranstaltningen, medmindre der er givet en forudgående dispensation i henhold til kapitel 6, afsnit I. Implementering kan dog undtages, hvis en foranstaltning vil kunne kompromittere operations-sikkerheden, jf. kapitel 5. Undtagelsen kan ske på baggrund af en risikovurdering, der er godkendt af Forsvarskommandoen (Operationsstaben). Det er dog et krav, at der med afsæt i risikovurderingen implementeres passende tilsvarende og/eller kompenserende, risikoreducerende foranstaltninger i forhold til informationssikkerheden. Hvad angår klassificerede systemer, kræver en undtagelse fra obligatoriske krav godkendelse fra CFCS som national it-sikkerhedsmyndighed. "Nej" betyder, at implementering kan fraviges på baggrund af en risikovurdering godkendt af risikoejeren/-erne. Hvis risikoejer ikke har et ledelsesansvar, skal fravigelsen godkendes af som minimum vedkommendes nærmeste leder.
Krav om dokumentation	"Ja" betyder, at der enten skal foreligge passende ledelsesgodkendt, skriftlig dokumentation eller dokumentation i en database, hvorfra der kan laves et udtræk. "Nej" kan betyde, at der ikke er et dokumentationskrav, eller at det følger andetsteds. Alle foranstaltninger skal som udgangspunkt således kunne dokumenteres i regi af ledelsessystemet for informationssikkerhed enten i SoA dokumentet eller i risikohåndteringsplaner.
Opgave med implementering	Anførslen af hvem der skal implementere en foranstaltning er vejledende. "-" betyder, at selve kravet til en foranstaltning er fastsat andetsteds, f.eks. i en politik, et direktiv eller en bestemmelse, således at kapitel 6 ikke introducerer en ny opgave.

	Hvem der i praksis og konkret skal implementere en foranstaltning fastlægges internt i det enkelte ledelsessystem for informationssikkerheden, herunder betydningen af "myndigheder" og "enheder". Med "it-leverandører" menes, medmindre andet er anført, såvel koncerninterne som eksterne leverandører af it-services og systemer, herunder driftsansvarlige for systemer. Her har forretningssiden typisk ikke en opgave. Hvor omvendt it-leverandører ikke er nævnt, betyder dette ikke, at de ikke har en implementeringsopgave, idet koncerninterne it-leverandører også kan være underlagt krav som "myndigheder".
Henvisning til interne og eksterne krav	Henvisningerne er ikke udtømmende. Myndighederne skal være opmærksomme på eventuelle, yderligere lovkrav, herunder EU-lovgivning, samt bestemmelser og afgørelser fra NATO og EU. Der kan rettes henvendelse til den nationale it-sikkerhedsmyndighed, FE's Center for Cybersikkerhed (CFCS), for rådgivning vedrørende eksterne krav til klassificerede systemer.

Nr. og profil	Foranstaltninger	Krav	Krav om dokumentation	Opgave med implementering	Henvisning til interne og eksterne krav
Organisatoriske foranstaltninger					
5.1	Politikker for informationssikkerhed				
5.1.1 A-C	Styrelsesspecifik politik	Ja	Ja	-	Se krav i FMNPOL 358-1 (kap. 6)
5.1.2 A-C	Emnespecifikke politikker, processer, procedurer og instrukser	Ja	Se krav i dette bilag 5	-	Se krav i dette bilag 5
5.2	Roller og ansvar for informationssikkerhed				
5.2.1 A-C	Definition og fordeling af alt ansvar for informations-sikkerhed	Ja	Nej	Alle myndigheder og enheder	FMNBST 358-1 (kap. 3 og bilag 2), FMNBST 358-2 (kap. 2), FKOBST 358-1 (kap. 1 med bilag 2)
5.2.2 A-C	Etablering af en informations-sikkerhedsorganisation	Ja	Ja	Alle myndigheder og enheder	FMNBST 358-1 (kap. 3)
5.2.3 A-C	Udpegning af system-sikkerhedsofficerer for visse systemer	Ja	Ja	Koncerninterne it-leverandører	FKOBST 358-1 (bilag 4 til kap. 6)

5.3	Funktionsadskillelse				
5.3.1 A-C	Adskillelse af modstridende funktioner og ansvarsområder	Ja	Nej	Alle myndigheder og enheder	FMNBST 358-1 (kap. 3)
5.3.2 A-C	Risikoreducerende foranstaltninger ved manglende funktionsadskillelse	Ja	Nej	Alle myndigheder og enheder	-
5.4	Ledelsesansvar				
5.4.1 A-C	Ledelsens understøttelse af målsætninger og krav	Ja	Nej	Ledelsen ved alle myndigheder og enheder	FMNPOL 358-1 (kap. 6)
5.4.2 A-C	Årlig informationssikkerhedsinstruktion med kvittering	Ja	Ja	Alle myndigheder og enheder	-
5.5	Kontakt med myndigheder				
5.1 A-C	Kontakt med internationale og nationale myndigheder	Ja	Nej	Alle myndigheder og enheder	Se også 5.14
5.6	Kontakt med særlige interessegrupper				
5.6.1 A-C	Kontakt med interessegrupper, sikkerhedsfora o.l.	Ja	Nej	Alle myndigheder	Se også 5.14
5.6.2 A-C	Abonnement på varsler og tweets	Ja	Nej	Alle myndigheder	CFCS' krav til et styrket cyberforsvar (5.4)
5.6.3 A-C	Gennemgang af vejledninger fra CFCS	Ja	Nej	Alle myndigheder	-
5.6.4 A-C	Vurdering af vejledninger fra andre myndigheder	Ja	Nej	Alle myndigheder	-
5.7	Trusselsefterretning				
5.7.1 A-C	Brug af FE's og CFCS' trusselvurderinger og varsler	Ja	Nej	-	Se krav i FMNBST 358-2 (kap. 7)
5.8	Informationssikkerhed ved projektstyring				
5.8.1 A-C	Risikostyring, herunder fastlæggelse af krav til informationssikkerhed	Ja	Ja	Alle myndigheder og enheder	FMIDIR 380-1 FMNBST 358-2 GDPR
5.8.2 A-C	Udarbejdelse af PIA hvis behandling af personoplysninger	Ja	Ja	-	Se krav i GDPR

5.8.3 A-C	Fastlæggelse og revurdering af sikkerhedsprofil herunder klassifikation og behov for akkreditering	Ja	Ja	Forretningsansvarlige i dialog med risikoejere	FKOBST 358-1 (kap. 1 og 4) Se også 8.20
5.8.4 B-C	Vurdering af behov for internetadgang	Ja	Ja	Forretningsansvarlige i dialog med risikoejere	CFCS' krav til et styrket cyberforsvar (6.2)
5.8.5 B-C	Beskrivelse af implementering af sikkerhedskrav i sikkerhedsdokumentationen	Ja	Ja	It-leverandører	-
5.9	Fortegnelse over aktiver				
5.9.1 A-C	Aktivliste forretningsprocesser, it-services og systemer	Ja	Ja	-	Se krav i FMNBST 358-1 (kap. 2.1) og FMNBST 358-2 (kap. 5)
5.9.2 A-C	Liste over aktiver der understøtter it-services og systemer, herunder teknisk infrastruktur	Ja	Ja	It-leverandører	-
5.9.3 A-C	Fortegnelse over behandlingsaktiviteter	Ja	Ja	-	Se krav i GDPR og FMNBST 358-1 (bilag 1)
5.10	Accepteret brug af aktiver				
5.10.1 A-C	Instrukser for brug af systemer og netværk	Nej	Ja	Forretningsansvarlige i dialog med it-ansvarlige	-
5.10.2 B-C	Regler om accepteret brug af klassificerede systemer i sikkerhedsdokumentationen	Ja	Ja	It-ansvarlige i dialog med forretningsansvarlige	-
5.10.3 C	Underskrevet erklæring fra brugere af klassificerede systemer	Ja	Ja	Informationssikkerheds-officerer eller TASO'er	-
5.11	Tilbagelevering af aktiver				
5.11.1 A-C	Procedure for tilbagelevering af aktiver med minimumskrav til kontrol og dokumentation for profil B og C systemer	Ja	Ja	Nærmeste ledelse	Se også 7.14
5.12	Klassifikation af information				

Implementeres gennem bestemmelserne i kap. 1 og 4					
5.13	Mærkning af information				
Implementeres gennem bestemmelserne i kap. 1 og 4 samt FMNBST 400-1					
5.14	Informationsoverførsel				
5.14.1 A-C	Regler, procedurer og foranstaltninger for sikker informationsoverførsel mellem systemer	Nej	Nej	Alle myndigheder og enheder	-
5.14.2 A-C	Aftaler med eksterne parter om sikker informations-overførsel	Nej	Ja	Alle myndigheder og enheder	-
5.14.3 A	Vurdering af klassifikation, mærkning og kommunikationsmidler	Ja	Nej	Alle myndigheder og enheder	Sikkerhedscirkulæret Se også 5.14
5.14.4 B-C	Automatiserede løsninger for mærkning og anførsel af klassifikationsgrad for klassificerede systemer skal godkendes af CFCS	Ja	Ja	It-leverandører	-
5.15	Adgangsstyring				
5.15.1 A-C	Regler for adgangsstyring	Ja	Ja	Forretningsansvarlige	Se 8.2 og 8.3 samt 5.16-5.18 FKOBST 358-1 (kap. 7)
5.16	Brugerregistrering og -afmelding				
5.16.1 A-C	Krav til til- og fratrædelses-procedure herunder med minimumskrav til kontrol for profil B og C systemer	Ja	Ja	Forretningsansvarlige	CFCS' krav til et styrket cyberforsvar (7.1)
5.16.2 A-C	Oversigt over brugere og brugerkonti	Ja	Ja	It-leverandører	-
5.16.3 C	Halvårlig kontrol af om proceduren er fulgt	Ja	Nej	Alle myndigheder og enheder	CFCS' krav til et styrket cyberforsvar (7.1)

5.17	Autentifikationsinformation				
5.17.1 A-C	Procedure for tildeling og styring af autentifikations-information	Ja	Ja	It-leverandører	
5.17.2 A-C	Krav til passwords	Ja	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (7.4 og 7.5) og krav nr. 11 i Tekniske minimumskrav 2023 Se også 8.5
5.17.3 A-C	Instruks til brugerne om passwords	Ja	Ja	Alle myndigheder og enheder	CFCS' krav til et styrket cyberforsvar (7.4)
5.17.4 C	Krav hvad angår samfunds-kritiske systemer, ift. ofte anvendte og lækkede passwords	Ja (hvor muligt)	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (7.5)
5.18	Adgangsrettigheder				
5.18.1 A-C	Oversigt over tildelte adgangsrettigheder	Ja	Ja	It-leverandører	Se 5.15 om krav til adgangsstyring
5.18.2 A-C	Gennemgang af adgangsrettigheder	Ja	Ja	Forretningsansvarlige	-
5.18.3 A-C	Stikprøvekontrol af faktisk adgang	Ja	Nej	It-leverandører	-
5.18.4 A-C	Procedure for inddragelse af rettigheder	Ja	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (7.1) Se procedurekrav i 5.16
5.18.5 A-C	Inddragelse og ændring af adgangsrettigheder	Ja	Nej	Alle myndigheder og enheder	CFCS' krav til et styrket cyberforsvar (7.1)
5.19	Informationssikkerhed i leverandørforhold				
5.19.1 A-C	Politik for informations-sikkerhed i leverandørforhold	Ja	Ja	Myndigheder på styrelsesniveauet	Se også 5.1.1 (kan indgå heri)
5.19.2 A-C	Proces for risikovurdering og fastlæggelse af krav	Ja	Ja	Myndigheder på styrelsesniveauet	FMIDIR 380-01, FMIBST 380-02

5.19.3 A-C	Procedurer og foranstaltninger til at styre risici	Ja	Ja	Alle myndigheder og enheder	FMIDIR 380-01, FMIBST 380-02
5.19.4 A-C	Kompenserende foranstaltninger ved manglende krav eller efterlevelse af krav	Ja	Ja	Alle myndigheder og enheder	-
5.19.5 C	Vurdering af behov for rådgivning fra CFCS ved indkøb og udbud af samfundskritiske systemer	Ja	Nej	Alle myndigheder og enheder	-
5.20	Håndtering af sikkerhed i leverandøraftaler				
5.20.1 A-C	Krav til fastlæggelsen af krav til informationssikkerhed i leverandøraftaler	Ja	Ja	Forretningsansvarlige	CFCS' krav til et styrket cyberforsvar (10.1) Sikkerdigital.dk (krav til kontraktbestemmelser)
5.20.2 A-C	Databehandleraftaler hvis behandling af personoplysninger	Ja	Ja	Forretningsansvarlige ved myndigheder med dataansvar	GDPR
5.20.3 A-C	Krav til SLA eller OLA med SKS hvis aftale om it-drift	Ja	Ja	Forretningsansvarlige i dialog med it-leverandører	FMIBST 380-02
5.20.4 A-C	Oversigt over leverandører og aftaler samt kravstillen	Ja	Ja	Alle myndigheder og enheder	-
5.20.5 B-C	Sikring af dokumentation for efterlevelsen af krav ved udbud og/eller aftaleindgåelse	Ja	Nej	Alle myndigheder og enheder	-
5.20.6 A-C	Gennemgang og eventuel opdatering af krav	Ja	Nej	Alle myndigheder og enheder	Se også 5.19.4
5.21	Informationssikkerhed i forsyningskæden for leverandørydelser				
5.21.1 A-C	Forhold vedr. forsyningskæden skal indgå i procedurer og aftaler	Ja	Ja	Alle myndigheder og enheder	Se også 5.19, 5.20 og 5.22
5.21.2 A-C	Krav til aftaler med underleverandører	Ja	Ja	Koncerninterne it-leverandører	-

5.22	Leverandørstyring				
5.22.1 A-C	Procedure for leverandørstyring	Ja	Ja	Myndigheder på styrelsesniveauet	-
5.22.2 A-C	Krav til leverandørstyring i aftaler med leverandører	Ja	Ja	Alle myndigheder og enheder	Se også 5.20
5.23	Informationssikkerhed ved brug af cloud services				
5.23.1 A-C	Processer for indkøb, anvendelse, styring af og exit fra cloud services	Ja	Ja	Koncerninterne it-leverandører	Se også 5.8.1
5.23.2 A-C	Risikovurdering af cloud services inden aftaleindgåelse	Ja	Ja	Forretningsansvarlige i dialog med it-ansvarlige	-
5.23.3 A-C	Specifikation af krav til informationssikkerhed	Ja	Ja	Forretningsansvarlige	Se også 5.19-5.22
5.24 - 5.28	Hændelsesstyring				
Implementeres gennem bestemmelserne i kap. 10					
5.29	Informationssikkerhedskontinuitet				
5.29.1 A-C	Planlægning af forebyggende foranstaltninger til at opretholde eller genoprette informationssikkerhed	Ja	Nej	Alle myndigheder og enheder	Se også 5.30
5.29.2 A-C	Krav til leverandører om informationssikkerhedskontinuitet	Ja	Ja	Forretningsansvarlige	Se også 5.20
5.29.3 A-C	Krav til processer, procedurer og foranstaltninger uagtet aftalegrundlag	Ja	Ja	Koncerninterne it-leverandører	-
5.29.4 A-C	Udpegning og instruktion af personale	Ja	Nej	Koncerninterne it-leverandører	-
5.29.5 A-C	Afprøvning af planer og procedurer	Ja	Nej	Alle myndigheder og enheder	-
5.29.6 B-C	Frekvens for afprøvning skal fremgå af sikkerheds-	Ja	Ja	It-ansvarlige	-

	dokumentationen for systemerne				
5.29.7 C	Gennemgang og sikring af efterlevelsen af CFCS' krav til et styrket cyberforsvar for samfundskritiske systemer	Ja	Nej	Alle myndigheder og enheder	CFCS' krav til et styrket cyberforsvar
5.30	It-beredskab for business continuity				
5.30.1 A-C	Krav til krisestyringsplan	Ja	Ja	Alle myndigheder og enheder	Se også 5.29
5.30.2 B-C	Krav til reetableringsplaner og test af reetablering	Ja	Ja	It-leverandører	Se også 5.20 og 5.29
5.30.3 A-C	Tilgængelighed af planer og kontrol heraf	Ja	Ja	Alle myndigheder og enheder	CFCS' krav til et styrket cyberforsvar (1.4)
5.30.4 A-C	Medarbejdere er gjort bekendt med planer, ansvar og opgaver samt kontrol heraf	Ja	Nej	Nærmeste ledelse	CFCS' krav til et styrket cyberforsvar (1.3) Se også 6.2 og 6.3
5.30.5 A-C	Gennemgang og opdatering af planer på baggrund af øvelser og tests m.v.	Ja	Ja	Alle myndigheder og enheder	CFCS' krav til et styrket cyberforsvar (1.1)
5.30.6 A-C	Proces for opdatering af lister med kontaktoplysninger	Ja	Nej	Alle myndigheder og enheder	CFCS' krav til et styrket cyberforsvar (1.2)
5.30.7 B-C	Procedurer ift. nedsat eller manglende tilgængelighed til it-services og systemer og krav til brug af alternative kommunikationsmidler	Ja	Ja	Alle myndigheder og enheder	CFCS' krav til et styrket cyberforsvar (1.5) Se også 5.30.1
5.30.8 B-C	Vurdering af systemarkitektur og forsyningssikkerhed	Ja	Nej	Koncerninterne it-leverandører	Se også 7.11
5.31	Identifikation af lov-, myndigheds- og kontraktkrav				
Implementeres gennem bestemmelserne i FMNBST 358-1, kap. 2.1					
5.32	Immaterielle rettigheder				

5.32.1 A-C	Procedurer til sikring af overensstemmelse med lov-, myndigheds- og kontraktkrav	Ja	Nej	Alle myndigheder og enheder	-
5.33	Beskyttelse af fortegnelser				
5.33.1 A-C	Regler og retningslinjer for beskyttelse af fortegnelser	Ja	Ja	Myndigheder på styrelsesniveauet	-
5.34	Privatlivets fred og beskyttelse af personoplysninger				
5.34.1 A-C	Procedurer og foranstaltninger til beskyttelse af personoplysninger og udøvelse af de registreredes rettigheder	Ja	Ja	Alle myndigheder og enheder	GDPR
5.35	Uafhængig gennemgang af informationssikkerhed				
Implementeres gennem bestemmelserne i FMNBST 358-1, kap. 6, og "Vejledning om databeskyttelsesrådgivere i Forsvarsministeriets koncern"					
5.36	Compliance med politikker og standarder for informationssikkerhed				
Implementeres gennem bestemmelserne i FMNBST 358-1, kap. 5					
5.37	Dokumenterede driftsprocedurer				
5.37.1	Dokumentation og tilgængelighed af driftsprocedurer	Ja	Ja	It-leverandører	-
Adfærdsmæssige foranstaltninger					
6.1	Screening				
Implementeres gennem bestemmelserne i kapitel 2					
6.2	Ansættelsesvilkår og -betingelser				
6.2.1 A-C	Beskrivelse af ansvar og forpligtelser i kontrakter	Ja	Ja	FPS (og FE)	Se også 6.6
6.2.2 A-C	Orientering af medarbejdere og samarbejdsparter ved tiltrædelse	Ja	Nej	Nærmeste ledelse	-
6.2.3 B-C	Udenlandsk ansat personel må ikke gives adgang til nationalt klassificerede systemer	Ja	Nej	Alle myndigheder og enheder	-

6.3	Awareness, uddannelse og træning				
6.3.1 A-C	Individuelle uddannelses-programmer	Ja	Ja	Nærmeste ledelse	-
6.3.2 A-C	Instruktion om informations-sikkerhed	Ja	Nej	Nærmeste ledelse	-
6.3.3 A-C	Koncernfælles awareness aktiviteter og materiale	Ja	Nej	FMN-CID	CFCS' krav til et styrket cyberforsvar (10.1)
6.3.4 A-C	Styrelsesspecifikke awareness aktiviteter	Ja	Nej	Myndigheder på styrelsesniveauet	CFCS' krav til et styrket cyberforsvar (10.1)
6.3.5 A-C	Opfølgning på deltagelsen i undervisning og awareness aktiviteter	Ja	Nej	Nærmeste ledelse	-
6.3.6 A-C	Kontrol af at medarbejderne ved, hvordan de skal hændelsesrapportere	Ja	Nej	Nærmeste ledelse	-
6.3.7 B-C	Uddannelse af kryptopersonel	Ja	Ja	Nærmeste ledelse ved myndigheder med krypto-personel	FKOBST 358-1 (bilag 3 til kap. 6)
6.4	Disciplinær processer (sanktioner)				
6.4.1 A-C	Kommunikation om sanktioner i forvaltningsgrundlaget	Ja	Nej	Alle myndigheder og enheder	-
6.4.2 A-C	Kommunikation om sanktioner ved tiltrædelse	Ja	Nej	Nærmeste ledelse	-
6.5	Ansættelsesforholdets ophør eller ændring				
6.5.1 A-C	Vurdering af behov for information om ansvar og forpligtelser efter fratrædelse	Ja	Nej	Nærmeste ledelse	Se også 6.2
6.5.2 A-C	Kommunikation ved ændrede forpligtelser	Ja	Nej	Nærmeste ledelse	-
6.5.3 C	Information om ansvar og forpligtelser på fratrædelsessamtale	Ja	Nej	Nærmeste ledelse	-
6.6	Fortroligheds- og non-disclosure aftaler				

6.6.1 A-C	Identifikation og gennemgang af krav til fortroligheds- og non-disclosure aftaler	Ja	Nej	Alle myndigheder og enheder	FKOBST 358-1 (kap. 2 og 8)
6.7	Fjernarbejde				
6.7.1 A-C	Risikovurdering af fjernadgang til netværk og implementering af foranstaltninger	Ja	Ja	Forretningsansvarlige	CFCS' krav til et styrket cyberforsvar (8.1)
6.7.2 A-C	Implementering af tekniske minimumsforanstaltninger	Ja	Ja	It-leverandører	Se også krav nr. 2, 10 og 20 i Tekniske minimumskrav 2023
6.7.3 B-C	Godkendelse af fjernadgang til klassificerede systemer fra CFCS	Ja	Ja	Alle myndigheder og enheder	-
6.8	Hændelsesrapportering				
Implementeres gennem bestemmelserne i kapitel 10 og FMNBST 280-2					
Fysiske foranstaltninger					
7.1	Fysisk perimetersikring				
Implementeres gennem bestemmelserne i kapitel 7					
7.2	Fysisk adgangskontrol				
Implementeres gennem bestemmelserne i kapitel 7					
7.3	Sikring af kontorer, lokaler og faciliteter				
Implementeres gennem bestemmelserne i kapitel 7					
7.4	Overvågning af fysisk adgang				
7.4.1 A-C	Overvågning af fysisk adgang til lokaliteter	Nej	Nej	Alle myndigheder og enheder	FKOBST 358-1 (kap. 7)
7.5	Fysiske og miljømæssige trusler				
7.5.1 A-C	Risikostyring for it-services og systemer ift. fysiske og miljømæssige trusler	Ja	Ja	Alle myndigheder og enheder	Se krav til risikostyring i FMNBST 358-2
7.6	Arbejde i sikre områder				
Implementeres gennem bestemmelserne i kapitel 7 og lokale instrukser for militær sikkerhed					
7.7	Ryddeligt skrivebord og blank skærm				
7.7.1 A-C	Ryddeligt skrivebord	Ja	Nej	Alle myndigheder og enheder	FKOBST 358-1 (bilag 1 til kap. 7)

7.7.2 A-C	Oplysningspligt om brug af skærmlås m.v.	Ja	Nej	Alle myndigheder og enheder	FKOBST 358-1 (bilag 1 til kap. 7)
7.8	Placering og beskyttelse af udstyr				
7.8.1 A-C	Sikker placering og beskyttelse af udstyr	Ja	Nej	Alle myndigheder og enheder	FKOBST 358-1 (bilag 1 og 2 til kap. 6 samt kap. 16 i bilag 3 til kap. 6)
7.9	Udstyr og aktiver uden for organisationen				
7.9.1 A-C	Fastlæggelse af ansvarsforhold	Ja	Nej	Alle myndigheder og enheder	-
7.9.2 A-C	Passende foranstaltninger herunder brugerinstrukser	Ja	Ja	Alle myndigheder og enheder	Se også 6.7
7.9.3 C	For profil C klassificerede systemer områdegodkendelse fra FE	Ja	Ja	Forretningsansvarlige	Sikkerhedscirkulæret
7.10	Håndtering af lagermedier				
7.10.1 A-C	Procedurer for håndtering af lagermedier, herunder med minimumskrav ift. mærkning, klassifikation, genanvendelse og destruktion samt kryptering	Ja	Ja	Alle myndigheder og enheder	FKOBST 358-1 (kap. 1 og 4) Se også 7.14
7.11	Forsyningssikkerhed				
7.11.1 A-C	Foranstaltninger mod forsyningssvigt	Nej	Nej	It-leverandører	FKOBST 358-1 (underbilag 2 til bilag 3 til kapitel 7)
7.11.2 A-C	Test og tilpasning af foranstaltninger	Ja	Nej	It-leverandører	-
7.11.3 B-C	Redundante netværksforbindelser og redundant kabelføring	Nej	Nej	It-leverandører	Se også 5.30
7.12	Sikring af kabler				
7.12.1 A-C	Beskyttelse af kabler til elektricitet og tele-	Ja	Nej	Alle myndigheder og enheder	For profil B og C systemer se også

	kommunikation mod indgreb, interferens og skader				FKOBST 358-1 (bilag 3 til kap. 6)
7.12.2 C	Lokale netværk (FTR og derover) skal godkendes af CFCS som led i en installationsakkreditering	Ja	Ja	Alle myndigheder og enheder	-
7.13	Vedligeholdelse af udstyr				
7.13.1 A-C	Vedligeholdelse af udstyr iht. leverandørens anbefalinger	Nej	Nej	Alle myndigheder og enheder	-
7.13.2 A-C	Kontrol af udstyr inden idriftsættelse	Nej	Nej	Alle myndigheder og enheder	-
7.13.3 A-C	Instruktion af leverandør eller reparatør om sikker destruktion	Ja	Nej	Alle myndigheder og enheder	Se også 7.10 om krav til destruktion
7.13.4 B-C	Sikkerhedsgodkendelse af reparatør eller overvågning af vedligeholdelse på tjenestestedet	Ja	Nej	Alle myndigheder og enheder	FKOBST 358-1 (bilag 5 til kap. 7)
7.13.5 B-C	Ingen opkobling til internettet	Nej	Nej	Alle myndigheder og enheder	-
7.13.6 B-C	Krav til undtagelsesvis vedligeholdelse uden for tjenestestedet	Ja	Nej	Alle myndigheder og enheder	-
7.14	Sikker bortskaffelse eller genbrug af udstyr				
7.14.1 A-C	Verifikation af sletning eller overskrivning af personoplysninger og andre følsomme data samt licensbeskyttet software	Nej	Nej	Alle myndigheder og enheder	Se også 7.10 om krav til destruktion
Tekniske foranstaltninger					
8.1	Slutbrugerudstyr				
8.1.1 A-C	Regler om sikker konfiguration og håndtering af slutbrugerudstyr	Ja	Ja	It-leverandører og forretningsansvarlige	Se også 8.9 om konfigurationsstyring

					Se også krav nr. 1, 4, 12 og 13 i Tekniske minimumskrav 2023
8.1.2 A-C	Kryptering af lagret information på mobilt udstyr og beskyttelse mod malware	Ja	Nej	It-leverandører	Se også krav nr. 3 i Tekniske minimumskrav 2023
8.1.3 A-C	Instrukser om regler og procedurer for beskyttelse af udstyr	Ja	Ja	It-leverandører	-
8.1.4 A-C	Indbygget privacy skærmfilter	Nej	Nej	It-leverandører	-
8.1.5 A-C	Instrukser og passende sikkerhedsforanstaltninger ved anvendelse af privat udstyr på gæstenetværk eller andre internetvendte tjenester	Ja	Ja	Alle myndigheder og enheder	-
8.1.6 B-C	Mærkning, registrering, opbevaring og transport af klassificeret mobilt udstyr	Ja	Nej	Alle myndigheder og enheder	Se krav i FKOBST 358-1 (kap. 4) Sikkerhedscirkulæret
8.1.7 B-C	Godkendelse ved CFCS af mobilt klassificeret udstyr	Ja	Ja	Forretnings- og it-ansvarlige	Sikkerhedscirkulæret
8.2	Privilegerede adgangsrettigheder				
8.2.1 A-C	Proces for begrænset og styret tildeling og anvendelse af privilegerede adgangsrettigheder	Ja	Ja	It-leverandører	Se også 5.15 om krav til adgangsstyring og krav nr. 6 i Tekniske minimumskrav 2023
8.2.2 A-C	Udløb af password efter maksimalt 30 dage	Ja	Nej	It-leverandører	-
8.2.3 A-C	Passwords på minimum 25 karakterer	Ja (hvis teknisk muligt)	Nej	It-leverandører	Se også 5.17
8.2.4 A-C	Dokumentation for tildeling af rettigheder	Ja	Ja	It-leverandører	-

8.2.5 A-C	Gennemgang af adgangsrettigheder årligt og ved organisationsændringer	Ja	Ja	It-leverandører	-
8.2.6 B-C	Halvårlig gennemgang af adgangsrettigheder	Ja	Ja	It-leverandører	-
8.3	Begrænset adgang til information				
8.3.1 A-C	Passende foranstaltninger til sikring af autoriseret adgang	Ja	Nej	It-leverandører	Se også 5.15 om krav til adgangsstyring
8.4	Adgang til kildekode				
8.4.1 A-C	Begrænset og styret adgang til kildekode, udviklingsværktøjer og softwarebiblioteker	Ja	Nej	It-leverandører	-
8.4.2 B-C	Implementering af funktionsadskillelse	Ja	Nej	It-leverandører	-
8.4.3 B-C	Stillingtagen til hjemtagning af kildekode	Ja	Nej	It-leverandører	-
8.5	Sikker autentifikation				
8.5.1 A-B	Multifaktor autentifikation af brugere	Nej	Nej	It-leverandører	-
8.5.2 A-C	Multifaktor autentifikation for internetvendte systemer og ved adgang til følsomme personoplysninger	Ja	Nej	It-leverandører	Se også krav nr. 8 og 10 i Tekniske minimums-krav 2023
8.5.3 A-C	Multifaktor autentifikation for privilegerede konti og halvårlig kontrol af dette	Ja	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (7.7)
8.5.4 A-C	Orientering om seneste log-on og mislykkede log-on forsøg	Ja (hvis teknisk muligt)	Nej	It-leverandører	-
8.5.5 A-C	Aktivering af låseskærm	Ja	Nej	It-leverandører	-
8.5.6 B-C	Multifaktor autentifikation af brugere	Ja	Nej	It-leverandører	-

8.6	Kapacitetsstyring				
8.6.1 A-C	Kapacitetsplaner for systemer	Ja	Ja	Koncerninterne it-leverandører i dialog med forretningsansvarlige	-
8.6.2 A-C	Overvågning og justering af kapacitet	Ja	Nej	It-leverandører	-
8.7	Beskyttelse mod malware				
8.7.1 A-C	Endpoint beskyttelse mod malware med automatisk opdatering	Ja (hvis teknisk muligt)	Nej	It-leverandører	Se også 8.32 om ændringshåndtering Se også krav nr. 1 og 4 i Tekniske minimumskrav 2023
8.7.2 C	Anvendelse af min. to leverandører af forskellige typer af værktøjer, hvad angår dataoverførsler via datadioder	Ja	Nej	It-leverandører	-
8.8	Styring af tekniske sårbarheder				
8.8.1 A-C	Processer og procedurer samt roller og ansvar for styring og håndtering af sårbarheder	Ja	Ja	It-leverandører	Se også 8.32 om ændringshåndtering Se også krav nr. 4 og 7 i Tekniske minimumskrav 2023
8.8.2 A-C	Teknisk risikovurdering af systemer og understøttende aktiver	Ja	Ja	It-leverandører	-
8.8.3 A	Årlige sårbarhedsscanninger af internetvendte systemer	Ja	Ja	It-leverandører	-
8.8.4 A-C	Penetrationstest af internetvendte systemer	Nej	Ja	It-leverandører	-
8.8.5 A-C	Politik for sikkerhedsopdatering	Ja	Ja	It-leverandører	CFCS' krav til et styrket cyberforsvar (2.3)
8.8.6 A-C	Sikkerhedsopdatering af systemer, klienter og slutbrugerudstyr	Ja	Nej	It-leverandører og slutbrugere	Se også krav nr. 5, 13 og 19 i Tekniske minimumskrav 2023

8.8.7 A-C	Dialog med forretningen om sårbarhedsstyringen	Ja	Ja	Koncerninterne it-leverandører	-
8.8.8 B-C	Halvårlige sårbarheds-scanninger af internetvendte systemer	Ja	Ja	It-leverandører	CFCS' krav til et styrket cyberforsvar (6.4)
8.8.9 B-C	Penetrationstest af systemer generelt	Ja	Ja	It-leverandører	-
8.9	Konfigurationsstyring				
8.9.1 A-C	Konfigurationer, herunder sikkerhedskonfigurationer, i hardware, software, services og netværk skal etableres, dokumenteres, implementeres, overvåges og løbende verificeres.	Ja	Ja	It-leverandører	Se også 8.32 om ændringshåndtering
8.9.2 C	Årlig kontrol af netværks-dokumentationen for samfundskritiske systemer	Ja	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (6.3)
8.10	Sletning af information				
8.10.1 A-C	Sletning iht. gældende lovgivning og når det ikke længere er påkrævet at gemme information og data	Ja	Ja	Alle myndigheder og enheder	Se også 7.14 og 8.13
8.10.2 A-C	Krav til sletning skal fremgå af leverandøraftaler	Ja	Ja	Forretningsansvarlige	Se også 5.20
8.10.3 A-C	Mulighed for genskabelse af information og data skal fremgå af sikkerheds-dokumentationen	Ja	Ja	It-leverandører	-
8.10.4 B-C	Sletning af information fra mistede enheder ved Remote Wipe	Ja (hvis teknisk muligt)	Nej	It-leverandører	-
8.11	Datamaskering				

8.11.1 A-C	Datamaskering iht. gældende lovgivning og databehandleraftaler	Ja	Nej	Dataansvarlige myndigheder	Se også 8.24 om kryptering
8.12	Forebyggelse af datalækage				
8.12.1 A-C	Forebyggende værktøjer på systemer, netværk og udstyr	Nej	Nej	It-leverandører	-
8.12.2 B-C	Forebyggende værktøjer på systemer, netværk og udstyr	Ja	Nej	It-leverandører	-
8.13	Backup				
8.13.1 A-C	Vedligehold og test af backup	Ja	Ja	It-leverandører	-
8.13.2 A-C	Procedure for backup	Ja	Ja	It-leverandører	-
8.13.3 A-C	Vurdering af opbevaring og fysisk beskyttelse	Ja	Ja	It-leverandører	-
8.13.4 C	Kvartalsvis kontrol af backup, opbevaring af kopi offline og af reetablering af data fra backuppen hvad angår samfundskritiske systemer	Ja	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (3.1 og 3.2)
8.14	Redundante informationsbehandlingsfaciliteter				
8.14.1 A-C	Redundans iht. aftalte krav til tilgængelighed	Ja	Nej	It-leverandører	Se også 5.30
8.15	Logning				
8.15.1 A-C	Logning af sikkerheds-betydende aktiviteter, afvigelser og hændelser	Ja	Ja	It-leverandører	CFCS' krav til et styrket cyberforsvar (5.1) Se også krav nr. 14 i Tekniske minimums-krav 2023
8.15.2 A-C	Beskrivelse af omfang og håndtering af logs i sikkerhedsdokumentationen	Ja	Ja	It-leverandører	-

8.15.3 A-C	Krav til opbevaring af logs for internetvendte tjenester og centrale interne systemer	Ja	Ja	It-leverandører	-
8.15.4 A-C	Detailregistrering af adgang til personoplysninger ved behandling af følsomme og fortrolige personoplysninger	Ja	Ja	It-leverandører	-
8.15.5 C	Årlig kontrol af logning	Ja	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (5.2)
8.16	Monitorering				
8.16.1 A-C	Monitorering af netværk, systemer og software	Nej	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (5.1)
8.16.2 A-C	Analyse af logs	Ja	Nej	It-leverandører	Se også 8.15
8.16.3 C	Kontrol af gennemgang af logs hvad angår samfundskritiske systemer	Ja	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (5.3)
8.17	Tidssynkronisering				
8.17.1 A-C	Tidssynkronisering	Ja	Nej	It-leverandører	-
8.18	Anvendelse af værktøjer til styring af privilegerede adgange				
8.18.1 A-C	Proces for tildeling af privilegerede rettigheder via værktøjerne	Ja	Ja	It-leverandører	Se også 8.32 om ændringshåndtering
8.19	Installation af software				
8.19.1 A-C	Procedurer til styring og godkendelse af software-installationer på produktionssystemer	Ja	Ja	It-leverandører	Se også 8.32 om ændringshåndtering
8.20	Netværkssikkerhed				
8.20.1 A-C	Opdaterede system- og netværksdiagrammer	Ja	Ja	It-leverandører	Se også 8.9 og 8.22
8.20.2 A-C	Services og porte der ikke anvendes skal lukkes	Ja	Nej	It-leverandører	-

8.20.3 B-C	Godkendelse ved CFCS hvis klassificerede systemer skal forbindes til andre systemer	Ja	Ja	Forretnings- og it-ansvarlige	Sikkerhedscirkulæret
8.20.4 C	Akkreditering af systemer og netværk der skal håndtere information klassificeret til FORTROLIGT eller derover	Ja	Ja	Forretnings- og it-ansvarlige	Sikkerhedscirkulæret
8.20.5 B	Akkreditering af systemer der skal transmittere information klassificeret TIL TJENESTEBRUG over internettet og/eller mellem flere myndigheder i staten	Ja	Ja	Forretnings- og it-ansvarlige	-
8.20.6 B	Akkreditering af kommunikationssystemer i øvrigt til kommunikation af information klassificeret TIL TJENESTEBRUG eller højere	Ja	Ja	Forretnings- og it-ansvarlige	-
8.21	Sikkerhed i netværksservices				
8.21.1 A-C	Identifikation, implementering og monitorering af sikkerhedsmekanismer, serviceniveauer og servicekrav	Ja	Ja	It-leverandører	Se også krav nr. 1 og 15 i Tekniske minimums-krav 2023
8.21.2 C	Årlig kontrol af konfiguration af firewallregler for samfundskritiske systemer	Ja	Nej	It-leverandører	CFCS' krav til et styrket cyberforsvar (4.2)
8.22	Netværkssegmentering				
8.22.1 A-C	Segmentering af brugervendte services, back-end services, klienter og privilegerede services	Ja	Nej	It-leverandører	Se også 8.20.1

8.22.2 A-C	Segmentering af kritiske eller sårbare systemer fra andre segmenter	Nej	Nej	It-leverandører	Se også 8.20.1
8.22.3 A-C	Management aktiviteter på infrastrukturkomponenter og services i eget segment	Ja	Nej	It-leverandører	Se også 8.20.1
8.23	Webfiltrering				
8.23.1 A-C	Blokering af adgang til visse hjemmesider	Ja	Nej	It-leverandører	Se også krav nr. 16 i Tekniske minimums-krav 2023
8.23.2 A-C	Eksponeringskriterier ift. blokering af adgange	Ja	Ja	It-leverandører	-
8.23.3 A-C	Procedurer for håndtering af afvigelser fra eksponeringskriterier	Ja	Ja	It-leverandører	-
8.24	Anvendelse af kryptografi				
8.24.1 A-C	Regler for anvendelse af kryptografi	Ja	Ja	Forretningsansvarlige og it-leverandører	Se også FKOBST 358-1 (bilag 3 til kap. 6), krav nr. 3, 9, 18 og 20 i Tekniske minimums-krav 2023 og GDPR
8.24.2 A-C	Procedurer for administration af kryptonøgler	Ja	Ja	It-leverandører	Se også FKOBST 358-1 (bilag 3 til kap. 6)
8.24.3 B-C	Kryptografisk metode skal være godkendt af den nationale it-sikkerhedsmyndighed hvad angår klassificerede systemer	Ja	Ja	Forretningsansvarlige i dialog med it-ansvarlige	Sikkerhedscirkulæret
8.25	Sikker udviklingscyklus				
8.25.1 A-C	Principper for udvikling af software og systemer	Ja	Ja	It-leverandører	Se også 5.8, 5.32 og 8.26-8.31
8.26	Applikationssikkerhed				

8.26.1 A-C	Sikkerhedskrav til nye applikationer og forbedringer	Ja	Ja	It-ansvarlige i dialog med forretningsansvarlige	-
8.26.2 B-C	Akkreditering inden idriftsættelse i klassificerede systemer	Ja	Ja	Forretningsansvarlige i dialog med it-ansvarlige	-
8.27	Sikkerhed i arkitekturudvikling				
8.27.1 A-C	Anvendelse af principper for udvikling af sikre løsninger i alle arkitekturlag	Ja	Ja	It-leverandører	-
8.27.2 A-C	Risikovurdering af anvendte teknologier og risiko-håndtering iht. risiko-håndteringsplan	Ja	Ja	It-leverandører	-
8.28	Principper for sikkerhed i softwareudvikling (sikker kodning)				
8.28.1 A-C	Principper for sikker kodning	Ja	Ja	It-leverandører	-
8.29	Sikkerhedstest				
8.29.1 A-C	Processer for sikkerhedstest under udvikling	Ja	Ja	It-leverandører	-
8.29.2 A-C	Sårbarhedsscanning før idriftsættelse	Ja	Ja	It-leverandører	-
8.29.3 A	Penetrationstest af internetvendte systemer	Nej	Ja	It-leverandører	-
8.29.4 B-C	Penetrationstest af systemer	Ja	Ja	It-leverandører	-
8.29.5 A-C	Kommunikation om sårbarheder	Ja	Nej	It-leverandører	-
8.29.6 C	Fastlæggelse af krav til sikkerhedstest i akkrediteringsplaner	Ja	Ja	Forretningsansvarlige i dialog med it-ansvarlige	-
8.30	Outsourced udvikling				
8.30.1 A-C	Tilsyn og overvågning af systemudviklingsaktiviteter med afsæt i en SKS	Ja	Ja	Koncerninterne it-leverandører	-

8.30.2 C	Fastlæggelse af sikkerheds- krav til udviklingsmiljøet i akkrediteringsplaner	Ja	Ja	Koncerninterne it- leverandører	-
8.31	Adskillelse af udviklings-, test- og produktionsmiljø				
8.31.1 A-C	Adskilte og sikrede udviklings-, test- og produktionsmiljøer	Ja	Ja	It-leverandører	Se også 8.20.1
8.32	Change Management (ændringshåndtering)				
8.32.1 A-C	Change Management proces	Ja	Ja	It-leverandører	-
8.32.2 A-C	Procedurer for ændringshåndtering	Ja	Ja	It-leverandører	-
8.32.3 A-C	Idriftsættelsestest af væsentlige ændringer	Ja	Ja	It-leverandører	-
8.33	Testdata				
8.33.1 A-C	Beskyttelse af testdata	Ja	Nej	It-leverandører	-
8.33.2 C	Fastlæggelse af krav til testdata i akkrediteringsplaner	Ja	Ja	Forretningsansvarlige i dialog med it-ansvarlige	-
8.34	Beskyttelse af systemer under audit				
8.34.1 A-C	Planlægning og aftaler om test i forbindelse med tilsyn	Ja	Ja	It-leverandører i dialog med forretningsansvarlige	-

KAPITEL 7

FYSISK SIKKERHED

1. INDLEDNING

Den fysiske sikkerhed har til formål at beskytte koncernens etableringer og enheder mod spionage, terror, sabotage, hærværk og tyveri mv. Uvedkommendes indtrængen og adgang til klassificerede informationer skal hindres eller imødegås. Dette sker ved at vælge og vedligeholde et optimalt og afbalanceret sæt af sikringsforanstaltninger inden for givne fysiske og økonomiske rammer.

De sikringsmæssige foranstaltninger omfatter mekanisk sikring, elektroniske overvågning og bevogtning.

Den fysiske sikkerhed skal dimensioneres efter princippet om risikostyring og grundlæggende minimumskrav, jf. kapitel 9.

Andre hensyn og regelsæt, herunder fredningsbestemmelser og arbejdsmiljøkrav, samt brand- og flugtvejskrav, kan gøre det umuligt at opfylde minimumskravene i dette kapitel. I givet fald skal Forsvarets Efterretningstjeneste (FE) inddrages, således at der evt. kan gives dispensation til en anden, sikkerhedsmæssigt forsvarlig løsning. Det samme gælder, hvis det vurderes, at en fravigelse af minimumskravene kan give en væsentlig besparelse, uden at hensynet til sikkerheden tilsidesættes.

2. FORMÅL

Formålet med dette kapitel er at beskrive de grundlæggende principper og minimumskrav for den fysiske sikkerhed i koncernen.

3. ANSVAR

Chefen er ansvarlig for, at der som led i risikostyringen udarbejdes risikovurderinger og på baggrund heraf sikringsplaner.

Ved alle bygge- og anlægsprojekter samt driftsprojekter skal overvejelser om de sikringsmæssige foranstaltninger indgå allerede i de tidligste faser af projektet. FE og Forsvarsmi-
nisteriets Ejendomsstyrelse (FES) skal skriftligt efterrettes om projektet og høres, om der evt. er supplerende krav udover det i FKOBST 358-1 beskrevne (se i øvrigt FES BST 610-1, kapitel 5).

FES har systemansvaret for etablering og drift af mekanisk sikring og elektronisk overvågning i koncernen. Ønsker om anskaffelser, etablering og ændringer af anlæg for mekanisk sikring og elektronisk overvågning fremsættes til FES.

4. RISIKOVURDERING

De fysiske sikringsforanstaltninger skal fastsættes på grundlag af en konkret risikovurdering. Den konkrete risikovurdering og det fastlagte sikringsniveau er styrende for de fysiske sikringsforanstaltninger. I fm. udarbejdelse af risikovurderingen foretages der en systematisk afvejning af trusler og mulige konsekvenser i forhold til de aktiver, der skal beskyttes. Vejledning til udarbejdelse af en risikovurdering fremgår af bilag 1 til kapitel 9. Vurderingen klassificeres efter indhold.

5. SIKRINGSPLAN

Vejledning for udarbejdelse af en sikringsplan fremgår af bilag 2 til kapitel 9. Planen klassificeres efter indhold og fordeles i begrænset antal.

6. OMRÅDEINDELING

Ved koncernens styrelser, stabe og myndigheder mfl., der opbevarer og behandler klassificeret materiale eller udfører aktiviteter (produktion mv.), som kræver fysisk sikkerhed, skal der etableres en områdeinddeling med varierede sikringsniveauer ud fra minimumskrav til opbevaring og sikring af det opbevarede materiale. Som en integreret del af fastsættelse af områdeinddeling skal der tages stilling til reaktionstiden. Der er f.eks. krav om reaktion fra en indsatsstyrke indenfor 5 eller 15 min. når der er tale om sikrede områder.

Sikringsniveauerne er opdelt i:

- Sikret område
- Kontrolleret område
- Overvåget område

6.1 Sikrede områder.

Område, hvor materiale, informationer mv. klassificeret FORTROLIGT og højere kan behandles og opbevares. Sikrede områder skal altid forelægges FE til evt. kommentering inden ibrugtagning. Hvis alle minimumskrav til den fysiske sikkerhed er overholdt vil der sædvanligvis ikke blive udfærdiget en formel skriftlig godkendelse, men alene en mail. Ved it-installationer skal gældende procedurer jf. kapitel 6 efterleves.

Sikrede områder opdeles og sikres således:

6.1.1 Kategori 1 område.

Er et område, hvor omfanget og karakteren af sikringsforanstaltningerne sikrer mod uvedkommendes adgang og indsigt.

Området skal sikres i overensstemmelse med følgende minimumskrav:

Adgangskontrol (Se også bilag 5)

- En tydelig defineret perimeter, der ved sine fysiske egenskaber kanaliserer legal passage gennem overvåget adgangsvej
- Der skal anvendes en sluse til kontrol af legal passage ved adgangsvejen til det sikrede område (se også underbilag 1 til bilag 5)
- Der etableres kontrol for identifikation af adgangsberettigede med henblik på udførelse af adgangs-, opholds- og udgangskontrol ved særligt adgangskort. Adgangskortet skal bæres synligt
- Kortet skal for fast tjenstgørende personel som minimum indeholde billede og navn på kortholderen/den adgangsberettigede. Gæstekort skal ikke indeholde billede og navn, men korthaveren skal kunne billedidentificeres, hvilket normalt sker i fm. udlevering af gæstekort
- Adgangskontrol skal foregå ved indsats af personel eller ved anvendelse af automatisk adgangskontrolanlæg
- Vedrørende adgangskriterier se bilag 5.

Sikringsniveau

Området skal være opført af stabile bygningsdele, der i skallen udgør en både fysisk og psykisk barriere. Området skal sikres således:

Enten:

Konstant bevogtning, der umiddelbart erkender og afværger uvedkommendes adgang eller forsøg herpå.

Eller:

Mekanisk sikring jf. RC 5 / RC 6 jf. EN 1627 – 1630.

Elektronisk overvågning iht. sikringsniveau 50/60, Ved verificeret alarm skal reaktion iværksættes i henhold til forholdsordren, og indsatsstyrken skal kunne afværge uvedkommendes adgang eller forsøg herpå inden for 5 min.

Ovenstående regler er gældende for allerede eksisterende kategori 1 områder, dvs. etableret før 31. december 2020.

Fra 1. januar 2021 er følgende krav til mekanisk sikring i kategori 1 områder gældende ved nyetablering og større renoveringer.

Ved sikringsniveau 50

Mekanisk sikring jf. EN 1627-30, RC 5 eller jf. EN 1143-1 grade 1, samt stabile bygningsdele med tilsvarende gennembrydningstid.

Alle døre skal være aflåst med to godkendte låseenheder IV. Der skal anvendes to af Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Ved sikringsniveau 60

Mekanisk sikring jf. EN 1627-30, RC 6 eller jf. EN 1143-1 grade 2, samt stabile bygningsdele med tilsvarende gennembrydningstid.

Alle døre skal være aflåst med to godkendte låseenheder IV. Der skal anvendes to af Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Det gælder for begge sikringsniveauer, at der ved verificeret alarm skal iværksættes reaktion i henhold til forholdsordren, og indsatsstyrken skal kunne afværge uvedkommendes adgang eller forsøg herpå inden for 5 minutter.

Kontorsikkerhed

Myndigheden udarbejder et kontrolsystem, jf. bilag 7 til kapitel 1, der sikrer, at materiale klassificeret FORTROLIGT og højere er opbevaret i sikkerhedsgodkendt opbevaringsmiddel, når det ikke er under fuld fysisk kontrol af en til FORTROLIGT eller højere klassifikation sikkerhedsgodkendt medarbejder.

6.1.2 Kategori 2 område

Er et område, hvor omfanget og karakteren af sikringsforanstaltningerne **standser/ hindrer** uvedkommendes adgang og indsigt.

Området skal sikres i overensstemmelse med følgende minimumskrav:

Adgangskontrol (Se også bilag 5)

- En tydelig defineret perimeter, der ved sine fysiske egenskaber kanalisere legal passage gennem overvåget adgangsvej
- Der skal anvendes en sluse til kontrol af legal passage ved adgangsvejen til det sikrede område. En undtagelse til kravet er våbenkamre, der er etableret i belægningsbygninger. Her er der ikke krav om en sluse (se også underbilag 1 til bilag 5)
- Der etableres kontrol for identifikation af adgangsberettigede med henblik på udførelse af adgangs-, opholds- og udgangskontrol ved særligt adgangskort. Adgangskortet skal bæres synligt
- Kortet skal for fast tjenstgørende personel som minimum indeholde billede og navn på kortholderen/ den adgangsberettigede. Gæstekort skal ikke indeholde billede og navn, men korthaveren skal kunne billedidentificeres, hvilket normalt sker i fm. udlevering af gæstekort

- Adgangskontrol skal foregå ved indsats af personel eller ved anvendelse af automatisk adgangskontrolanlæg
- Vedrørende adgangskriterier se bilag 5.

Sikringsniveau

Området skal være opført af stabile bygningsdele, der i skallen udgør en både fysisk og psykisk barriere. Området skal sikres således:

Enten:

- Konstant bevogtning, der umiddelbart erkender og afværger uvedkommendes adgang eller forsøg herpå.

Eller:

- Krav til mekanisk sikring ved sikringsniveau 20 og 30 er minimum stabile bygningsdele i f.eks. RC3 jf. EN 1627 – 1630.
- Krav til mekanisk sikring i sikringsniveau 40 er stabile bygningsdele i minimum RC 4 jf. EN 1627 – 1630.

Elektronisk overvågning iht. sikringsniveau 20/30/40, Ved verificeret alarm skal reaktion iværksættes i henhold til forholdsordren, og indsatsstyrken skal kunne afværge/standse uvedkommendes adgang eller forsøg herpå inden for 15 min.

Ovenstående regler er gældende for allerede eksisterende kategori 2 områder, dvs. etableret før 31. december 2020.

Fra 1. januar 2021 er følgende krav til mekanisk sikring i kategori 2 områder gældende ved nyetablering og større renoveringer.

Ved sikringsniveau 20 og 30

Krav til mekanisk sikring ved sikringsniveau 20 og 30 er som minimum stabile bygningsdele med en tilsvarende gennembrydningstid som RC3 jf. EN 1627 – 1630.

Alle døre skal være aflåst med en godkendt låseenhed III. Der skal anvendes en af Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Ved sikringsniveau 40

Mekanisk sikring jf. EN 1627-1630, RC 4 eller jf. EN 1143-1 grade 1, samt stabile bygningsdele med tilsvarende gennembrydningstid.

Alle døre skal være aflåst med to godkendte låseenheder IV. Der skal anvendes to af Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Kontorsikkerhed

Myndigheden udarbejder et kontrolsystem, jf. bilag 7 til kapitel 1, der sikrer, at materiale klassificeret FORTROLIGT og højere er opbevaret i sikkerhedsgodkendt opbevaringsmiddel når det ikke er under fuld fysisk kontrol af en til FORTROLIGT eller højere klassifikation - sikkerhedsgodkendt medarbejder.

6.2 Kontrolleret område

Område, hvor materiale, informationer mv. klassificeret TIL TJENESTEBRUG kan behandles og opbevares.

6.2.1 Kategori 3 område

Er et område, hvor omfanget og karakteren af sikringsforanstaltningerne hæmmer uvedkommendes adgang og indsigt.

Kategori 3 område skal sikres i overensstemmelse med følgende minimumskrav:

Adgangskontrol (Se også bilag 5)

- En tydelig defineret perimeter, der ved sine fysiske egenskaber kanalisere legal passage gennem overvåget adgangsvej. Der etableres normalt kontrol for identifikation af adgangssøgende med adgangskort ved indsats af personel eller ved anvendelse af automatiske adgangskontrolanlæg under anvendelse af medie (kort/brik) og korrekt personlig pin kode uden for tjenestetids ophør
- Der bør efter tjenestetids ophør ikke kunne ske ikke kontrolleret adgang af motorkøretøjer uden en godkendelse af tjenestedets sikkerhedsofficer eller ansvarlige chef
- Vedrørende adgangskriterier se bilag 5.

Sikringsniveau

Området skal være opført af bygningsdele, der i skallen udgør en fysisk barriere. Bygningskonstruktionerne kan bestå af såvel stabile som svage bygningsdele.

Området sikres normalt således:

- Uden for daglig tjenestetid gennemføres lejlighedsvis patruljering af indsatsstyrker for at konstatere evt. uregelmæssigheder og imødegå disse
- Mekanisk sikring foretages ved en sikkerhedsgodkendt aflåsning af adgangsveje. Adgangsveje /døre i bygninger skal som minimum aflåses med en sikkerhedsgodkendt låseenhed jf. F&P regelsæt.

Elektronisk overvågning anvendes normalt ikke.

Kontorsikkerhed

Myndigheden udarbejder bestemmelser for behandling, opbevaring og ophængning af materiale klassificeret TIL TJENESTEBRUG (se bilag 7 til kapitel 1). Bestemmelserne indarbejdes i sikkerhedsinstruksen.

Materiale klassificeret højere må ikke opbevares i området.

6.3 Overvåget område (periodisk)

Er et område, uden for militært etablissement, men med periodisk tilsyn, fx fritliggende magasiner og depoter samt militære myndigheder beliggende på civil område, hvor materiel, våben, ammunition og eksplosivstoffer kan behandles og opbevares.

6.3.1 Kategori 4 område

Er et område, hvor omfanget og karakteren af sikringsforanstaltningerne **standser/ hindrer/hæmmer** uvedkommendes adgang til området afhængigt af de etablerede sikringsforanstaltninger relateret til aktivernes interesseværdi for uvedkommende. Er et område, hvor materiale, informationer mv. klassificeret ikke højere end TIL TJENESTEBRUG kan behandles og opbevares. Hvis der undtagelsesvis er behov for opbevaring af materiale, informationer mv. klassificeret højere end TIL TJENESTEBRUG, skal der indhentes godkendelse ved FE.

Sikringsforanstaltninger skal være en kombination af mekaniske sikringsforanstaltninger, elektroniske overvågningsforanstaltninger og bevogtning.

Kategori 4 område skal sikres i overensstemmelse med følgende minimumskrav:

Adgangskontrol (Se også bilag 5)

- En synlig markeret afmærkning, indhegning eller et perimeterhegn, der medvirker til at advisere et område, hvor adgang er forbudt for uvedkommende
- Vedrørende adgangskriterier se bilag 5.

Sikringsniveau

Området sikres normalt således:

- **Mekanisk sikring**

- Området skal være opført af stabile bygningsdele, der i skallen udgør en fysisk barriere
- Bygningskonstruktionerne kan bestå af såvel svage som stabile bygningsdele
- Adgangsveje/døre i bygninger skal som minimum aflåses med en sikkerheds-godkendt låseenhed jf. F&P regelsæt
Den mekaniske sikring skal etableres iht. et sikringsniveau, der ækvivalerer sikringskravet til de opbevarede beholdninger herunder vitalt/sensitivt materiel jf. kapitel 3.

- **Elektronisk overvågning**

- Elektronisk overvågning iht. sikringsniveau 20/30/40

- **Bevogtning**

- Ved en verificeret alarm skal der reageres i henhold til forholdsordren. Ved alarm udsendes en indsatsstyrke for at konstatere uregelmæssigheder og imødegå disse

Kontorsikkerhed

Myndigheden udarbejder bestemmelser for behandling, opbevaring og ophængning af materiale klassificeret TIL TJENESTEBRUG (se bilag 7 til kapitel 1). Bestemmelserne indarbejdes i sikkerhedsinstruksen.

Materiale klassificeret højere må ikke opbevares i området.

7. SIKRINGSNIVEAU

De kombinerede sikringsforanstaltningers modstandsevne skal ækvivalere minimumskravene til sikring af klassificerede dokumenter og informationer, klassificeret materiel samt vitalt og/eller sensitivt materiel.

Som minimumskrav til sikringsforanstaltningernes modstandsevne er der opstillet seks sikringsniveauer, niveau 10 - 60. Disse niveauer er beskrevet i Forsikring og Pensions (F&P) retningslinjer for minimumskrav til tekniske sikringsforanstaltninger, jf. bilag 1.

Det nødvendige sikringsniveau fastsættes på grundlag af områdeinddeling og sikringskrav, således:

OMRÅDEINDELING / SIKRINGSNIVEAU

			SIKRINGSNIVEAU					
			10	20-0	30	40	50	60
OMRÅDE-INDELING	1	SIKRET					•	•
	2			•	•	•		
	3	KONTROLLERET	•					
	4	OVERVÅGET	•	•	•	•		

Eksempler på anlægsprojektering fremgår af underbilag 1 til bilag 1.

8. MEKANISK SIKRING

Mekanisk sikring omfatter som minimum stabile bygningsdele for sikring af grænseflader - mure, vægge, gulve, tage døre og vinduer. Herudover indgår sikkerhedsgodkendte låse, beslag, gitre og lignende, der gør op lukning og/eller gennembrydning vanskelig. Ved mekanisk sikring skelner man mellem skalsikring, cellesikring og objektsikring. Mekanisk sikring omfatter endvidere etablering af hegn mv. med henblik på forbedring af sikringsforanstaltningerne på etablissementet.

8.1 Skalsikring

Etablering af sikring i bygningens grænseflade således at opbevaring kan ske i valgfrie lokaler. Bygningens grænseflader skal være mekanisk sikrede og elektronisk overvågede. Adgang skal foregå fra overvåget/kontrolleret område til sikret område.

8.2 Cellesikring

Etablering af sikring i et eller flere lokaler (evt. til højere sikringsniveau) inden for skalsikringen. Cellens grænseflader skal være mekanisk sikrede og elektronisk overvågede

8.3 Objektsikring

Ved objektsikring skal der etableres elektronisk overvågning (EO) af objektet (stålskab, pengeskab eller sikringsskab), samt af rummet.

Ved objektsikring af f.eks. malerier eller andet af betydelig værdi skal FE godkende løsningen.

8.4 Perimetersikring

Perimeter/markering/områdesikring betegner en markering, en barriere eller et hegn, der etableres i omkredsen af udendørsarealer, med det formål yderligere at sikre og/eller markere et område, hvortil der ikke ønskes adgang for uvedkommende. Hegn, markering og evt. barriere kan suppleres med elektronisk overvågning.

Beskrivelse af mekanisk sikring fremgår af bilag 2.

9. ELEKTRONISK OVERVÅGNING

Elektronisk overvågning (EO) omfatter automatisk indbrudsalarmanlæg (AIA), adgangskontrolanlæg (ADK), TV- og videoovervågningsanlæg (TVO). Ved anvendelse af elektronisk overvågning skal AIA alarmer sendes til og alarmbehandles på en døgnbemandet kontrolcentral samt evt. til en lokal vagtcentral, der sikrer, at indsatsstyrker alarmeres og indsættes.

Elektronisk overvågning skal opbygges på en sådan måde, at antallet af uhensigtsmæssige alarmer reduceres mest muligt og at kravene til et fuldt adresserbart sikringssystem efterleves, således at eks. en verificeret alarm jf. F&P regelsæt kan alarmbehandles.

Hvis den elektroniske overvågning er af ældre dato, og derfor ikke er opbygget som verificeret overvågning, skal alarmen altid opfattes som en verificeret alarm.

Beskrivelse af metoder og krav til elektronisk overvågning fremgår af bilag 3.

9.1 Automatisk indbrudsalarmanlæg

Automatisk indbrudsalarmanlæg er et elektronisk overvågningsanlæg, der automatisk registrerer og alarmerer, når gennembrydning, op lukning eller forsøg herpå finder sted, samt når bevægelser i de overvågede lokaler eller områder finder sted.

9.2 Automatisk adgangskontrolanlæg

Automatisk adgangskontrolanlæg er et elektronisk kontrolanlæg, der automatisk kontrollerer, registrerer og tillader adgangsberettigedes ind- og ud passage. Ved adgang til sikrede områder skal der anvendes medie (brik eller kort) og personlig kode.

9.3 TV- og videoovervågningsanlæg

TV- og videoovervågningsanlæg (TVO) er et elektronisk overvågningsanlæg, der kontinuerligt optager billeder af f.eks. perimeterhegn, bygninger, områder, lokaler eller adgangsveje. TVO supplerer andre sikringssystemer, f.eks. indbrudsalarmanlæg og adgangskontrolanlæg. TVO skal kunne anvendes hele døgnet. TVO anvendes til verificering, til registrering og undersøgelse af hændelser eller præventivt.

Når TVO ønskes anvendt, skal der i kravspecifikationen tages stilling til kvaliteten af TVO, og dermed skal der angives et af følgende formater: Observation, Verifikation, Identifikation eller Inspektion, som entydigt fastlægger kravene til billedkvaliteten.

9.4 Overfaldstryk.

Overfaldstryk er en kontakt, der betjenes manuelt for at alarmere vagtpersonel (indsatsstyrke) eller politiet i en trusselsituation iht. gældende forholdsordre. Aktivisering af overfaldstrykket starter en overfaldsalarm i den kontrolcentral (KC), hvor alarmen terminerer. Overfaldstryk skal kunne verificeres fra kontrolcentralen ved enten indlytning eller videoverifikation.

9.5 Overvågning

Overvågning kan udføres som:

9.5.1 Skalovervågning

Skalovervågning omfatter overvågning af vinduer og døre i grænseflader.
(se underbilag 2 til bilag 1)

9.5.2 Rumovervågning

Rumovervågning omfatter oplukningsovervågning af vinduer, døre og porte i grænseflader suppleret med elektronisk overvågning af rummet (se underbilag 2 til bilag 1).

9.5.3 Celleovervågning

Celleovervågning omfatter elektronisk overvågning af cellen og overvågning af adgangsmuligheder (se underbilag 2 til bilag 1).

9.5.4 Objektovervågning

Objektovervågning omfatter elektronisk overvågning af objektet.
(se underbilag 2 til bilag 1)

9.5.5 Overvågning af adgangskontrol, perimeter og områder

Overvågning og monitorering af adgangskontrol, perimeter og områder kan etableres ved TVO og/eller ADK.

Elektronisk overvågning som supplement til fysisk perimetersikring (hegn) skal vurderes i relation til begrænsning af u hensigtsmæssige alarmer.

TVO af områder kan med fordel kombineres med andre detektorer, der kan alarmere om, at der sker aktivitet i det overvågede område.

9.6 Belysning.

Belysning kan gennemføres som permanent belysning eller som detektoraktiveret belysning. Belysningen kan være synlig (hvidt lys) for etablering af identifikation eller usynligt lys (f.eks. IR-belysning) for anvendelse af kamera om natten.

10. BEVOGTNING

Bevogtning er den del af den fysiske sikkerhed, der omfatter anvendelse af bevæbnet personel til overvågning, patruljering og reaktion på alarmer mv. samt ledsagelse af transporter. Bevogtningen har til formål at imødegå og hindre uvedkommendes indtrængen og adgang til personel og til vitalt og/eller sensitivt materiel, herunder information, våben, ammunition og eksplosivstoffer.

Bevogtning af områder og objekter skal tilrettelægges således, at der kan indsættes et eller flere indsatshold på mindst to mand. Antallet af indsatshold afhænger af størrelse/antal af områder, der skal bevogtes og reaktionstiden til disse. Antallet fastsættes efter koordinat mellem de berørte myndigheder af den myndighed, der har ansvaret for udførelse af bevogtningen. Afstandsmæssige forhold kan afstedkomme krav om tilstedeværelse af indsatskøretøj. Indsats skal kunne ske uden at udførelsen af adgangskontrol og overvågning af alarmanlæg kompromitteres. Til støtte for bevogtningen kan der indsættes hunde jf. gældende bestemmelser.

Det aktuelle behov for bevogtning udledes af risikovurderingen og fastsættes i sikringsplanen. Bevogtning gennemføres på døgnbasis.

En nærmere beskrivelse af bevogtning fremgår af bilag 4.

10.1 Ansvar.

10.1.1 Forsvarskommandoen.

Forsvarskommandoen (FKO) udarbejder og vedligeholder Forsvarets Beredskabsplan ([FKOBST O.120-1](#)) der fastsætter planlægningsgrundlaget for gennemførelse af bevogtning under alle forhold (bevogtningstrin 0-3).

Indeværende bestemmelse fastsætter de overordnede bestemmelser for den daglige bevogtning af koncernens etableringer (bevogtningstrin 0 og 1).

10.1.2 Forsvarets Efterretningstjeneste.

Indeværende bestemmelse udarbejdes og vedligeholdes af FE. Bestemmelsen fastsætter de overordnede bestemmelser for bevogtning af koncernens etableringer og transporter.

10.1.3 Styrelser, stabe og myndigheder.

Styrelser, stabe og myndigheder har ansvaret for at der sker planlægning, tilrettelæggelse og gennemførelse af bevogtning indenfor deres respektive myndighedsområder, jf. FKOBST O.120-1.

FKO udgiver supplerende bestemmelser for bevogtningstjeneste under øvelser og internationale operationer.

10.2 Tilsyn med fysisk sikkerhed

Tilsynet er ikke en del af bevogtningstjenesten og kan udføres af ubevæbnede enkeltpersoner, der ikke er uddannede i bevogtningstjeneste. Tilsynet kan dog også udføres af bevogtningspersonel, herunder af indsatsstyrker som led i deres patruljering. Områder og objekter uden for militært etablissement (overvågede områder) tilses periodisk. Ved tilsynet kontrolleres den mekaniske sikring (perimeter, aflåsning, bygningsdele, evt. belysning mm.), samt om installationer til elektronisk overvågning er aktiveret. Endvidere kontrolleres det, om der er forøvet hærværk eller gjort forsøg på indbrud.

Kvalitetskontrol skal foretages af mekanisk sikring og elektronisk overvågning af fagteknisk sikringskyndige med detaljeret kendskab og ekspertviden om koncernens minimumskrav til sikringsanlæg, sikringssystemer og sikringsinstallationer.

10.3 Uddannelse.

Det påhviler enhver chef, der afgiver personel til udførelse af bevogtning at sikre sig, at

det er uddannet i våbenbrug og "forhold som bevogtningsstyrke" samt i etablissemets/enhedens generelle vagtbestemmelser. Dette er en nødvendig forudsætning for, at bevogtningspersonellet kan optræde med den fornødne myndighed og sikkerhed.

11. KONTROL AF FÆRDEL

Al færdsel i fm. sikrede områder skal kontrolleres ved

- adgangskontrol
- opholdskontrol og
- udgangskontrol.

Al færdsel i fm. kontrollerede områder skal efter normal arbejdstids ophør kontrolleres med f.eks. bom eller port.

Hvis adgangskontrollen alene udføres vha. automatisk adgangskontrol anlæg, må der ikke alene anvendes bom. Bommen skal suppleres med dør eller port.

Ind- og udgangskontrol skal udføres af personel eller ved anvendelse af automatiske adgangskontrolanlæg ved anvendelse af adgangskort og personlig kode.

11.1 Adgangskontrol.

Kontrol ved indgang udføres for at tilsikre, at kun dertil autoriseret og evt. ledsaget personel får/har adgang til området.

11.2 Opholdskontrol.

Opholdskontrol udføres for at kontrollere, om personer, der befinder sig i områderne, er autoriseret hertil eller ledsaget. Som led i opholdskontrollen skal der, afhængig af områdekategori, udleveres adgangskort til de dertil autoriserede og besøgende.

11.3 Udgangskontrol.

Udgangskontrol udføres for at kontrollere, at alle personer, der er passeret ind, også senere passerer ud.

En nærmere beskrivelse af kontrol af færdsel fremgår af bilag 5.

12. STØTTEVÆRKTØJ

Til brug for internationale operationer er der udarbejdet et støtteværktøj (kapitel 5, bilag 2, pkt. 5), der kan hjælpe sikkerhedsofficeren ved vurderingen af den fysiske sikkerhed.

Værktøjets del 8 fokuserer på, hvad der skal beskyttes, og dermed hvilke krav der skal stilles til såvel mekanisk sikring som elektronisk overvågning.

FASTLÆGGELSE AF SIKRINGSNIVEAUER

Ref.: [Brancheorganisationen Forsikring & pensions hjemmeside](#)

Underbilag:

1. Eksempler på anlægsprojektering.
2. Oversigt over fysiske sikringsforanstaltninger.

1. INDLEDNING

Forsikring & Pension (F&P) har udarbejdet retningslinjer for minimumskrav til tekniske sikringsforanstaltninger. De tekniske foranstaltninger er en kombination af mekaniske sikrings- og elektroniske overvågningsforanstaltninger, samlet benævnt indbrudssikring.

Princippet i F&P krav om indbrudssikring er:

- Jo mere "tyvetækkelige" materialer, jo større krav til indbrudssikring
- Jo større mængde af de pågældende materialer, jo større krav til indbrudssikring.

Ud fra dette princip er opstillet sikringsniveauer fra 10 – 60, med 10 som det niveau, der omfatter det laveste sikringskrav. Inden for niveauerne 20 – 60 vil der være mulighed for at vælge mellem en skalsikring, cellesikring og eller en objektsikring.

Generelt for samtlige sikringsniveauer gælder, at alle større åbninger i bygninger, rum og lokaler skal være lukket med døre, vinduer eller andre former for lukker.

Koncernen anvender DS/EN standard som kravstillende til de sikringsprodukter, som anvendes.

Koncernen har tidligere anvendt Standard-Tyv-Metoden (STM), benævnt SKAFOR og senere F&P, der blev erstattet af DS/EN standard pr. 01. januar 2016. Der findes stadig sikringsprodukter i koncernen, som er godkendt efter den metode. Ældre sikringsprodukter, som er godkendt efter den metode, er stadig godkendt i koncernen, men vil over tid blive udskiftet til produkter, som er godkendt efter DS/EN standard.

2. SIKRINGSNIVEAU 10

Alle døre skal være af en solid og stabil beskaffenhed, og låst med en af F&P sikkerheds godkendt låseenhed I.

Der etableres kontrolleret adgang til bygningen, enten ved hjælp af ADK eller et nøglesystem.

Celle- og objektsikring anvendes ikke på dette niveau.

3. SIKRINGSNIVEAU 20

Dette niveau anvendes kun i forbindelse med objektsikring i f.eks. bygninger, rum og lokaler. Se underbilag 2 til bilag 1.

4. SIKRINGSNIVEAU 30

Grænsefladen skal etableres i stabile bygningsdele, som modsvarer RC 3 jf. EN 1627 – 1630.

Fra 1. januar 2021 skal alle døre/porte/lemme i sikringsniveau 30 ved nyetablering og større renoveringer som minimum overholde RC3 jf. EN 1627 – 1630.

Alle døre skal være aflåst med en godkendt låseenhed III. Der skal anvendes en af Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Der skal etableres et F&P godkendt (min. klasse 3) indbrudsalarmanlæg (AIA).

AIA omfatter overvågning mod:

- åbning af døre, vinduer, porte og lemme i grænsefladerne,
- gennembrydning af glas i døre, vinduer, porte og lemme i grænsefladerne, samt rumovervågning.

Alarmoverførsel skal foregå til kontrolcentral og til en eventuel lokal vagtcentral.

5. SIKRINGSNIVEAU 40

Grænsefladen skal etableres i stabile bygningsdele, som modsvare RC 4 jf. EN 1627 – 30 eller jf. EN 1143-1 grade 1.

Døre og vinduer skal om minimum overholde RC 4 jf. EN 1627 – 1630 (F&P GUL klasse, HGR 2/HGR 1) eller med f.eks. fast RC 4 gitter eller en dør i EN 1143-1 Grade I. Glas skal overholde standarden EN 356 minimum P6B.

Alle døre skal være aflåst med en sikkerhedsgodkendt låseenhed IV. Der skal anvendes Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Fra 1. januar 2021 skal alle døre være aflåst med to sikkerhedsgodkendte låseenheder IV ved nyetablering og større renoveringer. Der skal anvendes Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Der skal etableres et F&P godkendt (min. klasse 3) indbrudsalarmanlæg (AIA).

AIA omfatter overvågning mod:

- åbning af døre, vinduer, porte og lemme i grænsefladerne, samt rumovervågning.
- gennembrydning af glas i døre, vinduer, porte og lemme i grænsefladerne og
- gennembrydning af døre, porte, lemme samt forstærket svage bygningsdele.

Hvor grænsefladerne i det sikrede område indgår som en del af garnisonens ydre perimenter, skal der ske en overvågning mod gennembrydning af grænsefladerne. Overvågningen skal detektere fysiske anslag på grænsefladen.

Ovenstående regler er gældende for allerede eksisterende sikrede områder dvs. etableret før 31. december 2020.

Fra 1. januar 2021 er følgende supplerende krav til den elektroniske overvågning gældende ved nyetablering og større renoveringer.

Der skal ske overvågning mod gennembrydning af grænsefladerne ind til det sikrede område. Overvågningen skal detektere fysiske anslag på grænsefladen.

Alarmoverførsel skal foregå til kontrolcentral samt til en eventuel lokal vagtcentral.

6. SIKRINGSNIVEAU 50

Grænsefladen skal etableres i stabile bygningsdele, som modsvare RC 5 jf. EN 1627 – 30 eller jf. EN 1143-1, grade 1.

Døre skal som minimum overholde RC5 jf. EN 1627 – 1630 (F&P BLÅ klasse HGR 2) eller en dør i EN 1143-1, grade 1.

Glas i døre skal undgås, hvor det er muligt. Evt. Glas i døre skal overholde standarden EN 356 minimum P7B.

Vinduer skal som minimum overholde standarden EN 356, P6B med gitter eller P7B. Overholder gitter EN 1627 – 1630, RC5 og sikres elektronisk mod gennembrydning kan krav til vindue tilsidesættes.

Alle døre skal være aflåst med en godkendte låseenhed IV. Der skal anvendes Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Fra 1. januar 2021 skal alle døre være aflåst med to sikkerhedsgodkendte låseenheder IV ved nyetablering og større renoveringer. Der skal anvendes Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Der skal etableres et F&P godkendt (min. klasse 3) indbrudsalarmanlæg (AIA).

AIA omfatter overvågning mod:

- åbning af døre, vinduer, porte og lemme i grænsefladerne, samt rumovervågning
- gennembrydning af glas i døre, vinduer, porte og lemme i grænsefladerne og
- gennembrydning af døre, porte, lemme samt forstærket svage bygningsdele.

Hvor grænsefladerne i det sikrede område indgår som en del af garnisonens ydre perimenter, skal der ske en overvågning mod gennembrydning af grænsefladerne. Overvågningen skal detektere fysiske anslag på grænsefladen.

Ovenstående regler er gældende for allerede eksisterende sikrede områder dvs. etableret før 31. december 2020.

Fra 1. januar 2021 er følgende supplerende krav til den elektroniske overvågning gældende.

Der skal ske overvågning mod gennembrydning af grænsefladerne ind til det sikrede område. Overvågningen skal detektere fysiske anslag på grænsefladen.

Alarmoverførsel skal foregå til kontrolcentral samt til en eventuel lokal vagtcentral.

7. SIKRINGSNIVEAU 60

Grænsefladen skal etableres i stabile bygningsdele, som modsvare RC 6 jf. EN 1627 – 30 eller jf. EN 1143-1, grade 2.

Døre skal som minimum overholde RC6 jf. EN 1627 – 1630 (~~F&P RØD klasse HGR 2~~) eller minimum EN 1143-1, grade 2.

Der må ikke anvendes glas i døre på dette sikringsniveau.

Vinduer skal som minimum overholde standarden EN 356, P7B med gitter eller P8B. Overholder gitter EN 1627 – 1630, RC6 og sikres elektronisk mod gennembrydning kan krav til vindue tilsidesættes.

Alle døre skal være aflåst med sikkerhedsgodkendte låseenheder IV. Der skal anvendes en af Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Fra 1. januar 2021 skal alle døre være aflåst med to sikkerhedsgodkendte låseenheder IV ved nyetablering og større renoveringer. Der skal anvendes Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY).

Der skal etableres et F&P godkendt (min. klasse 3) indbrudsalarmanlæg (AIA).
AIA omfatter overvågning mod:

- åbning af døre, vinduer, porte og lemme i grænsefladerne, samt rumovervågning
- gennembrydning af glas i døre, vinduer, porte og lemme i grænsefladerne og
- gennembrydning af døre, porte, lemme samt forstærket svage bygningsdele.

Hvor grænsefladerne i det sikrede område indgår som en del af garnisonens ydre perimenter, skal der ske en overvågning mod gennembrydning af grænsefladerne. Overvågningen skal detektere fysiske anslag på grænsefladen.

Ovenstående regler er gældende for allerede eksisterende sikrede områder dvs. etableret før 31. december 2020.

Fra 1. januar 2021 er følgende supplerende krav til den elektroniske overvågning gældende.

Der skal ske overvågning mod gennembrydning af grænsefladerne ind til det sikrede område. Overvågningen skal detektere fysiske anslag på grænsefladen.

Alarmoverførsel skal foregå til kontrolcentral samt til en eventuel lokal vagtcentral.

EKSEMPLER PÅ ANLÆGSPROJEKTERING

1. SIGNATURFORKLARING	7-3-1-2
2. ANVENDELSE OG OPBEVARING.....	7-3-1-3
2.1. Områdekategori 4, Sikringsniveau 30	7-3-1-3
2.2. Områdekategori 4, Sikringsniveau 40	7-3-1-3
2.3. Områdekategori 3, Sikringsniveau 10	7-3-1-4
2.4. Områdekategori 2, Sikringsniveau 20	7-3-1-4
2.5. Områdekategori 2, Sikringsniveau 30	7-3-1-5
2.6. Områdekategori 2, Sikringsniveau 40	7-3-1-5
2.7. Områdekategori 1, Sikringsniveau 50	7-3-1-6
2.8. Områdekategori 1, Sikringsniveau 60	7-3-1-6
3. MAGASINER	7-3-1-7
3.1. Sikring af magasin type 2	7-3-1-7
3.2. Sikring af magasin type 2a.....	7-3-1-8
3.3. Sikring af magasin type 3	7-3-1-9
3.4. Sikring af magasin type: Magasin med patronkasserum.....	7-3-1-10
3.5. Sikring af magasin type: Ammunitionsmagasin.....	7-3-1-11
3.6. Sikring af magasin type: Magasin	7-3-1-12
3.7. Sikring af magasin type: Magasin	7-3-1-13
3.8. Sikring af magasin type: Krudtmagasin	7-3-1-14
3.9. Sikring af magasin: Suspekt magasin type 2	7-3-1-15
3.10. Sikring af magasin type: Iglo.....	7-3-1-16
3.11. Sikring af magasin type: Iglo type 16	7-3-1-17
3.12. Sikring af magasin type 4	7-3-1-18

1. SIGNATURFORKLARING



Åbningskontakt



F&P sikkerhedsgodkendt lås, Låseenhed I jf. EN 1303



Sikkerhedsgodkendt lås, Låseenhed IV jf. EN 1303 med Forsvarets låsecylinder (ABLOY).



Mekanisk sikringsprodukt i form af gitter eller døre, lukker, vinduer m.m. jf. gældende DS/EN standard.



Elektronisk rumovervågning – bevægelsesføler.



Overvågning mod gennembrydning.



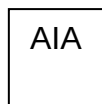
Seismisk detektor/vibrationsdetektor.



Forbikobler.

BP

Betjeningspanel.



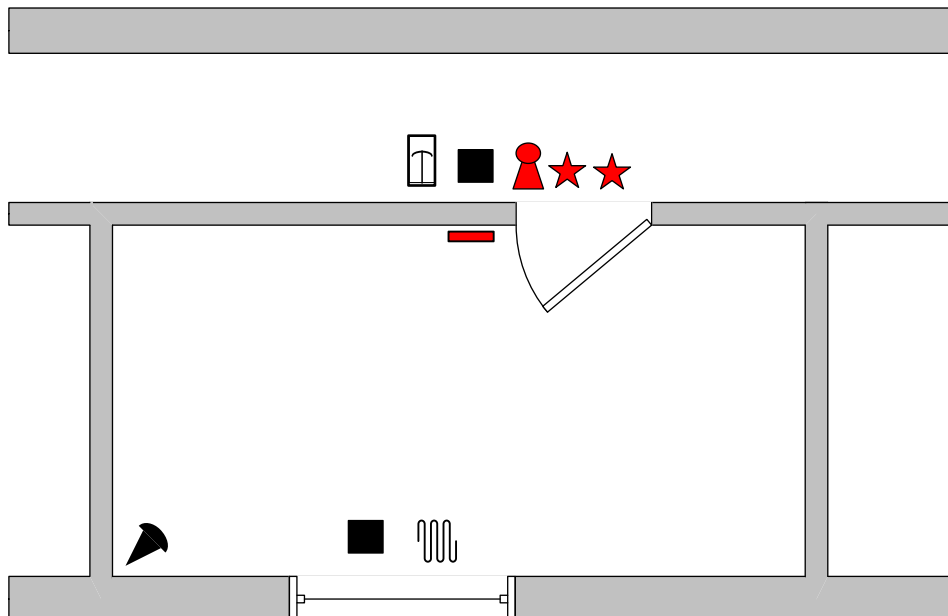
AIA- central.



Opbevaringsmiddel, militær klassifikation.

2. ANVENDELSE OG OPBEVARING

2.1. Områdekategori 4, Sikringsniveau 30



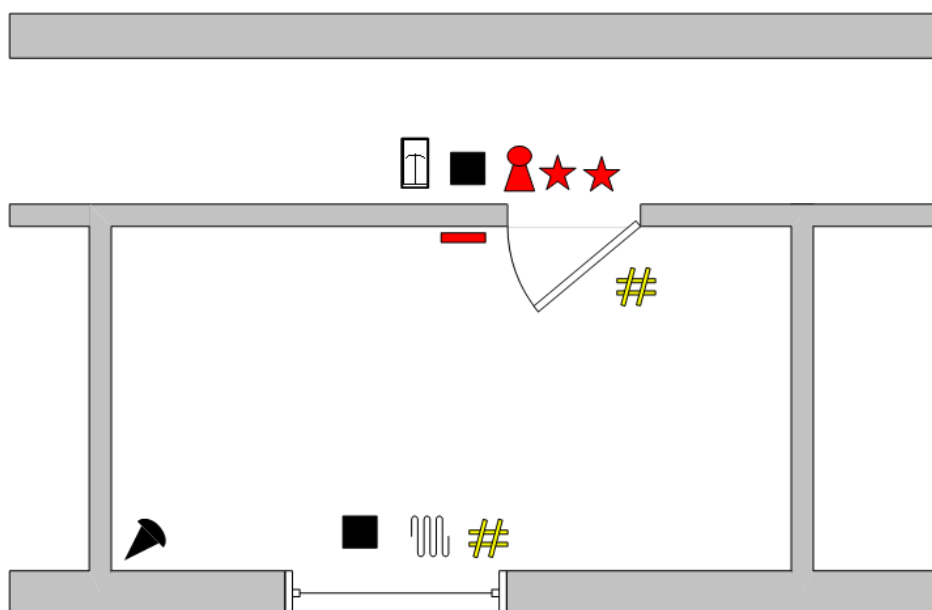
Mekanisk sikring: Sikkerhedsgodkendt lås og Forsvarets låsecylinder (ABLOY)

Elektronisk overvågning: **AIA**

Reaktionstid for vagt: **Efter tjenstedets bestemmelser**

Anvendelse: **Depot, TTJ**

2.2. Områdekategori 4, Sikringsniveau 40



Mekanisk sikring: **Sikkerhedsgodkendt lås og Forsvarets låsecylinder (ABLOY)**

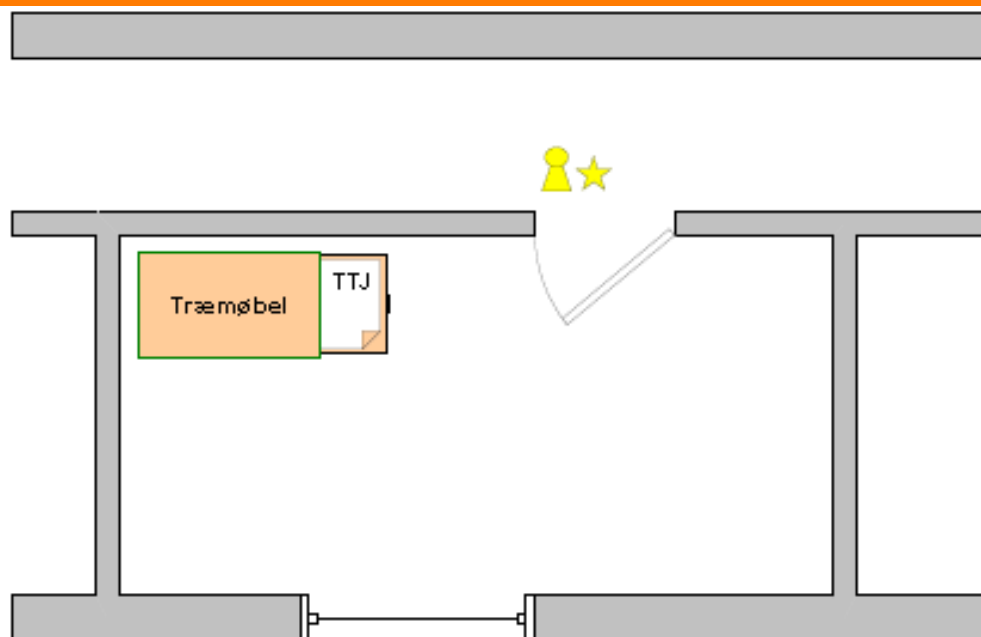
Mekanisk sikring: **Døre EN 1627 RC4, vinduer EN356 P6B eller fast gitter.**

Elektronisk overvågning: **AIA**

Reaktionstid for vagt: **Efter tjenestestedets bestemmelser**

Anvendelse: **Depot / Magasin, TTJ**

2.3. Områdekategori 3, Sikringsniveau 10

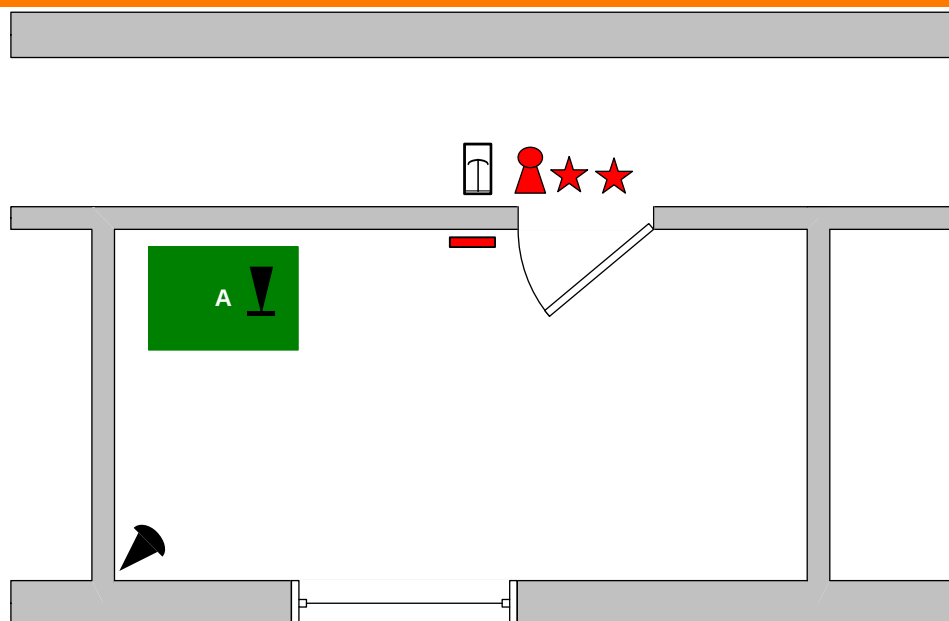


Mekanisk sikring: **Sikkerhedsgodkendt lås**

Elektronisk overvågning: **Ingen**

Anvendelse: **Sagsbehandling TTJ**

2.4. Områdekategori 2, Sikringsniveau 20



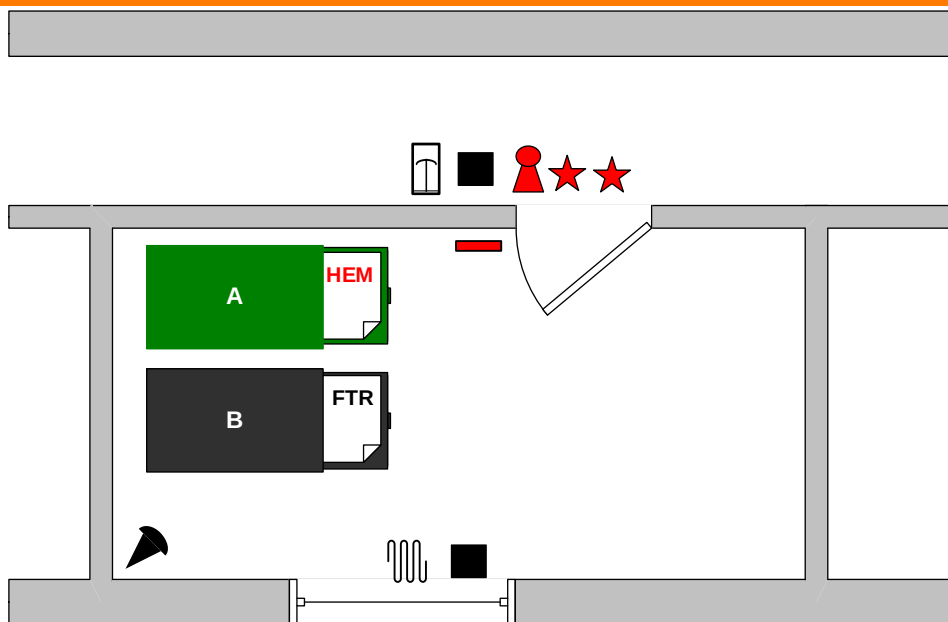
Mekanisk sikring: **Sikkerhedsgodkendt lås og Forsvarets låsecylinder (ABLOY)**

Elektronisk overvågning: **AIA, på eller af opbevaringsmiddel**

Reaktionstid for vagt: **Ingen**

Anvendelse: **Pengeopbevaring. Mindre mængde af klassificeret materiale til og med FTR**

2.5. Områdekategori 2, Sikringsniveau 30



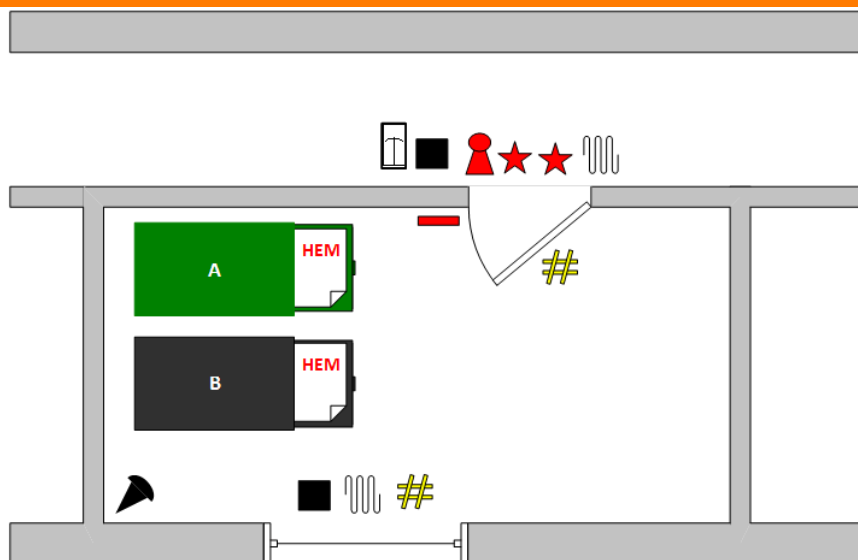
Mekanisk sikring: **Sikkerhedsgodkendt lås og Forsvarets låsecylinder (ABLOY)**

Elektronisk overvågning: **AIA.**

Reaktionstid for vagt: **Max. 15 min. Hvis reaktionsstyrken kan være fremme på max. 5 min. kan HEM opbevares i KLASS B opbevaringsmiddel.**

Anvendelse: **Sagsbehandling FTR / HEM**

2.6. Områdekategori 2, Sikringsniveau 40



Mekanisk sikring: **Sikkerhedsgodkendt lås og Forsvarets låsecylinder (ABLOY)**

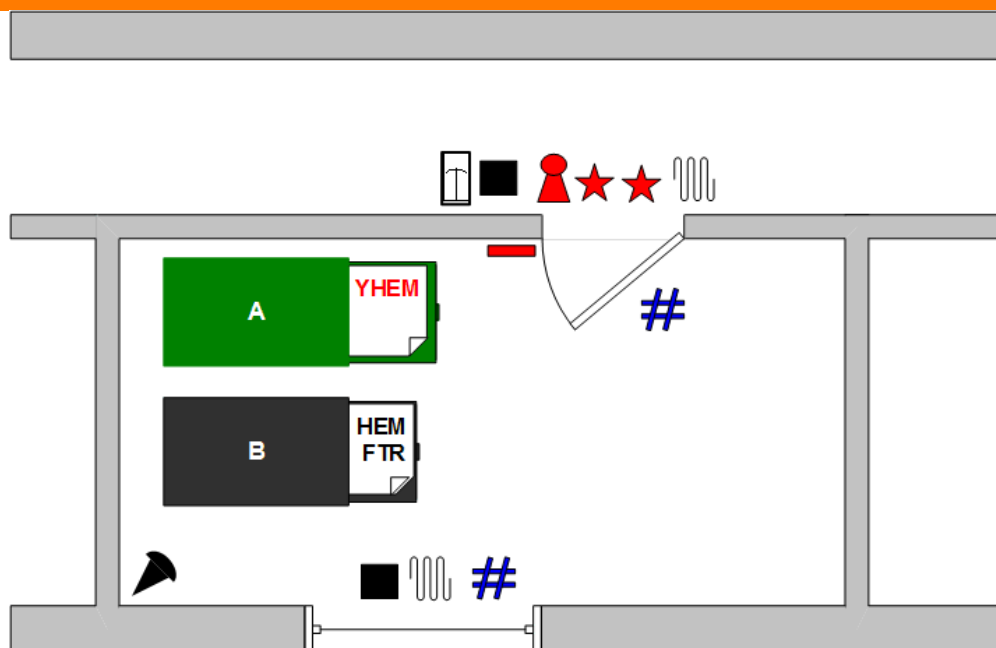
Mekanisk sikring: **Døre EN 1627 RC4, vinduer EN356 P6B eller fast gitter.**

Elektronisk overvågning: **AIA**

Reaktionstid for vagt: **Max. 15 min. Hvis KLASS B skab så er reaktionstid 5 min.**

Anvendelse: **Arkiv (NIV III) HEM.**

2.7. Områdekategori 1, Sikringsniveau 50



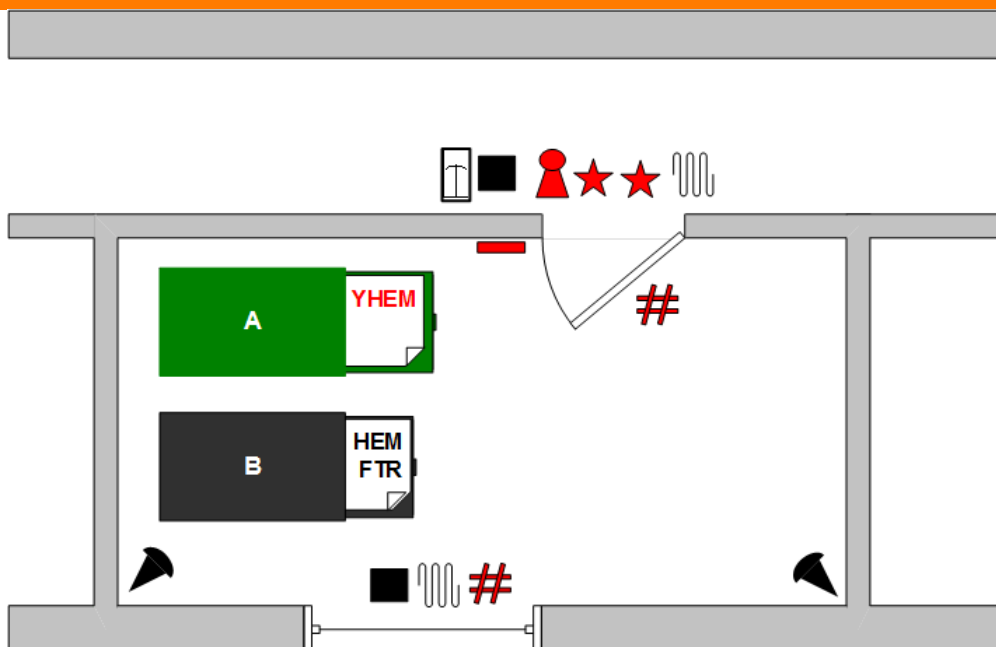
Mekanisk sikring: **Sikkerhedsgodkendt lås og Forsvarets låsecylinder (ABLOY)**

Mekanisk sikring: **Døre EN 1627 RC5, vinduer EN356 P7B eller fast gitter.**

Elektronisk overvågning: **AIA**

Reaktionstid for vagt: **Max. 5 min.**

2.8. Områdekategori 1, Sikringsniveau 60



Mekanisk sikring: **Sikkerhedsgodkendt lås og Forsvarets låsecylinder (ABLOY)**

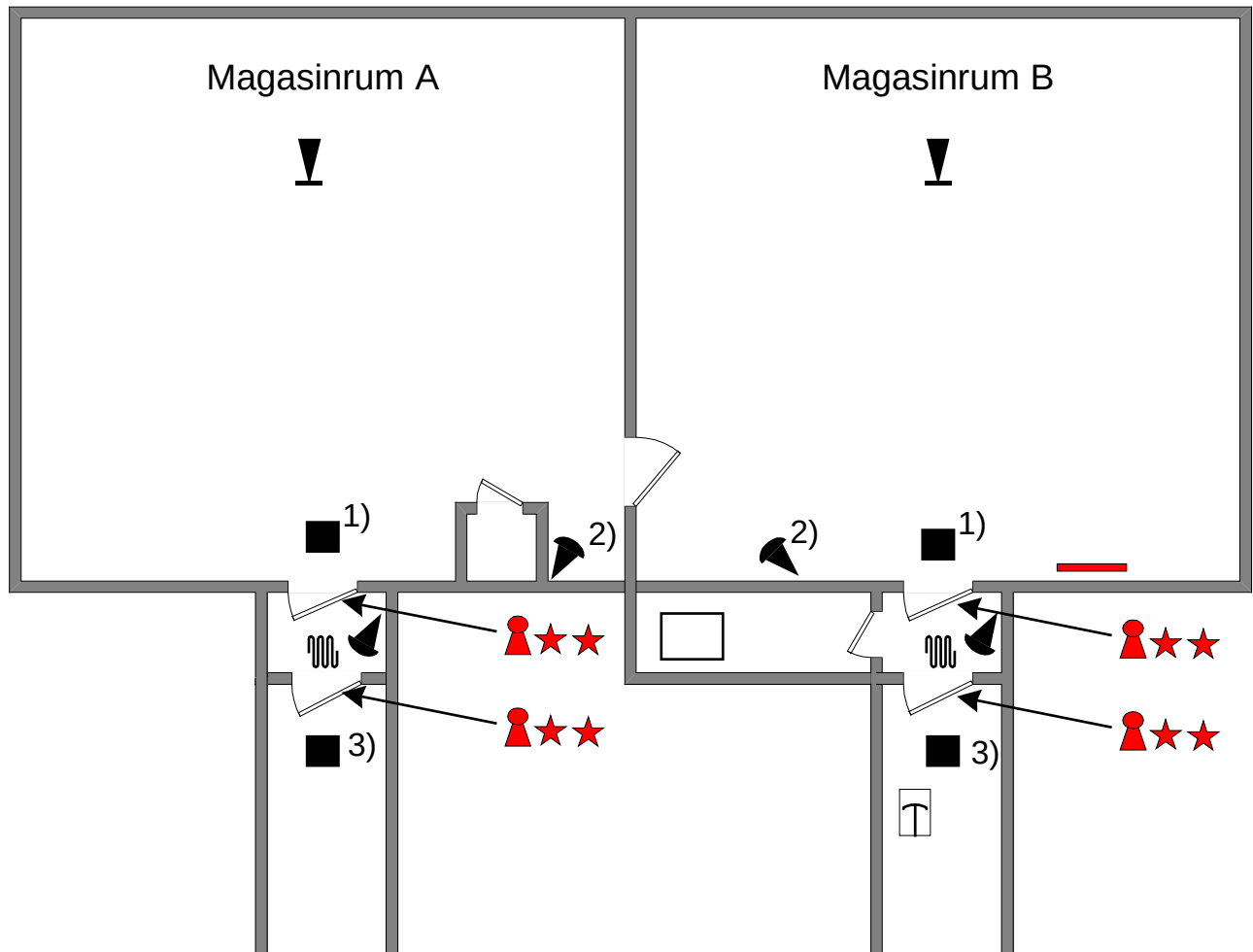
Mekanisk sikring: **Døre EN 1627 RC6, vinduer EN356 P7B med gitter eller EN356 P8B.**

Elektronisk overvågning: **AIA, ved 60C krav om bl.a. minimum 2 detektorer i cellen**

Reaktionstid for vagt: **Max. 5 min.**

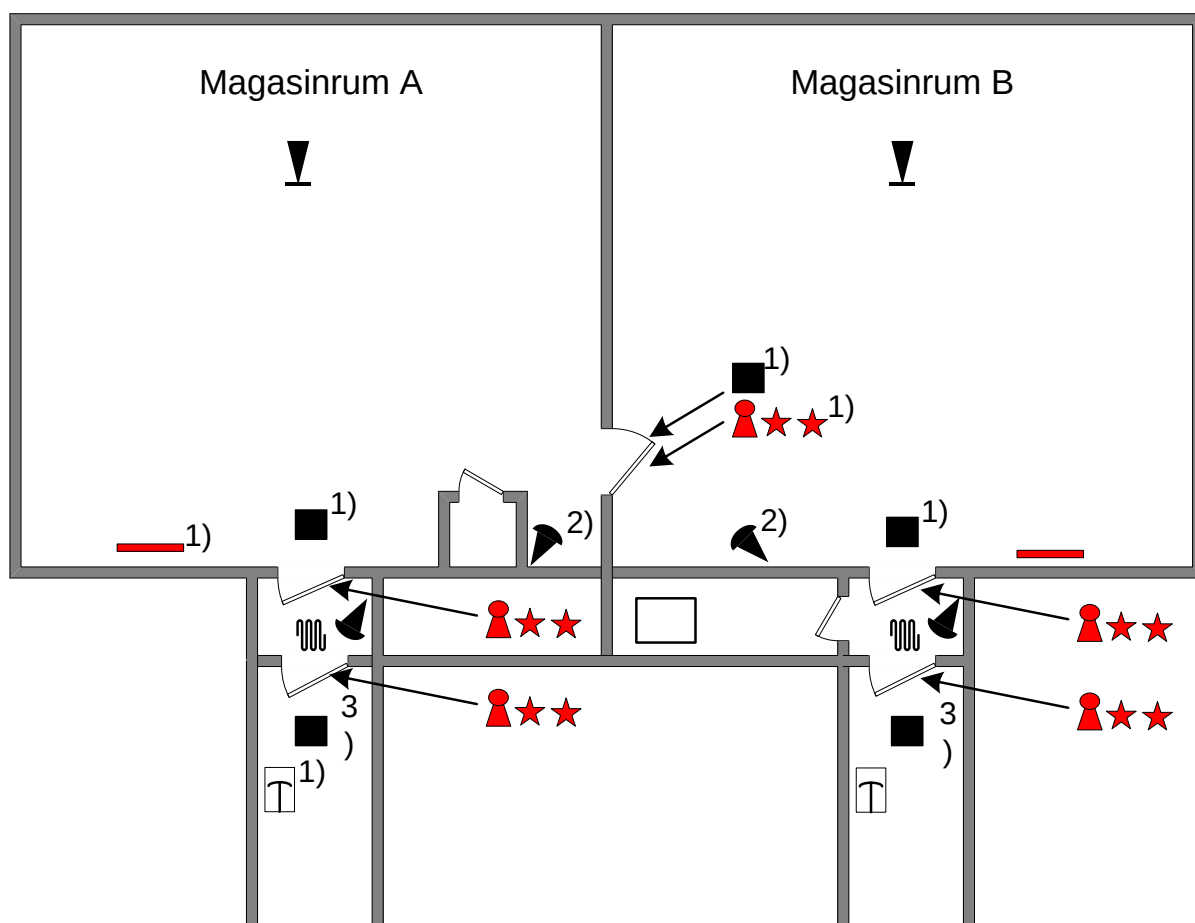
3. MAGASINER

3.1. Sikring af magasin type 2



- 1) Kan undlades
- 2) Beror på en konkret vurdering, men bør normalt være tilstede.
- 3) Eventuelt på låseoverfald

3.2. Sikring af magasin type 2a

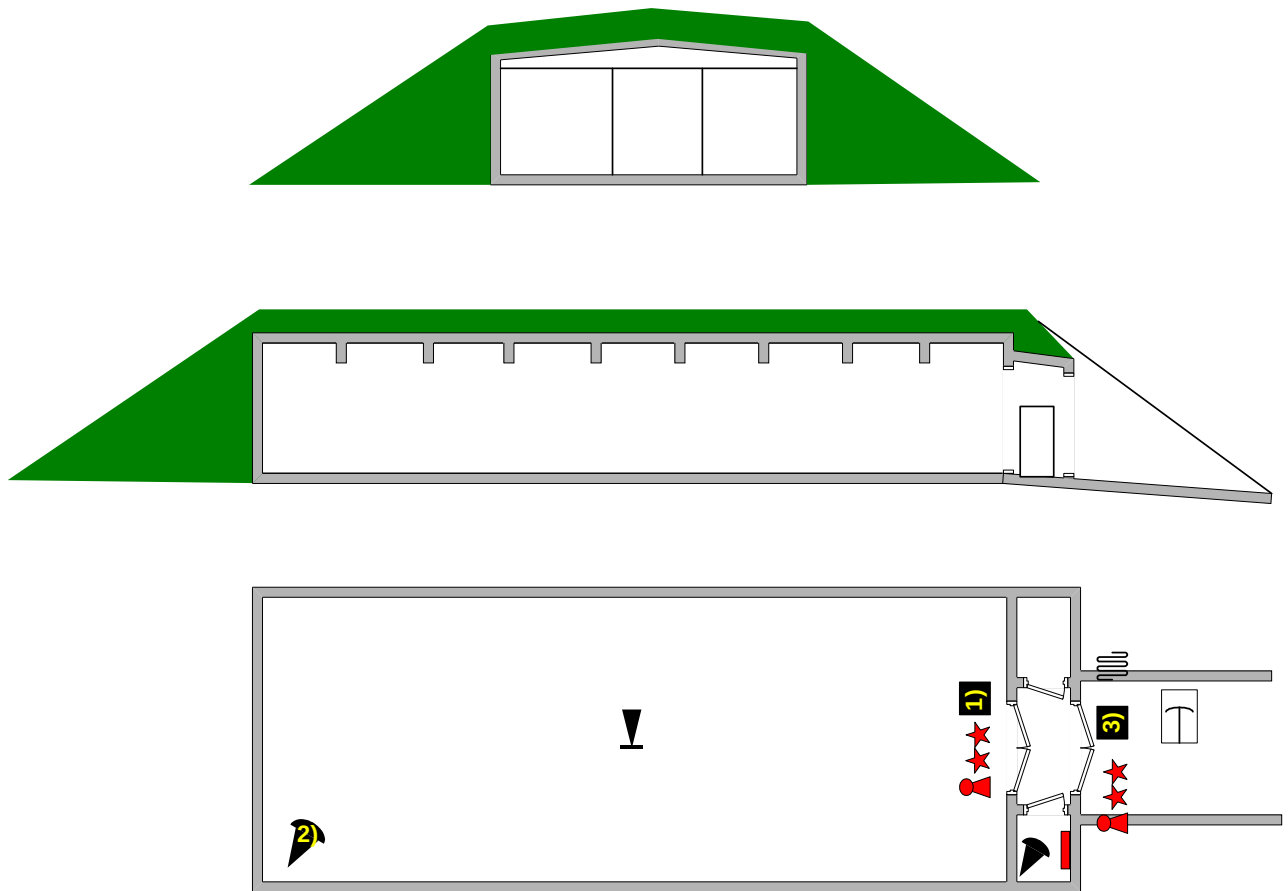


Eksempel udvisende 2 myndigheder med hver sin opbevaringsfacilitet, henholdsvis magasin A og B.

Hvis én myndighed råder over begge magasiner kan ét betjeningspanel og én forbikobler udelades

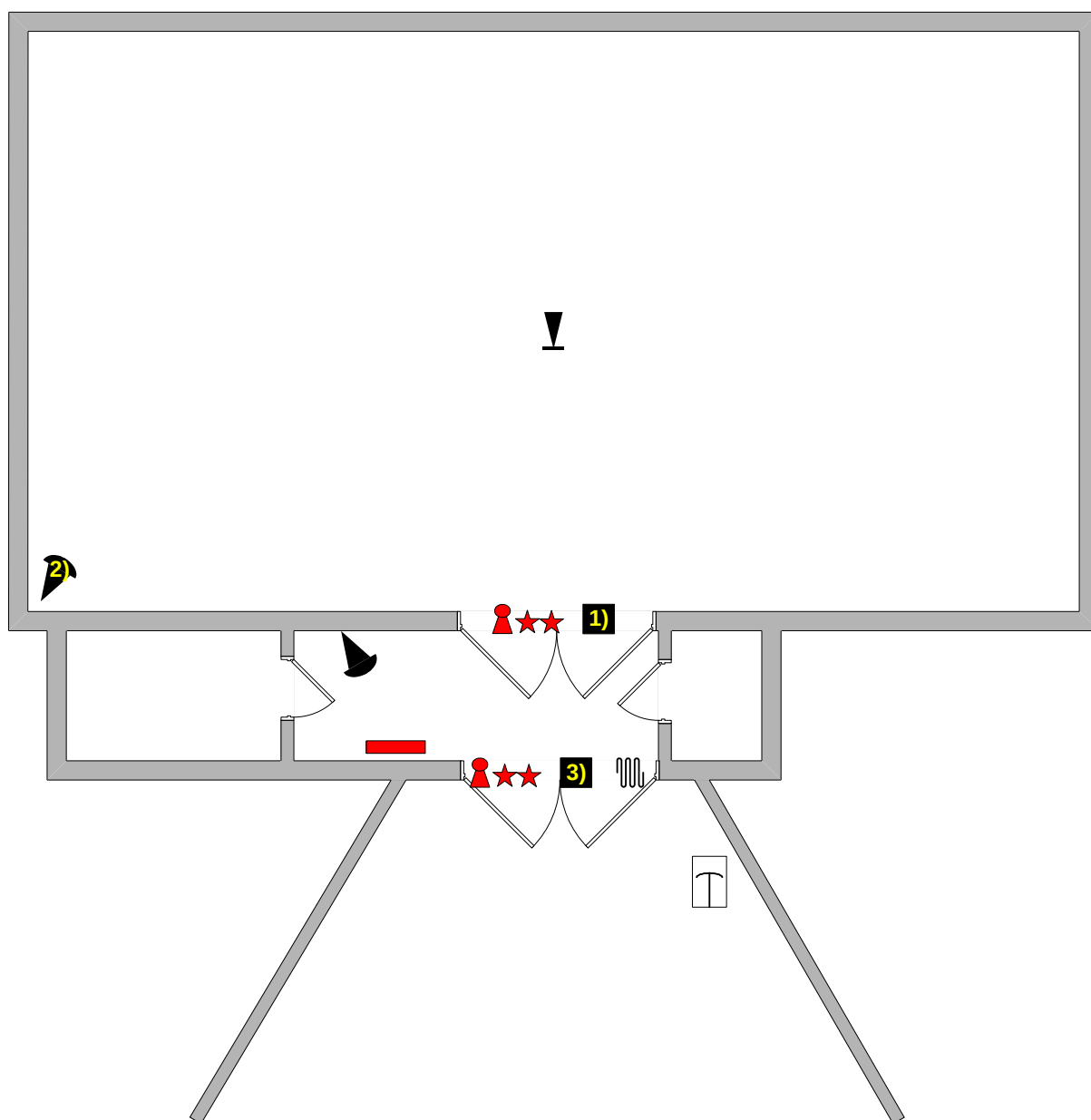
- 1) Kan undlades
- 2) Beror på en konkret vurdering, men bør normalt være tilstede.
- 3) Eventuelt på låseoverfald

3.3. Sikring af magasin type 3

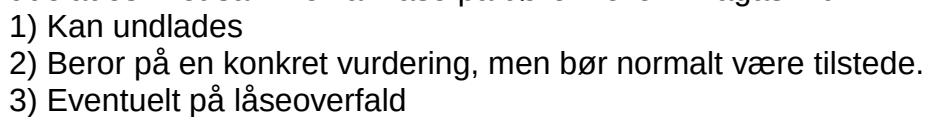


- 1) Kan undlades
- 2) Beror på en konkret vurdering, men bør normalt være tilstede.
- 3) Eventuelt på låseoverfald

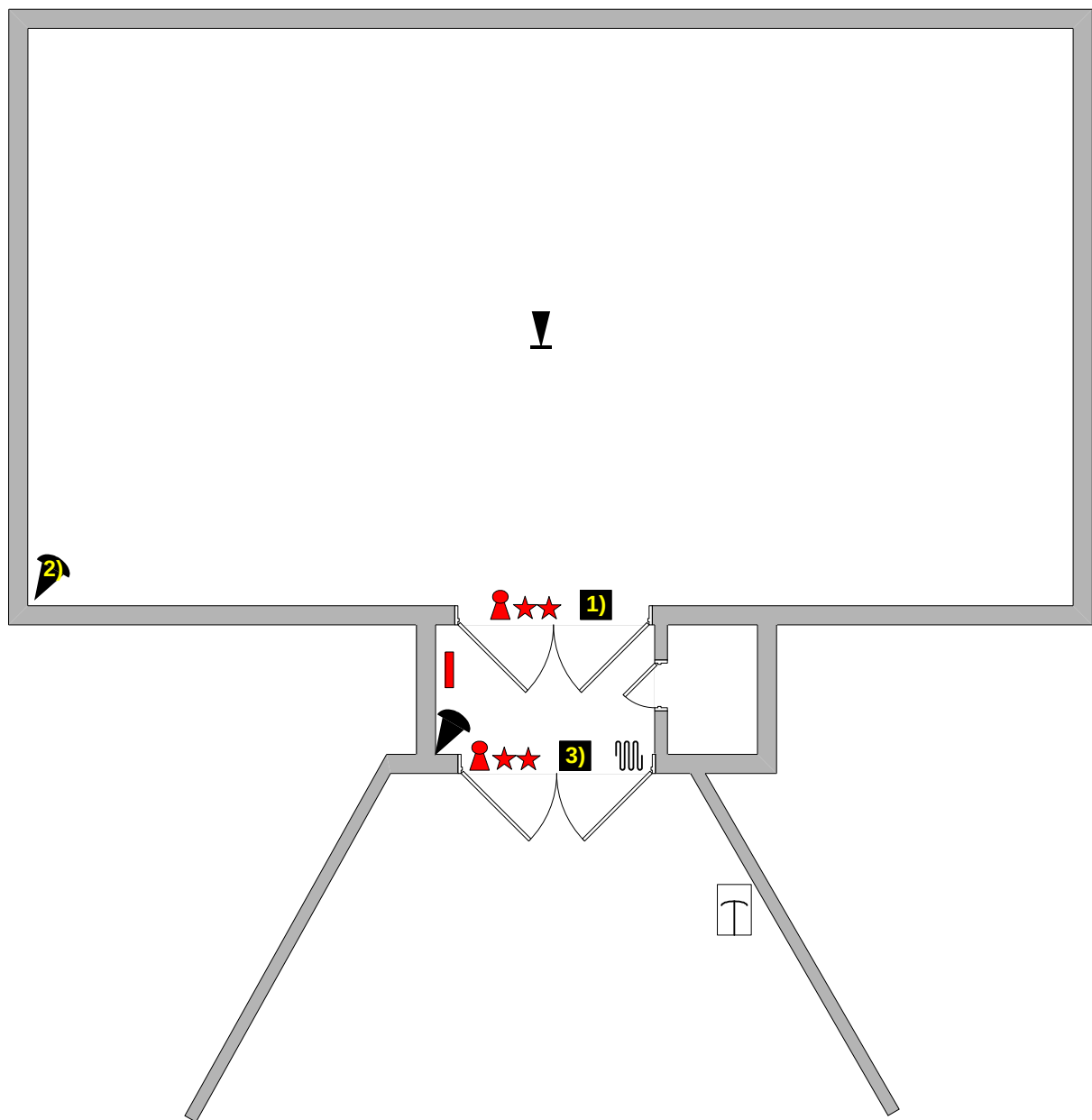
3.4. Sikring af magasin type: Magasin med patronkasserum



- 1) Kan undlades
- 2) Beror på en konkret vurdering, men bør normalt være tilstede.
- 3) Eventuelt på låseoverfald

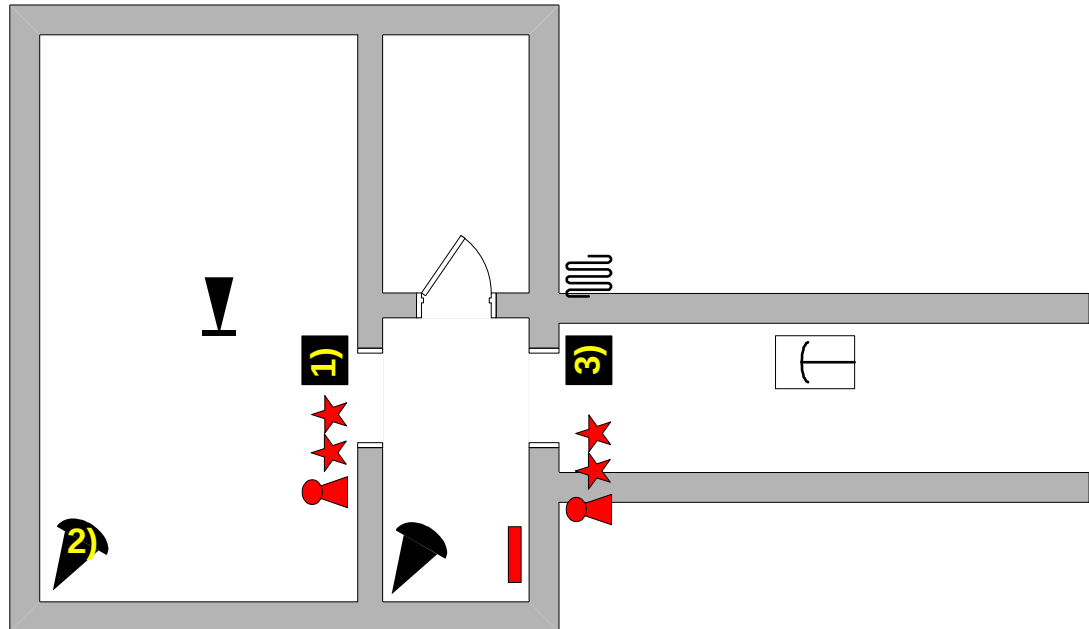


3.6. Sikring af magasin type: Magasin



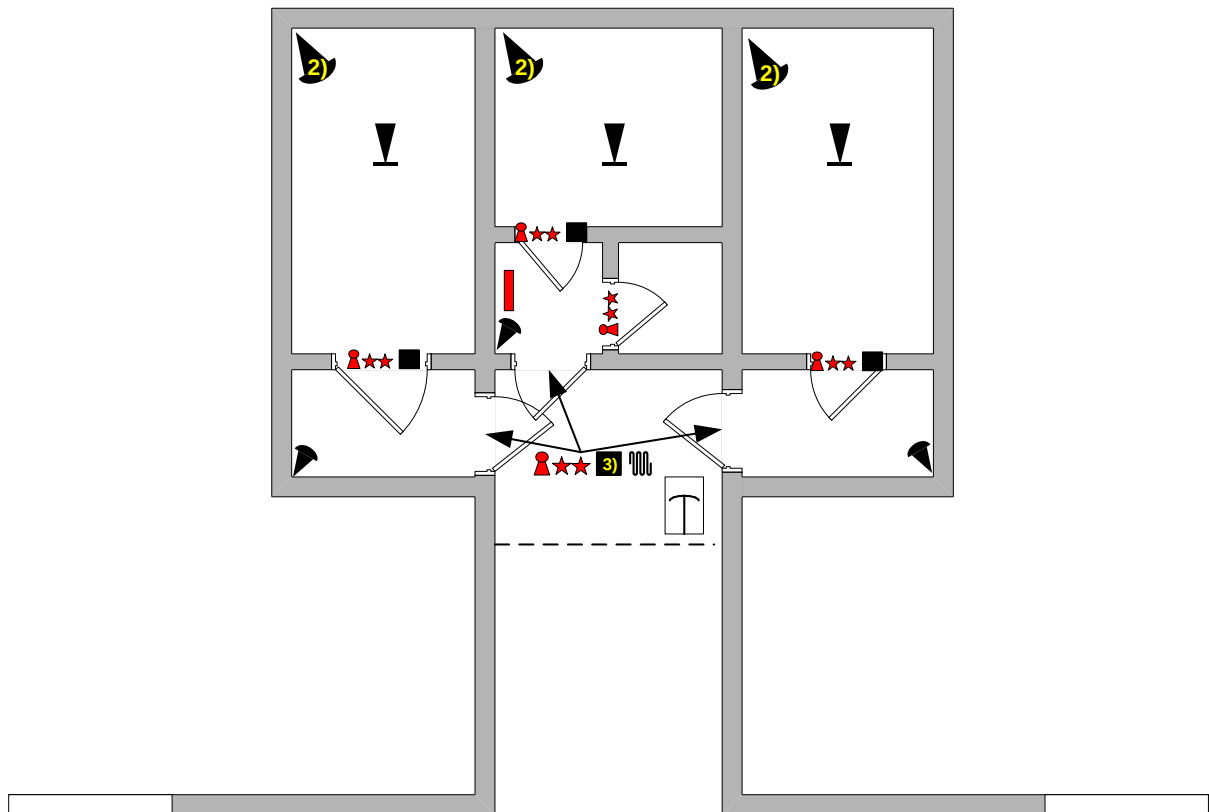
- 1) Kan undlades
- 2) Beror på en konkret vurdering, men bør normalt være tilstede.
- 3) Eventuelt på låseoverfald

3.7. Sikring af magasin type: Magasin

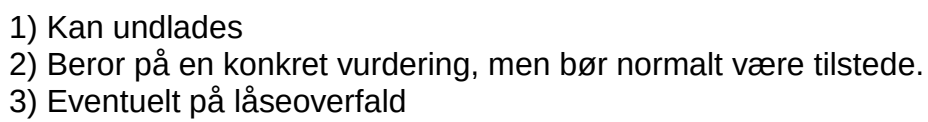


- 1) Kan undlades
- 2) Beror på en konkret vurdering, men bør normalt være tilstede.
- 3) Eventuelt på låseoverfald

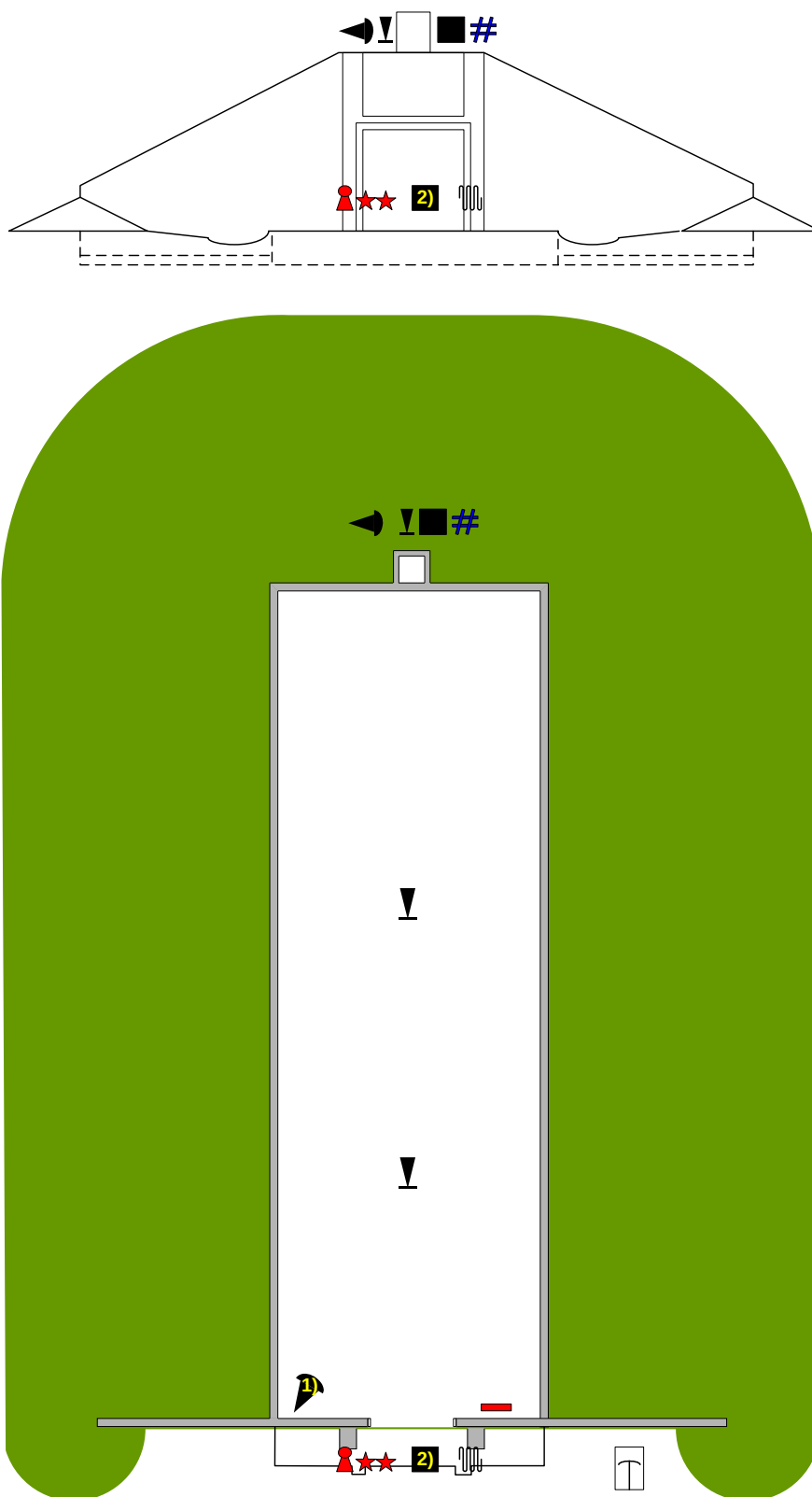
3.8. Sikring af magasin type: Krudtmagasin



- 1) Kan undlades
- 2) Beror på en konkret vurdering, men bør normalt være tilstede.
- 3) Eventuelt på låseoverfald

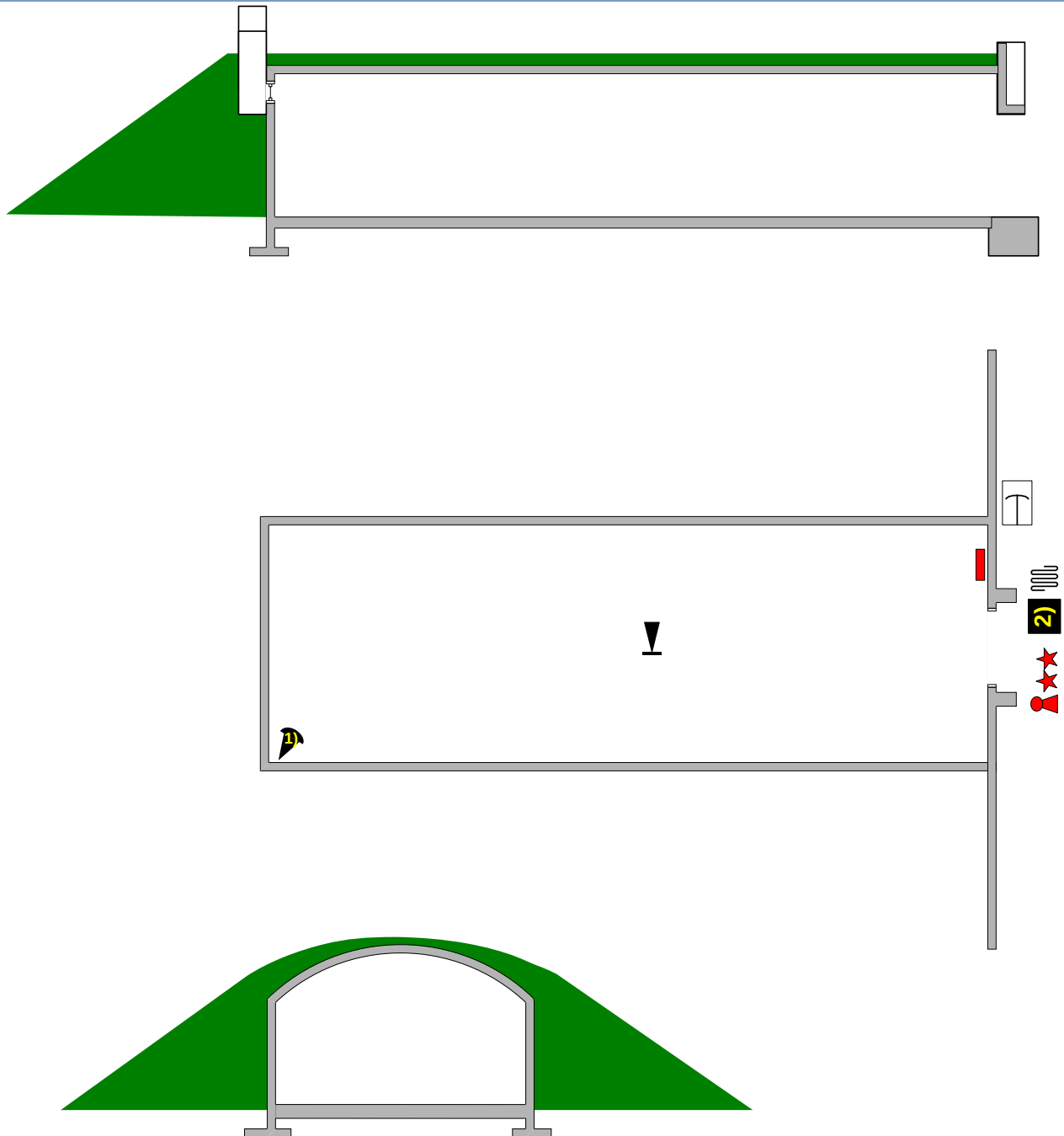


3.10. Sikring af magasin type: Iglo



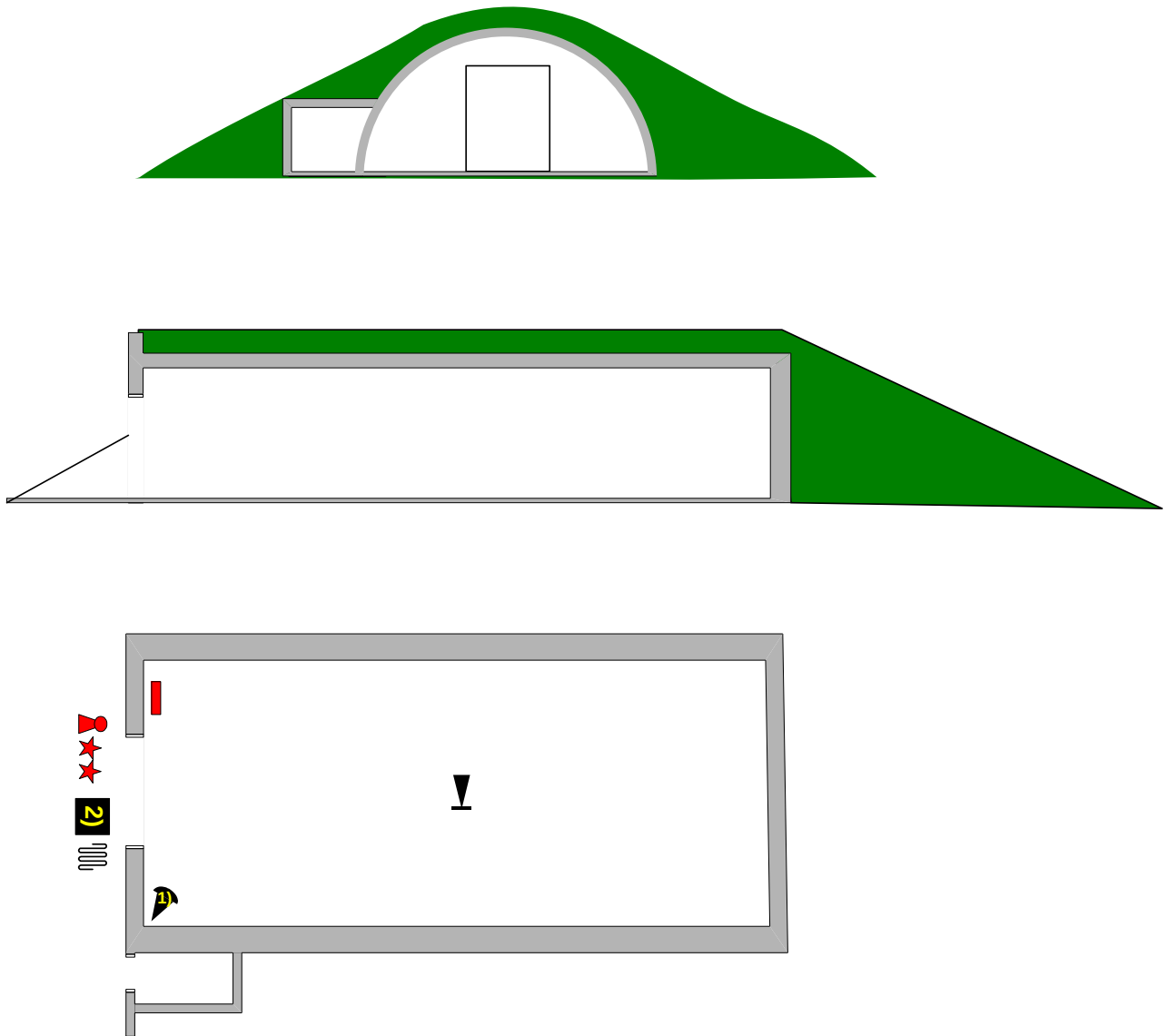
- 1) Beror på en konkret vurdering, men bør normalt være tilstede.
2) Eventuelt på låseoverfald

3.11. Sikring af magasin type: Iglo type 16



- 1) Beror på en konkret vurdering, men bør normalt være tilstede.
- 2) Eventuelt på låseoverfald

3.12. Sikring af magasin type 4



- 1) Beror på en konkret vurdering, men bør normalt være tilstede.
- 2) Eventuelt på låseoverfald

OVERSIGT OVER SIKRINGSMÆSSIGE TILTAG INDENFOR BEVOGTET ETABLISSE- MENTS PERIMETERHEGN

Områdeinddeling	Områdekategori	Reaktionstid, minutter	Sikringsniveau	Mekanisk sikring minimumskrav							Elektronisk overvågning - minimumskrav							
				Døre/ porte/ lemme		Vinduer	Krav til opbevaringsmiddel i forhold til opbevaret klassifikation Klasse / Grade				Elektronisk skalovervågning i grænsefladen						Rum/ objekt over- vågning	
				Låseenhed	Sikring mod gennembrydning		TTJ	FTR	HEM	YHM	Døre/porte/ lemme	Vinduer	Overvågning mod åbning	Overvågning mod gennembrydning	Overvågning mod åbning	Overvågning mod gennembrydning	Montering af rumovervågning	Overvågning på/af opbevaringsenhed
Kontrolleret	3		10-S				C ²⁾											
Sikret	2	15	20-O					A/1 ¹⁾									•	•
		15	30-S/C		EN 1627 RC3			A/1	A/1		•		•	•	•	•	•	•
		15	40-S/C		EN1627 RC4 eller EN 1143-1 GRADE 1	EN356 P6B		B/1	1/A		•	• ³⁾	•	•	•	•	•	•
	1	5	50-S/C		EN1627 RC5 eller EN1143-1 GRADE 1	EN356 P6B med gitter eller P7B		B/1	B/1		•	• ³⁾	•	•	•	•	•	•
		5	60-S/C		EN1627 RC6 eller EN1143-1 GRADE 2	EN356 P7B med gitter eller P8B		B/1	B/1		•	• ³⁾	•	•	•	•	•	•

S=	Skalsikring		1)	Bør overvejes til opbevaring af kontanter
C=	Cellesikring		2)	F.eks. skrivebordsskuffe i træmøbel
O=	Objektsikring		3)	Vægge, loft og gulv overvåges mod gennembrydning
				Låseenhed I
				Låseenhed IV med suppleringslås i sikringsniveau 40, 50 og 60. Der anvendes Låseenhed III i sikringsniveau 30

OVERSIGT OVER SIKRINGSMÆSSIGE TILTAG INDENFOR BEVOGTET ETABLISSE- MENTS PERIMETERHEGN

Militær område inddeling	Område kategori	Sikrings-niveau	Indhold
Klassificeret materiel	(Kategori X område)	F&P	
Kontrolleret	3	10	Kontorområder og øvrige områder når aflåst. Max klassifikation TTJ. MAT: AMM uden sprængladning til tunge våben (jf. kapitel 3)
Sikret	2	20	Mindre mængde FTR, HEM og kontanter under 40.000 kr. ¹⁾ i et klasse A opbevaringsmiddel.
		30	Kontorområder Max. klassifikation FTR & HEM, i klasse A/Grade 1 opbevaringsmiddel. Hvis der opbevares HEM, skal indsatsstyrken være fremme inden for 5 minutter. Våbenopbevaring: Mindre mængder våben uden vital våbendel i et klasse A/Grade 1 opbevaringsmiddel. Vital del i et andet klasse A/Grade 1 opbevaringsmiddel. Indsatsstyrken skal være fremme på 5 min.
		40	Kontorområder: max. Klassifikation HEM (FTR og HEM i klasse B/Grade 1 opbevaringsmiddel). Depoter, våbenkammer/rum: Våben: uden vital del, vital del i klasse A/Grade 1 opbevaringsmiddel. Pistoler kan opbevares samlet, såfremt pkt. 6.2.1 Våbenopbevaring i kapitel 3 overholdes. MAT: Max. FTR samt vitalt/sensitivt (jf. kapitel 3).
	1	50	Kontorområder: klassifikation HEM og højere (FTR og HEM i klasse B/Grade 1 opbevaringsmiddel). Depoter, våbenkammer/rum: Våben: uden vital del. (Mulighed for funktionsduelig efter godkendelse af FE. MAT: Max. HEM samt vitalt og/eller sensitivt (jf. kapitel 3).
		60	Kontorområder: klassifikation HEM eller højere. YHM i klasse A/Grade 1 opbevaringsmiddel. MAT/AMM: Særligt sikkerhedsbehov. FE/Den militære sikkerhedsafdeling skal inddrages.

¹⁾ Hvis beløbet overstiger 40.000 kr., skal risikoejeren godkende opbevaringen.

OVERSIGT OVER SIKRINGSMÆSSIGE TILTAG UDENFOR BEVOGTET ETABLISSE- MENTS PERIMETERHEGN

Områdeinddeling		Områdekategori		Mekanisk sikring minimumskrav								Elektronisk overvågning – minimumskrav																			
Overvåget				Sikringsniveau		Døre/porte/ lemme		Vin- duer		Krav til opbevaringsmiddel i for- hold til opbevaret klassifikation Krav til opbevaringsmiddel i forhold til opbevaret klassifikation Klasse / Grade				Elektronisk skalovervågning i græn- sefladen				Rum/ objekt overvåg- ning		Forbikobling af adgangsveje til betjeningspanel		Centraludstyr i overvåget område									
														Døre/porte/ lemme		Vinduer								Overvågning mod åbning		Overvågning mod gennembrydning		Overvågning mod åbning		Overvågning mod gennembrydning	
10-S		Låseenhed		Sikring mod gennembrydning		Sikring mod gennembrydning		Vitale våbende		TTJ		FTR		Øvrigt materiel		Overvågning mod åbning		Overvågning mod gennembrydning		Overvågning mod åbning		Overvågning mod gennembrydning		Montering af rumovervågning		Overvågning på/af opbevaringsenhed					
20-O		Låseenhed		Sikring mod gennembrydning		Sikring mod gennembrydning		Vitale våbende		TTJ		FTR		Øvrigt materiel		Overvågning mod åbning		Overvågning mod gennembrydning		Overvågning mod åbning		Overvågning mod gennembrydning		Montering af rumovervågning		Overvågning på/af opbevaringsenhed					
30-S/C		Låseenhed		Sikring mod gennembrydning		Sikring mod gennembrydning		Vitale våbende		TTJ		FTR		Øvrigt materiel		Overvågning mod åbning		Overvågning mod gennembrydning		Overvågning mod åbning		Overvågning mod gennembrydning		Montering af rumovervågning		Overvågning på/af opbevaringsenhed					
40-S/C		Låseenhed		Sikring mod gennembrydning		Sikring mod gennembrydning		Vitale våbende		TTJ		FTR		Øvrigt materiel		Overvågning mod åbning		Overvågning mod gennembrydning		Overvågning mod åbning		Overvågning mod gennembrydning		Montering af rumovervågning		Overvågning på/af opbevaringsenhed					

S=	Skalsikring			
C=	Cellesikring		1)	F.eks. skrivebordsskuffe i træmøbel
O=	Objektsikring		2)	I henhold til kapitel 3
			3)	Mindre mængde FORTROLIGE dokumenter og kontanter under 40.000 kr. 1).
			4)	Vægge, loft og gulv sikres mod gennembrydning
				Låseenhed I
				Låseenhed IV med suppleringslås i sikringsniveau 40, 50 og 60. Der anvendes låseenhed III i sikringsniveau 30

¹⁾ Hvis beløbet overstiger 40.000 kr., skal risikoejeren godkende opbevaringen.

**OVERSIGT OVER SIKRINGSMÆSSIGE TILTAG UDENFOR BEVOGTET ETABLISSE-
MENTS PERIMETERHEGN**

Militær område inddeling	Område kategori	Sikringsniveau	Indhold
Klassificeret materiel	(Kategori X område)	F&P	
Overvåget	4	10	Øvrigt materiel. MAT, der ikke betegnes som vitalt/sensitivt med krav om højere sikringsniveau.
		20-O	Mindre mængde FORTROLIGT (f.eks. dokumenter) og kontanter under 40.000. ¹⁾
		30-S/C	Øvrigt materielt samt vitalt sensitivt materiel når dette oplægges i godkendte opbevaringsmidler militær klasse A.
		40-S/C	Vitalt sensitivt materiel IKKE KLASSIFICERET. Opbevaring i godkendte opbevaringsmidler bør overvejes. Våben uden vital del. Våben og AMM i godkendte AMMMAG (type 2 og højere) med AIA.

¹⁾ Hvis beløbet overstiger 40.000 kr., skal risikoejeren godkende opbevaringen.

F&P FARVEKLASSIFICERING ¹

Farveklassificering af mekaniske sikringselementer, konstruktioner og enheder mv. sker efter F&P's målsætning enten ved prøvning eller ved en vurdering.

Farveklassificeringen er opdelt i fire grade/klasser: RØD, BLÅ, GRØN og GUL hvor RØD har det højeste niveau.

1. RØD – SIKKER:

Er en F&P-godkendt sikringsenhed, der udviser så stor modstand mod indbrudsforsøg, at den kan antages at være sikker ved gennembrydnings-/oplukningsforsøg.

2. BLÅ – STANDSENDE:

Er en F&P-godkendt sikringsenhed, der udviser så stor modstand mod indbrudsforsøg, at den kan antages at have en standsende effekt ved gennembrydnings-/oplukningsforsøg.

3. GRØN – HINDRENDE (anvendes ikke i forsvaret):

Er en F&P-godkendt sikringsenhed, der udviser så stor modstand mod indbrudsforsøg, at den kan antages at være hindrende ved gennembrydnings-/oplukningsforsøg.

4. GUL – HÆMMENDE:

Er en F&P-godkendt sikringsenhed, der udviser en vis modstand mod indbrudsforsøg, at den kan antages at have en hæmmende effekt ved gennembrydnings-/oplukningsforsøg.

Som supplement til den mekaniske sikring anvendes på sikringsniveauerne 20 – 60 elektronisk overvågning.

¹ Standarden er udgået, men bibeholdes indtil videre pga. sikringsprodukter i koncernen, der er godkendt efter standarden.

MEKANISK SIKRING

- Ref.: a. Brancheorganisationen Forsikring & pensions hjemmeside (Tyveri)
b. Brancheorganisationen Forsikring & pensions hjemmeside (Sikringsprodukter)

Underbilag:

1. F&P farveklassificering.
2. F&P Standardtyvmetoden. Vurdering af gennembrydnings- og/eller oplukningstid.
3. Perimetersikring og indhegning.
4. Præventiv belysning.
5. Opbevaringsmidler. Penge- og sikringsskabe.
6. Godkendte klassificerede låseenheder, F&P klassificering.
7. Låse, nøgler og koder.

1. MEKANISK SIKRING

Mekanisk sikring er en sikring af grænsefladen med låse, beslag, gitre og lignende, der gør oplukning og/eller gennembrydning besværlig. Endvidere omfatter mekanisk sikring etablering af perimetersikring, der kan suppleres med præventiv belysning med henblik på at forbedre de sikkerhedsmæssige foranstaltninger på etablissementet. Mekanisk sikring kan udføres som skalsikring, cellesikring og objektsikring.

2. F&P- REGELSÆTTETS ANVENDELSE I KONCERNEN

Generelt anvendes F&P-regelsættet jf. ref. i koncernen i forbindelse med projektering og udførelse af mekanisk sikring og elektronisk overvågning med følgende undtagelser:

- Der skal anvendes stabile bygningsdele i alle konstruktioner fra sikringsniveau 20 og højere.
- Døre i sikringsniveau 20 og højere samt opbevaringsmidler aflåses kun med Forsvarets sikkerhedsgodkendt lås.
- Alarmoverførsel fra lokal AIA- central til vagt/kontrolcentral skal udføres jf. minimumskravene, som er anført i Forsvarsministeriets Ejendomsstyrelses fagbeskrivelse "Sikkerhedsnettet".
- Der skal anvendes "skandinaviske nøglecylindre" (rund eller oval), og der må ikke anvendes DIN låsecylindre (ofte benævnt dråbelås), hvor der er beskyttelseskrævende aktiver bag grænsefladen uanset sikringsniveau.
Ved eftermontering af sikkerhedsgodkendt suppleringslås kan der ofte opnås en godkendt aflåsning. Allerede installerede dråbelåscylindre bør udskiftes, eller der skal indhentes FE godkendelse af løsningen.
- Koncernens krav til bygningsdele er skærpede i forhold til de af F&P anvendte krav.

3. GRÆNSEFLADEN

Grænsefladen til sikrede områder (områdekategori 1 og 2) skal være udført af stabile bygningsdele, som tilgodeser de respektive sikringsniveauer.

Svage bygningsdele i grænsefladen skal forstærkes med fx jern- og/eller finerplader mv. jf. ref. b.

F&P godkendte døre/porte og vinduer fremgår af ref. b.

Indgår der i grænsefladen åbninger der enten kan være en åbning på mere en 0,1 kvadratmeter uanset form, eller en åbning som er mere en 12 cm på hver side i et kvadrat uanset om det samlede areal er under 0,1 kvadratmeter skal åbningen sikres fx med gitter jf. ref. b.

4. GRÆNSEFLADER MINDST 4 METER OVER TERRÆN

Indgår der i den udvendige grænseflade lukker (vinduer, ventilationsriste mv.), som er placeret mindst 4 meter over terræn og udbygning, kan den mekaniske sikring af disse undlades, medmindre der på anden måde er indkrybningsmuligheder via balkon, murfremspring, nedløbsrør el. lign.

Den elektroniske overvågning skal bibeholdes i fuldt omfang jf. det krævede sikringsniveau uanset antallet af etager.

Reglen for grænseflader mindst 4 meter over terræn er ikke gældende for sikringsniveau 50 og 60. Ved sikringsniveau 50 og 60 skal der etableres mekaniske sikring ved lukker (vinduer, ventilationsriste mv.), uanset højde.

F&P STANDARDTYVMETODEN ¹**VURDERING AF GENNEMBRYDNINGSG- OG/ELLER OPLUKNINGSTID****1. STANDARDTYVMETODEN**

Standardtyvmetoden er en kriminalteknisk prøvningsmetode (human test) til bedømmelse af mekaniske sikringsforanstaltningers indbrudsmodstand.

Prøvningsmetodens hovedprincip er en anvendelse af de angrebsmetoder og værktøjssammensætninger, der efter en særlig prøvningsgruppes erfaringer er sammenlignelige med de angrebsmetoder og værktøjssammensætninger, som anses for sandsynlige ved en "standard tyvs" indbrudsangreb mod sikringsenheden.

Standardtyvmetoden vil normalt være egnet til test af alle typer af indbrudsforebyggende mekaniske sikringsforanstaltninger.

2. INDELING

Sikringsforanstaltningerne inddeles ved prøvning og klassificering i to hovedgrupper afhængig af deres anvendelsesform og benævnes sikringsenheder.

2.1. Hovedgruppe 1:

- beslag, speciallåse mm.
- bygningsdele
- døre, porte og lemme
- gitre - faste/rulle
- gitterskabe/pladeskabe
- glas og polycarbonat
- jern- og finérplader
- nøglebokse
- vinduer.

2.2. Hovedgruppe 2:

- sikringsskabe og sikringsdøre

3. SIKRINGSENHED

For, at en sikringsenhed skal leve op til betegnelsen skal modstandsevnen overfor indbrud - udført i en prøvesituation - under anvendelse af let håndværktøj minimum være som følger:

- Materiel i hovedgruppe 1, 3 min.
- Materiel i hovedgruppe 2, 12 min.

Sikringsenhedens modstandsevne anses for brudt såfremt oplukning eller frembringelse af en åbning, som overstiger 0,1 m², og hvor begge sider er længere end 120 mm.

¹ Standarden er udgået, men bibeholdes indtil videre pga. sikringsprodukter i koncernen, der er godkendt efter standarden.

4. KLASSIFICERING

Gennembrydnings- og/eller oplukningstid (anslået).

STANDARDTYVMETODEN

Klassificering	Bemærkninger	Hovedgruppe 1	Hovedgruppe 2
INGEN KLASSIFICERING	Ingen bemærkninger	< 3 min.	< 12 min.
GUL HÆMMENDE	Enheden udviser en vis modstand mod indbrudsforsøg, og kan derfor antages at have en hæmmende effekt ved gennembrydnings-/oplukningsforsøg.	3-5 min.	12-20 min.
GRØN HINDRENDE	Enheden udviser en så stor modstand mod indbrudsforsøg, at den kan antages at være hindrende ved gennembrydnings-/oplukningsforsøg.	5 min.	20-28 min.
BLÅ STANDSENDE	Enheden udviser så stor modstand mod indbrudsforsøg, at den kan antages at være standsende ved gennembrydnings-/oplukningsforsøg.	7-10 min	28-40 min.
RØD SIKKER	Enheden udviser så stor modstand mod indbrudsforsøg, at den må antages at være sikker ved gennembrydnings-/oplukningsforsøg.	> 10 min.	> 40 min.

5. VÆRKTØJSLISTE

Til brug for afprøvning af sikringsenhedens modstandsevne anvendes let håndværktøj jf. følgende liste. Der anvendes ikke elværktøj for ledningstilslutning (220 volt).

- Skruetrækker over 25 cm
- Skruetrækker under 25 cm
- Koben
- Brækjern
- Rørtang
- Smedehammer
- Hammer
- Klaphammer
- Dorne
- Stemmejern

- Knive
- Hobbykniv
- Nedstryger
- Lille nedstryger
- Brandøkse
- Stor nedstryger
- Stiksav
- Bor
- Gasblæselampe
- Boresving
- Ledningsfrit el-håndværktøj
- Økse
- Pladesaks
- Boltsaks
- Hulskærer
- Manipulationsudstyr
- Kiler
- Snittap
- Glasskærer
- Skiftenøgle
- Mejsel
- Knibtang
- Multigrebtang
- Bidetang
- Bidetang med udveksling
- Kørner.

6. MÆRKNING

Godkendte sikringsenheder må markedsføres som godkendt og klassificeret af F&P, såfremt de i monteret stand er forsynet med et synligt godkendelsesmærke. Godkendelsesmærket skal som minimum være forsynet med navnet Forsikring & Pension samt prøvningsnummer og farveklassifikation - fx. BLÅ. (Sikringsenhederne må ikke markedsføres som godkendt af politiet eller forsikringsselskaberne.)

PERIMETERSIKRING OG INDHEGNING

Ref.: [Brancheorganisationen Forsikring & pensions hjemmeside \(Tyveri\)](#)

1. INDLEDNING

Perimetersikring betegner en barriere, der etableres i omkredsen af udendørsarealer med det formål at markere en juridisk afgrænsning, som - i forbindelse med en vis hindreværdi - kan udgøre en væsentlig støtte ved udførelse af bevogtning eller overvågning.

Indhegning kan have mere eller mindre præventiv karakter, men er kun effektiv, såfremt adgang og passage foretages gennem en kontrolleret adgangsvej. Den kontrollerede adgang kan enten foretages manuelt eller via et adgangskontrolsystem (ADK) med anvendelse af medie og personlig kode.

Hegnsbeplantning kan have hindrende værdi, når der anvendes stikkende eller tornede vækster. Medens beplantning er under opvækst, vil særlige foranstaltninger midlertidigt være påkrævet fx etablering af flethegn.

Hegnsbeplantning kan anvendes som supplement til anden indhegning, specielt gitter og palisadehegn.

Øvrig vegetation i tilknytning til perimeterhegn skal være af en sådan beskaffenhed, at der ikke via denne kan skaffes adgang over hegn til etablisementsområdet.

Beskrivelsen af sikringskravene basis, middel og høj sikkerhed vedrørende perimeterhegn er vejledende sikringskrav. Etablering bør vurderes i relation til den aktuelle risikovurdering. Som en del af risikovurderingen skal der tages stilling til behovet for en køretøjssluse. Det vil være normalt ved valg af perimeterhegn med høj sikkerhed.

2. SIKRINGSKRAV

2.1. Basissikkerhed.

Dersom kravet til sikkerhed er relativt beskedent, dvs., hvis man kun skal beskytte mindre attraktive materielkategorier, eller hvis man af den ene eller anden grund bedømmer risikoen for indbrud som værende af minimal karakter, er det ofte tilstrækkeligt med en basisbeskyttelse. Områder med basissikkerhed kan tillade åbne porte i perimeteren indenfor almindelig arbejdstid, men skal være lukkede ved arbejdstids ophør og på søn- og helligdage efter den lokale chefs bestemmelse. Af hensyn til at kunne iværksætte øget bevogtning ved beredskabsforøgelse, bør der alle steder være etableret de mekaniske arbejder (f.eks. porte), der er en forudsætning for at kunne lukke perimeteren.

Som basisbeskyttelse bør opføres et hegn, der bør være mindst 2 meter højt og være forsynet med tre rækker vandret pigtråd.

Basisbeskyttelse skal være så vedligeholdelsesfri som overhovedet muligt. Ved hjælp af områdeafmærkning markeres grænsen til et område, og samtidig får man en vis støtte til at hindre uvedkommendes indtrængen.

Der er en del af koncernens sikrede områder, der er placeret i tæt bymæssig bebyggelse. Her er det normalt ikke muligt at skabe en egentlig perimetersikring. Her er skallen af bygningen normalt perimeteren. I de tilfælde bør der etableres en basis sikkerhed på sikringsniveau 40 i som minimum underetagen – for at skabe tid til at en indsatsstyrke kan være rettidigt fremme ved indbrud, sabotage og terrorhandlinger.

2.1.1. Hegn.

Hegn findes i forskellige kvaliteter og konstruktioner spændende fra enkelt tråd over flettet hegn til svejst hegn og fx palisadehegn.

Valg af hegn afhænger bl.a. af:

- Lovmæssige krav for lokalområdet
- Det indhegnedes tyvetækkelighed
- Hærværksrisiko.
- De aktiver der skal passes på.

2.1.2. Porte.

Porte fremstilles som manuelt betjente og elektrisk betjente porte i meget varierende kvalitet og styrke. Ved valg af port og andre adgangslukker er det vigtigt, at den mekaniske styrke svarer til styrken i det øvrige hegn.

Låger og portes hængsler skal som minimum sikres således, at de ikke kan afløftes.

Af hensyn til en smidig ind- og udpassage bør porte normalt kombineres med vippebomme, der kan have samme sikringsmæssig værdi som bevægelige skydeporte, men er langt hurtigere i sin bevægelse.

2.1.3. Pigtråd.

For at forøge sikkerheden kan pigtråd anvendes ved at forlænge toppen af hegnspælene og montere pigtråd på forlængelsen.

Forlængelsen bør normalt laves i en vinkel på 45°. Underkanten af flethegn kan også forsynes med pigtråd. Flethegn kan suppleres med pigtrådsspiralhegn.

2.2. Middel sikkerhed.

Såfremt der er behov for en sikker ind- og udpassage kombineret med en tidlig indikation af, at uvedkommende forsøger at trænge ind på området, skal et beskyttelsessystem af middel sikkerhed etableres.

Ved middel sikkerhed bør hegnet være mindst 2 meter højt med tre rækker pigtråd evt. skråtstillet. Maskestørrelse på hegnet bør højst være 80 mm x 30 mm.

En elektronisk overvågning (eks. på hegn, i jord, aktive skud mv.) i forbindelse med hegn øger sikringsværdien.

Det vil også være muligt at etablere perimetersikring i form af f.eks. jordarbejder, beton plantekasser, betonmure, niveauforskelle i veje og stier samt anvendelse af vand og vådområder m.m. Den type løsninger beskrives ofte som urban engineering. Det er kendetegnet for denne type løsning, at den ikke hindrer personadgang i særlig høj grad, men forhindrer indkørsel af motorkøretøjer.

Hvis urban engineering vælges, skal FE inddrages - og det vil oftest medføre et krav om, at perimeteren elektronisk overvåges med detektorer, TV- og videoovervågning og lignende.

Kørende trafik kan kontrolleres på en sikker måde, ved hjælp af adgangskontrol (ADK) som automatisk aktiverer porte og bomme for adgang evt. suppleret med trafiklys.

2.2.1. Rotationsporte.

For at registrere alle personer ved ind og ud passage kan fodgængere eksempelvis passere gennem en rotationsport, med adgangskontrol (ADK), der giver en sikker passage både indendørs og udendørs.

Rotationsporte kan være forsynet med anti pass back for entydig registrering af personer, som færdes i området.

Porten skal sædvanligvis give mulighed for at medtage cykler, men ikke ladcykler.

2.2.2. Portautomatik.

Porte kan leveres med forskellige funktionsmuligheder, betjent af vagt eller ved hjælp af nøgle, kodelås, ADK, induktive følere i jord, transportable sendere mv. Med hensyn til evt.

remote styring fra kontrolcentral/vagtcentral skal Forsvarsministeriets Ejendomsstyrelses fagbeskrivelse følges.

2.2.3. Bomme.

Bomme findes i stort udvalg - manuelle eller automatiske. Bomme er hensigtsmæssige ved afvikling af meget trafik samtidig med en kontrol af bilpassage.

2.2.4. Trafiklys.

Trafiklys i kombination med porte og bomme medvirker til at trafikken afvikles på en kontrolleret og hensigtsmæssig måde.

2.2.5. Alarm.

Elektronisk hegnsalarm overvåger hegnet sektionsvis via en centralenhed, som tilsluttes den lokale AIA central. Anvendelsen af elektronisk hegnsalarm kan potentielt medføre et stort antal u hensigtsmæssige alarmer. Anvendelse af elektronisk hegnsalarm skal altid godkendes af FE, da elektronisk hegnsalarm ikke er godkendt som en sikringskomponent og dermed ikke har en udstyrsklasse.

2.3. Høj sikkerhed.

Hvis kravet til sikkerhed er meget stort, kræver dette en områdebeskyttelse med et højt sikringsniveau. Skal løsningen være både effektiv og troværdig skal det være tidskrævende og vanskeligt for uvedkommende at trænge ind uden at blive opdaget. FE rådgivning skal indhentes.

En kombination af eks. urban engineering, hegn, porte, bomme, sluser, rotationsporte skal sikre en høj sikkerhed og være udformet på en sådan måde, at det dels giver en tilstrækkelig beskyttelse mod indtrængen, dels garanterer en sikker passagekontrol.

Beskyttelsen bør bestå af to fysiske hindringer. Mellem disse hindringer etableres en overvågningsalarm. Den yderste beskyttelse kan bestå af et min. 2 meter højt hegn med pigtråd samt elektronisk overvågning (eks. på hegn, i jord, aktive skud mv.). Den inderste beskyttelse kan bestå af et 3 meter højt hegn med pigtråd. Dette hegn skal forsinke den indtrængende så meget, at der bliver tid til at foretage effektive modforholdsregler. Beskyttelsen kan eventuelt suppleres med TV- og videoovervågningsanlæg og gennemkørselsbeskyttelse (pullerter, road blockers mv.).

2.3.1. Svejste hegn eller palisader.

Af sikkerhedsmæssige grunde skal svejste hegn eller palisader anvendes. De vanskeliggør klipning og klatring. Svejste hegn og palisader fremstilles i forskellige udførelser.

2.3.2. Vejspærring.

Til effektiv beskyttelse af indfartsveje anvendes forskellige typer vejspærringer. De kan tilpasses de foreliggende sikringskrav.

2.3.3. Adgangskontrolsystem.

Der findes flere forskellige adgangskontrol (ADK) fabrikater, som alle skal kunne læse og anvende de i koncernen anvendte adgangskort til kontrol af ind- og udpassage i koncernen.

2.3.4. TV- og videoovervågningsanlæg.

Portenheder og låger, som kan fjernbetjenes, skal overvåges af TV- og videoovervågningsanlæg (TVO).

Ved høj sikkerhed skal der anvendes termiske kameraer for en 24/7 overvågning.

Områder med elektronisk overvågning kan suppleres med TVO for verifikation.
Adgangsveje kan suppleres med TVO for identifikation.

3. MATERIALER

3.1. Hegnstyper.

Af hegstyper kan nævnes

- enkeltrådshegn
- flethegn,
- pressegitterhegn,
- svejste hegn,
- palisadehegn,
- flytbare hegn,
- punktsikring,
- pigtrådshegn, samt
- murer og plankeværk.

De i koncernen primært anvendte hegn beskrives kortfattet nedenfor.

3.1.1. Svejste hegn.

Svejste hegn udgør en væsentlig sikring mod gennemtrængning, hvorfor det er meget anvendeligt som ekstern perimetersikring. Hegnet monteres på specialstolper og på forlængelsen monteres pigtråd "lige op" eller "skråtstillet".

Hegnet kan udbygges fra lav over middel til høj sikkerhed.

Hegnet er velegnet for montering af elektronisk hegnsalarm.

3.1.2. Flethegn.

Flethegn har kun begrænset værdi som barriere, med mindre der udføres særlige foranstaltninger i tilslutning til hegnet. Det er derfor primært anvendeligt som intern perimetersikring. Toppen af hegnspælene kan forlænges, og på forlængelsen kan monteres pigtråd.

Forlængelsen bør normalt vende udefter i en vinkel på 45°, dog indefter, hvis hegnet støder op til offentlig vej. Også underkanten af flethegn kan forsynes med pigtråd. Flethegn kan suppleres med pigtrådsspiralhegn.

3.1.3. Pigtrådshegn.

Pigtrådshegn er særligt egnet som hindring om eller ved interne objekter på militært område, hvortil uvedkommende ikke har adgang. Pigtrådshegn kan evt. suppleres med visse typer af elektroniske overvågningsanlæg. Pigtrådsspiralhegn kan anvendes som supplement til flethegn.

3.1.4. Mure og plankeværk.

Anvendes for at vanskeliggøre uvedkommendes indsigth i et område. Højden bør være mindst 2 meter, og hindringen bør være vanskelig at gennembryde eller undergrave. For at vanskeliggøre overklatring kan der på toppen af hindringen fastgøres pigtråd eller opadrettede jernpigge. Ved ældre etableringer er undertiden anvendt gitterkonstruktioner (palisadegitter). Visse typer elektronisk overvågning kan anvendes i forbindelse med mure eller plankeværk.

4. ETABLERING AF INDHEGNING

4.1. Perimeterhegn.

Valg af indhegning bør tilpasses områdets art, karakter, beliggenhed, omgivelser, øvrige sikringsforanstaltninger mv. Det bør tilstræbes, at der ved kategori 1 område og om muligt også ved kategori 2 område etableres en ydre perimeter, i form af indhegning, af hindrende værdi.

Af hensyn til bevogtning og evt. etablering af elektronisk overvågning bør det tilstræbes, at hegnsføringen består af rette linier med færrest mulige knæk.

Indhegning som ydre perimeter bør ikke ligge for tæt på "de sikrede objekter". Det betyder normalt 5 m på hver side af hegnet.

Ved vandarealer samt ved bygninger, der ligger op til eller udgør en forlængelse af en indhegning, må der træffes særlige foranstaltninger for at hindre uønsket passage. Træer, opstabilede materialer og andre objekter, der kan udnyttes til at lette uønsket forcering af indhegningen, bør fjernes eller ryddes.

4.2. Porte, døre og låse.

Hegnsporte og -døre bør konstrueres og monteres således, at de repræsenterer en hindring af mindst samme værdi som den etablerede indhegning. Konstruktion og montering må ikke give mulighed for uhindret passage og bør være vanskelig at angribe, fx med brækjern o.l.

Portstolper bør være solidt forankret evt. ved forstærkning med skråstivere for at opnå tilstrækkelig stabilitet. Tilsvarende bør porte være stabile, idet portrammen evt. forstærkes med diagonaljern. Porte bør sikres mod "undergravning", fx. ved en støbt betonsokkel. Overklatering af porte kan vanskeliggøres ved montering af jernpigge eller pigtråd for oven. Porte må ikke kunne løftes af hængsler eller gangjern.

Af hensyn til en smidig ind- og udpassage bør porte normalt kombineres med vippebomme, der kan have samme sikringsmæssig værdi som bevægelige skydeporte, men er langt hurtigere i sin bevægelse.

Hegnsporte og -døre kan aflåses med fastmonterede låse eller hængelåse. Ved fastmonteret lås må det kontrolleres, at riglen har tilstrækkelig indgreb i slutblik, og at låsen ikke kan demonteres fra ydersiden. Ved brug af hængelås bør beslaget være påsvejet ramme/stolpe. Brug af kæder frarådes.

5. VEDLIGEHOLDELSE OG EFTERSYN

Værdien af et hegn er afhængig af, at det til enhver tid holdes i god stand. Enhver beskadigelse skal hurtigst muligt udbedres, og der bør inden for hegnet være oplagt materialer til udbedring af mindre skader. Alle dele af hegnet skal til alle tider kunne inspiceres visuelt for brud på bundtråd, huller og andre skader. Hegnet må således ikke være delvist skjult af bevoksning, materielgenstande eller andre dækkende emner.

Ethvert hegn bør jævnligt inspiceres i hele sin udstrækning som en del af de pligter, der påhviler vagter og/eller tilsynsførende. Sådanne eftersyn bør omfatte såvel hegnets tilstand som bevoksning, materiel og materialer, der kan udnyttes ved uvedkommendes forcering af hegnet.

PRÆVENTIV BELYSNING

1. INDLEDNING

Belysning af adgangsveje, perimetre samt vitale områder er en del af de fysiske sikringsforanstaltninger, der kan træffes for at beskytte Forsvarets etableringer.

Belysning kan være permanent eller tændes ved detektering. I tilslutning til overvågningsanlæg kan belysning have en umiddelbar præventiv virkning, der mindsker forsøg på uretmæssig adgang. Belysning gør det muligt for bevogtnings/kontrolcentralspersonel, at opdage indtrængende personer før de når frem til deres mål.

Belysning kan såfremt den ikke vælges og anvendes rigtigt, være til større hjælp for indtrængerne end for vagtpersonellet. Belysning må således ikke kunne afsløre vagtposters opholdssted eller bevægelser, hvorfor det er af stor betydning, at belysning koordineres med øvrige sikringstiltag.

1.1. Permanent belysning af områdets grænser, adgangsveje og vitale områder kan monteres på forskellige måder, fx ved lysarmaturer anbragt på master, husmure eller hegn. En god permanent belysning kan betyde, at der kan etableres nummerpladegenkendelse samt anvendelse af farvekameraer 24/7 for identifikation af personer, uden brug af yderligere hvidt suppleringslys og i højere grad kan der gennemføres TVO.

1.2. Detektoraktiveret belysning kan etableres som belysning af områdets grænser, adgangsveje og vitale områder iværksat ved påvirkning af sensorer, detektorer o.l.

For begge typer belysning gælder, at de ved anvendelse som perimeterbelysning bør ligge på en højere lysstyrke end omgivelserne og ikke være placeret på en sådan måde, at de er til gene for patruljerende bevogtningspersonel.

OPBEVARINGSMIDLER

PENGE- OG SIKRINGSSKABE

Ref.: [Brancheorganisationen Forsikring & pensions hjemmeside](#)

1. INDLEDNING

Denne bestemmelse er udarbejdet for at sikre, at man inden for koncernens område anvender ensartede principper for opbevaring af klassificeret materiale og vitalt sensitivt materiel, samt værdigenstande og penge mv.

Bestemmelsen skal give sikkerhedsofficeren et indblik i de forskellige typer af pengeskabe mv., såvel de gamle som findes ved tjenestestederne, som de ny der markedsføres af leverandørerne.

For at begrænse mulighederne for tyveri af rede penge og pengerepræsentativer skal disse opbevares i værdiopbevaringsenheder, suppleret med elektronisk overvågning.

Opbevaringsmidler med vægt under 1.000 kg, der indeholder materiale klassificeret FORTROLIGT eller højere, skal fastboltes til stabil bygningsdel med min. 4 Ø 10 mm bolte eller franske skruer. Fastbolting af opbevaringsmidler placeret i kategori 1 og 2 område kan undlades, når der er bevæbnet reaktionsstyrke til rådighed inden for 5 min. reaktionstid. Opbevaringsmidler, som indeholder våben og/eller vitale våbendele, og som er placeret i områdekategori 2 og 4, skal uanset vægt altid fastboltes.

Våbenskabe skal altid fastboltres.

Beskrivelse af værdiopbevaringsenheder og standarder for prøvning fremgår af ref.

2. MILITÆR KATEGORISERING

2.1. Opbevaring af klassificeret materiale.

Klassificeret materiale skal, når det ikke er under konstant opsyn/kontrol, sikres i opbevaringsmidler, der omfatter:

- boksrums og arkivrum, klasse A
- pengeskabe, klasse A og B
- stålskabe, klasse A og B
- sikringsskabe, klasse A og B
- andre opbevaringsmidler, klasse A, B og C.

3. BOKSRUM OG ARKIVRUM, KLASSE A OG B

Et boksrums er et opbevaringsmiddel, hvori klassificeret materiale af alle klassifikationsgrader kan placeres fx på åbne hylder.

3.1. Boksrums opført af beton.

Følgende minimumskrav skal være opfyldt:

- Vægge, gulv og loft udføres af 15,5 cm beton armeret med to net 20/20, Ø 5 mm eller andet materiale med tilsvarende indbrudsmodstand

- Indgår der i grænsefladen åbninger der enten kan være en åbning på mere en 0,1 kvadratmeter uanset form, eller en åbning som er mere en 12 cm på hver side i et kvadrat uanset om det samlede areal er under 0,1 kvadratmeter skal åbningen sikres fx med gitter jf. ref. b.
- Kun én adgangsvej, der skal lukkes af en ståldør i stålkarm (boksdør), som fastgøres solidt med murankre e.l., om muligt faststøbes i 200 mm fiberbeton
- Døren skal bestå af en 8 mm stålplade, og døren skal være forsynet med rigleværk for lodrette og vandrette rigler, faste bagkantsrigler samt sprængsikring. Mellem dørens inderside (bagplade) og lås bør være påsvejet en boresikker 6 mm stålplade
- Døren skal forsynes med en sikkerhedsgodkendt 3-tals eller 4-tals kodelås og kan yderligere være forsynet med en sikkerhedsgodkendt nøglelås (pengeskabslås).

3.2. Boksrums opført af stålmoduler.

Som alternativ til boksrums opført af beton kan anvendes stålmoduler (densitbeton). Modulerne sammenboltes til den ønskede størrelse inkl. top og bund. Der anvendes boksdør som anført under pkt. 3.1.

Et boksrums opført af stålmoduler kan adskilles, nedtages og opføres andet steds, og det kan reduceres eller tilbygges efter behov.

Standardmål på stålmoduler er følgende:

Højde x Bredde x Tykkelse
2000 x 625 x 100 mm

3.3. Arkivrum.

Rum, som har karakter af boksrums, fx beskyttelsesrum, men som ikke på alle måder opfylder de anførte minimumskrav, kan ikke betegnes som boksrums. Disse rum kan betegnes som arkivrum klasse B, hvori materiale klassificeret inkl. HEM kan opbevares på åbne hylde, når følgende betingelser er opfyldt:

- Arkivrummet skal som minimum etableres i et sikret område, kategori 1, sikringsniveau 50 IV
- Kravet om en reaktionstid på max. 5 min. skal kunne overholdes under alle forhold
- Vægge, gulv og loft udføres som stabile ydervægge jf. ref. fane 20, fx enten minimum 20 cm beton, 24 cm mursten eller 30 cm letbetonblokke
- Indgår der i grænsefladen åbninger der enten kan være en åbning på mere en 0,1 kvadratmeter uanset form, eller en åbning som er mere en 12 cm på hver side i et kvadrat uanset om det samlede areal er under 0,1 kvadratmeter skal åbningen sikres fx med gitter jf. ref. b.
- Der må kun være én adgangsvej, der skal lukkes af en ståldør, der minimum opfylder kravene til en arkiv dør jf. EN 1143-1 Grade1 eller EN 1627 – 1630 RC 5 (F&P RØD klasse, hovedgruppe 2). Dørkarmen skal fastgøres solidt med murankre eller lignende og om muligt faststøbes i minimum 200 mm fiberbeton
- Døren skal aflåses med enten en sikkerhedsgodkendt 3-tals eller 4-tals mekanisk kombinationslås eventuelt suppleret med nøglelås eller en elektronisk kombinationslås, der modsvarer sikringsniveau 50.

4. PENGESKABE, KLASSE A OG B

Pengeskabe, klasse A, jf. EN 1143-1 Grade 1 eller EN1627-30 RC5 er opbevaringsmidler, som yder betydelig sikkerhed ved opbrydning med boreværktøj, skærebrænder og sprængstof samt ved borttransport (tyveri) og oplukning ved nedstyrtning.

Pengeskabe, klasse A, skal opfylde følgende minimumskrav:

- Yderskabet er fremstillet af 2 mm stålplade (helsvejset) og inderskabet er af stålplade. Hulrummet mellem yder- og inderskab - 100 mm - er opfyldt med beton eller andet brandsikkert materiale. Skab og dør er forsynet med brandfals
- Døren er af 6 mm stålplade. Mellem dørens inderside (bagplade) og lås kan være påsvejset en 6 mm boresikker stålplade. Døren er forsynet med rigleværk for vandrette og eventuelt lodrette rigler, faste bagkantsrigler, samt sprængsikring
- Døren er forsynet med sikkerhedsgodkendt 3-tals eller 4-tals kodelås og/eller sikkerhedsgodkendt nøgkelås (pengeskabslås) eller elektronisk kombinationslås
- Skabet skal veje mindst 250 kg. Skabe under 1000 kg. skal fastgøres.

Pengeskabe, som ikke på alle områder opfylder de anførte minimumskrav, betegnes som pengeskabe, klasse B.

5. STÅLSKABE, KLASSE A

Stålskabe, klasse A, er opbevaringsmidler, som yder nogen sikkerhed mod opbrydning, men betydelig sikkerhed mod opdirkning mv. Skabene består yderst af mindst 2 mm helsvejset stålplade og har – med enkelte undtagelser – inderbeklædning af tyndere stålplade. Skabene er forsynet med rigleværk samt sikkerhedsgodkendt kodelås og/eller nøgkelås (pengeskabslås).

6. STÅLSKABE, KLASSE B

Stålskabe, klasse B, er opbevaringsmidler, som yder begrænset sikkerhed mod opbrydning, men nogen sikkerhed mod opdirkning mv. Det er ved konstruktionen tilstræbt, at angreb let kan konstateres. Skabene har intet eller kun et spinkelt rigleværk. Den primære aflåsning er normalt en sikkerhedsgodkendt hængelås.

7. SIKRINGSSKABE, KLASSE A OG B

Sikringsskabe indbrudsprøvet efter F&P Standardtyvmetoden, hovedgruppe 2, og klassificeret efter denne prøvningsmetode er beskrevet i ref. og afmærket med følgende informationer:

F&P sikringsskab, typenummer og standardtyv prøvningsnummer samt en af klassificeringsfarverne GUL, BLÅ eller RØD.

Ved indbrudsprøvningen er udelukkende anvendt let håndværktøj.

Sikringsskabe klassificeret efter denne prøvningsmetode - minimum farven BLÅ - er egnet til at beskytte vitalt/sensitivt materiel, herunder våben.

Standardtyvmetoden (STM) er udgået, men teksten bibeholdes i bestemmelsen indtil videre

8. SIKRINGSSKAB, KLASSE A

Der skal anvendes skabe godkendt i henhold til standarden EN 1143-1 grade 0 eller højere f. eks. grade 1. Fremadrettet (fra juni 2018) vil der blive stillet krav om en grade 1 jf. EN 1143-1. De nuværende indkøbte skabe kan fortsat anvendes. Andre skabe kan godkendes med FE og Forsvarsministeriets Materiel- og Indkøbsstyrelses

medvirken i fysisk test af produktet. Ældre skabe, der overholder kravene jf. Standard-Tyv-Metoden, BLÅ klasse hovedgruppe 2 eller RØD klasse hovedgruppe 2, kan fortsat anvendes som et klasse A skab.

Ovenstående regler er gældende for allerede indkøbt sikringsskabe dvs. indkøbt før 31. december 2020.

Fra 1. januar 2021 vil der blive stillet krav om grad 1 eller højere jf. EN 1143-1.

9. SIKRINGSSKAB, KLASSE B

Et sikringsskab klasse B skal fremover minimum overholde standarden SSF 3492 eller tilsvarende.

Andre skabe kan godkendes med FE og FMI medvirken i fysisk test af produktet.

Ældre skabe, der overholder kravene jf. Standardtyvmetoden, GUL klasse hovedgruppe 2, kan fortsat anvendes som et klasse B skab.

10. ANDRE OPBEVARINGSMIDLER, KLASSE C

Opbevaringsmidler af træ, klasse C.

Opbevaringsmidler af træ (skriveborde, skabe, kasser mv.) må normalt kun anvendes til permanent opbevaring af materiale, der er klassificeret til og med TTJ. Solide opbevaringsmidler af træ med sikkerhedsgodkendt aflåsning anvendes under feltmæssige forhold, hvor der til stadighed skal være etableret bevogtning/kontrol.

"RUM I RUM" CELLESKAB:

Der anvendes i høj grad i dag bygningskonstruktioner med store glaspartier og med få rumadskillelser, der har karakter af stabil bygningsdel.

Det vil derfor ofte være vanskeligt, og måske økonomisk set være for dyrt at etablere de ønskede rum (celler) i stabile bygningsdele i en allerede opført bygning.

Der er i stedet mulighed for at anvende det der kan betegnes som "rum i rum" løsninger. Konstruktionen går i sin enkelthed ud på at etablere et rum (celle) i det ønskede rum.

Celleskabe skal være konstrueret af minimum 2 – 4 mm stålplade med en tilsvarende dør og sikkerhedsgodkendt låseenhed IV. Lås skal være en af Forsvaret sikkerhedsgodkendt ABLOY type.

Inde i cellen placeres sikringsskabet, der fastgøres til gulv og stålvæg i cellen.

Størrelsen af celleskabet i stål er normalt så stor, at det skal samles inde i det rum, hvor det skal opstilles. Det betyder, at skabet ikke kan fjernes af uvedkommende, når det først er monteret, uden at vægge rives ned.

Celleskabet kan leveres i størrelse efter mål og i de farver, der ønskes.

Fordelen ved denne løsning er, at celleskabet kan nedtages og flyttes til et andet rum efter behov.

"Rum i rum" løsningen skal som minimum objektsikres i form af elektronisk overvågning. Produktet er ikke testet efter nogen standard, men der findes leverandører, som kan tilbyde modulskabene.

11. MATERIALER OG LEVERANDØRER

Oversigt over ståldøre til boks- og arkivrum, våbenkamre mv. samt oversigt over penge-skabe, sikringsskabe og opbevaringsmidler kan indhentes ved Forsvarets Hovedværksteders, Installationsværksted Korsør. Anskaffelse af opbevaringsmidler skal finde sted i samarbejde med Forsvarets Låsetjeneste af hensyn til muligheden for at gennemføre vedligeholdelse/reparation.

Produkterne er kodificerede og fremgår af materieloversigter.

MEKANISK SIKRING

GODKENDTE KLASSIFICEREDE LÅSEENHEDER

Ref.: [Brancheorganisationen Forsikring & pensions hjemmeside \(Sikringsprodukter\)](#)

Efterfølgende tekst i kursiv er regler F&P anvendte i forbindelse med Standardtyvmetoden. Teksten bibeholdes indtil videre på grund af de produkter og låseenheder, der anvendes i koncernen efter den gamle standard.

1. GODKENDTE /KLASSIFICEREDE LÅSEENHEDER

Godkendte og klassificerede låseenheder indgår som en del af ref. Regler for indbrudssikring stiller krav om godkendte låse med tilhørende slutblik. *Som aflåsningsform til låsekasserne anvendes låsecylinder- eller tilholderprincippet, der, jf. efterfølgende tekst, giver mulighed for klassificering i klasserne GUL, GRØN, BLÅ og RØD.*

I koncernen anvendes alene klasserne GUL (i kontrollerede/overvågede områder) og RØD (i sikrede områder).

En låseenhed består af:

- En Mekanisk låsecylinder (EN 1303)/Mekatronisk låsecylinder (EN 15684),
- En sikkerhedsgodkendt låsekasse (EN 12209)/ Sikkerhedsgodkendt låseslutblik (EN 14846),
- Beslag (EN 1906).

Ved sikringsniveau 20 – 60 skal der anvendes Forsvarets låsecylindre (ABLOY), der skal leveres og monteres af Forsvarets Hovedværksteders Låsetjeneste.

Ved sikringsniveau 10 skal låseenheder monteres af en F&P godkendt låsesmed.

Endvidere findes klassificerede hængelåse med tilhørende beslag.

2. GODKENDTE LÅSEKASSER (EN 12209, EN 14846)

Godkendelse af låsekasser beror primært på afprøvninger foretaget af Stöldskyddsföreningen i Stockholm og af Verband der Sachversicherer e.V. i Köln i henhold til Dansk Standard nr. 350.

Grundlæggende krav:

- Falle- og rigellås anvendes normalt
- Riglen skal mindst have 20 mm fremspring i én tur ved nøgledrejning 360°
- Rigle skal være af mindst 20 mm lamineret zinkbehandlet stål
- Låsekassen skal
 - Mindst være en grade 3 i henhold til DS/EN 12209 (sikringsniveau 10)
 - Mindst være en grade 7 i henhold til DS/EN 12209 (sikringsniveau 20 til 60)
- Såfremt der ønskes en elektromekanisk betjent lås i yderdøre skal det være en motorlås.

3. GODKENDTE SLUTBLIK (EN 12209, EN 14846)

Til de godkendte låse hører normalt et godkendt slutblik, der ligeledes har været underkastet afprøvninger, hvis primære formål er, at slutblikket kan modstå et tryk/træk på minimum 700 kg.

4. KLASSIFICEREDE LÅSECYLINDRE (NØGLECYLINDER)

Cylinderen er en udskiftelig del af låsen og bør, jf. klassificeringen, svare til kravene om mekanisk sikring i klasserne GUL, GRØN, BLÅ og RØD.

Cylindre af GUL klasse kan anvendes i sikringsniveau 10.

Cylindre af RØD klasse kan anvendes i sikringsniveau 20 til 60. Cylindre af rød klasse leveres, monteres og serviceres af Forsvarets Hovedværksteders Låsetjeneste.

Grundlæggende krav:

- Låsecylinderen skal mindst have 6 stifter/skiver
- Låsecylinderen skal være dirkesikker og borebeskyttet
- Nøglen skal kunne være en system nøgle
- Nøglen skal være patenteret
- Låsecylinderen skal være en skandinavisk cylinder
- En klassificeret låsecylinder på en godkendt låsekasse skal altid beskyttes med et sikkerhedslangskilt eller en cylinderring
- Låsecylinderens fremspring må max. være 2 mm.

Låsecylindre af DIN typen (også benævnt dråbelås) må ikke anvendes i koncernen som sikkerhedsbetydende aflåsning.

5. SIKKERHEDSGODKENDTE HÆNGELÅSE

Sikkerhedsgodkendte hængelåse, der skal anvendes i sikrede områder, skal leveres og serviceres af Forsvarets Hovedværksteders Låsetjeneste.

6. MOTORLÅSE OG MAGNETLÅSE

Der kan anvendes en mekanisk sikkerhedsgodkendt modul låsekasse med korrekt slutblik mv. for korrekt aflåsning af yderdøre og døre ind til sikrede områder (betydende døre med Forsvarets låsecylinder).

Alternativt kan der anvendes sikkerhedsgodkendte motorlåse i yderdøre og til sikrede områder ud fra ønsket om en elektronisk registrering af brugerne (ADK).

Elektroniske låse (magnetlåse, el-slutblik og langskilte) kan alene anvendes i inderdøre i sikrede områder (ikke sikkerhedsmæssige betydende døre).

7. KRAV TIL YDERDØRE

Låseenheden til yderdøre skal enten være:

- En sikkerhedsgodkendt mekanisk modullås eller
- En sikkerhedsgodkendt motorlås.

Leverandøren af døre skal tilsikre, at der kan monteres en sikkerhedsgodkendt låsekasse i dimensionen 22 x 94 x 150 mm.

MEKANISK SIKRING

LÅSE, NØGLER OG KODER

1. INDLEDNING

1.1. Låse.

Låse er mekaniske sikringsforanstaltninger, der omfatter nøglelåse og kodelåse (kombinationslåse) anvendt som fast monterede låse eller hængelåse. Låse med tilhørende slutblik eller beslag har varierende anvendelsesmuligheder og sikringsmæssig værdi.

1.2. Nøglerlåse.

Nøglerlåse omfatter et stort antal enheder, der strækker sig fra simple konstruktioner, som let kan brækkes eller dirkes op, til avancerede låse, som vanskeligt kan brydes op, og som ikke kan dirkes op.

1.3. Kodelåse.

Kodelåse omfatter et begrænset antal typer, som alle yder god sikkerhed mod manipulation.

1.4. Elektriske låseenheder.

Elektriske låseenheder, der er baseret på andre former for spærreorganer end de mekaniske, må benyttes, hvis de opfylder krav til styrke, sikkerhed og holdbarhed.

Elektriske låseenheder kan benyttes i forbindelse med fjernoplukning, adgangskontrolanlæg, port- og dørtelefonanlæg, elektrisk fjernaflåsning og elektriske dørlåse.

2. SIKKERHEDSGODKENDTE LÅSE

Låse, der anvendes i sikre områder (kategori 1 og 2), skal være sikkerhedsgodkendt, samt være bestykket med en af Forsvaret godkendt låsecylinder Abloy.

Sikkerhedsgodkendte låsecylindre i koncernen er låse, der forvaltes og serviceres alene af Forsvarets Hovedværksteders Låsetjeneste.

Nøgler til sikkerhedsgodkendte låsecylindre har en beskyttet profil og nøglerne tildannes og leveres af Forsvarets Hovedværksteders Låsetjeneste med 2 stk. pr. lås.

Sikkerhedsgodkendte låse omfattende fast monterede nøglelåse og hængelåse er i et fabrikat (særlig profil), der er forbeholdt Forsvaret.

Forsvarets Hovedværksteders låsetjeneste varetager sammen med Forsvarsministeriets Materiel- og Indkøbsstyrelse opretholdelse af Forsvarets særlige låsecylinderprofil.

3. FAST MONTEREDE NØGLELÅSE

Fastmonterede nøglelåse findes som dørlåse, pengeskabslåse, stålskabslåse, møbellåse osv.

3.1. Tilholderlåse.

Tilholderlåse findes i forskellige fabrikater og med forskelligt antal tilholdere. Tilholderlåse kan anvendes til aflåsning i kategori 3 og 4 område.

Af sikringsmæssige hensyn bør nøglelåse, hvor nøglen kun kan anvendes fra den ene side (usymmetrisk nøgleudskæring), foretrækkes.

3.2. Stiftcylinderlås.

Stiftcylinderlås findes i forskellige fabrikater med forskelligt antal stifter og forskellige nøgleprofiler. Den almindeligt anvendte cylinderlås med 5 stifter yder – uanset nøgleprofil – kun ringe sikkerhed mod opdirkning. Stiftcylinderlås med kun 5 stifter skal snarest belejligt udskiftes til minimum en 6 stiftet låsecylinder.

3.3. Skivecylinderlås.

Skivecylinderlås findes af fabrikat ABLOY med forskellige nøgleprofiler. Låsen yder god beskyttelse mod opdirkning. ABLOY skivecylinderlås med Forsvarets profil er sikkerhedsgodkendt til aflåsning.

3.4. Pengeskabslås.

Pengeskabslås findes i forskellige fabrikater og er monteret i opbevaringsmidler, klasse A og B. Pengeskabslås, som er monteret i autoriserede opbevaringsmidler, klasse A og B, er alle sikkerhedsgodkendte låse.

4. FAST MONTEREDE KODELÅSE

Fast monterede kodelås (kombinationslås) findes som 3-tals kodelås, fx SARGENT AND GREENLEAF 8415, og 4-tals kodelås, fx. KROMER 3010, og anvendes i opbevaringsmidler. De i koncernen anvendte fast monterede kodelås er alle manipulationssikret og sikret mod radiologisk forcering samt sikkerhedsgodkendt til aflåsning for alle klassifikationsgrader og særlige mærkninger.

Elektroniske kodelås må ikke anvendes som primær aflåsning i ydre skallen indtil sikrede område kategori 1 og 2.

5. HÆNGELÅSE

Hængelås findes i mange fabrikater og i mange forskellige kvaliteter. Hængelås og beslag er lette at montere, men er sårbare over for angreb fx overskæring af låsebøjle eller låsebeslag. Hængelås med fjederpåvirket bøjle (smæklås) bør undgås. Hængelås bør betragtes som en sekundær aflåsning og bør kun anvendes som primær aflåsning, hvor fast monterede låse ikke kan anvendes, og hvor de sikringsmæssige hensyn er tilgodeset på anden måde (bevogtning, tilsyn, overvågning mv.).

Sikkerhedsgodkendt aflåsning omfatter såvel hængelås som låsebeslag og hængelåsskyttelse. De sikkerhedsgodkendte nøgle-hængelås har skivecylinder og speciel nøgleprofil samt hærdet stålbøjle, minimum 8 mm til indendørs brug og minimum 10 mm til udendørs brug. Disse hængelås kan anvendes som sikkerhedsgodkendt aflåsning.

6. LÅSESYSTEM (NØGLESYSTEM)

Ved låsesystemer opnås mulighed for, at ihændehaber af en nøgle i systemet kan åbne netop de låse, som vedkommende har behov for at kunne åbne. Et låsesystem kan omfatte:

- Centralnøglesystem, hvor forskellige nøgler kan åbne fælles låse.
- Hovednøglesystem, hvor én hovednøgle kan åbne forskellige eller alle låse.
- Generalhovednøglesystem, hvor én generalhovednøgle kan åbne forskellige eller alle låse i flere hovednøglesystemer.

Låsesystemer i koncernen omfatter udelukkende cylinderlåse, oftest fast monterede låse, men også hængelåse kan indgå i systemet. Anvendelse af låsesystemer kan give indlysende fordele, men medfører samtidig sikkerhedsmæssige svagheder. Bortkomst af en systemnøgle kompromitterer hele eller dele af et låsesystem, og brugeren af et lokale kan påberåbe sig, at andre til enhver tid kan få adgang til lokalet. Desuden vil den sikringsmæssige værdi af en lås, som kan åbnes af flere forskellige nøgler, reduceres i takt med antallet af sådanne åbningsmuligheder. Lokaler, hvis indhold eller anvendelse kræver særlig sikkerhedsbeskyttelse, samt opbevaringsmidler for klassificeret materiale bør ikke indgå i låsesystemer.

Skematisk oversigt over et låsesystem fremgår af pkt.8.1 – 8.3 og nøgleplan af pkt. 9.1.

7. FORVALTNING AF NØGLER OG KODER

Nøgler, der giver adgang til sikrede områder, ammunitionsmagasiner, sikkerhedsgodkendte opbevaringsmidler samt anden sikkerhedsgodkendt aflåsning, benævnes sikkerhedsbetydende nøgler. Disse nøgler leveres af Forsvarets Hovedværksteders Låsetjeneste. Brugernøgler er betegnelsen for nøgler til kontorer og opbevaringsmidler, der dagligt anvendes af personellet.

Når sikkerhedsbetydende brugernøgler ikke anvendes, skal de enten opbevares i et klasse A nøgleskab, i en celle, som er sikret til sikringsniveau 40 (fx et nøgleskab), der kan være suppleret med "musefælder", således at ingen uvedkommende har adgang til en anden brugers nøgler, eller ved opbevaring under fuld kontrol ved et kontrolpunkt, vagtlokale el. tilsvarende.

Sikkerhedsbetydende brugernøgler må ikke medtages fra tjenestestedet med mindre det er i tjenstligt øjemed..

Reservenøgler er betegnelsen for nøgler til kontorer og opbevaringsmidler, der kun tages i anvendelse, såfremt brugernøgler periodisk ikke er til rådighed. Reservenøgler må kun anvendes med tilladelse af sikkerhedsofficeren. Reservenøgler opbevares i autoriseret kuvert centralt ved sikkerhedsofficeren eller en af ham udpeget person. Reservenøgler skal opbevares på en sådan måde at ibrugtagning registreres. Brugernøgler og reservenøgler må ikke opbevares i samme opbevaringsmiddel.

Sikkerhedsofficeren er ansvarlig for, at der udarbejdes en nøgleplan over sikkerhedsbetydende nøgler.

Opbevaringsmidler, der indeholder sikkerhedsbetydende nøgler, skal såfremt de ikke er under direkte fysisk kontrol (fx i vagtlokale eller kontrolpunkt) anbringes i sikret område og efter nærmere direkte aftale med FE i overvåget område.

Procedurer for ind- og udlevering af nøgler/koder og reservenøgler, samt rekvirering/omlægning af nøgler/koder og kontrol af nøgler/koder bør fremgå af den lokale sikkerhedsinstruks.

7.1. Pengeskabslåse.

Pengeskabslåse leveres med to nøgler. Der skal foreligge bestemmelser for opbevaring af brugs- og reservenøgler, og der skal etableres kvitteringssystem for udleverede brugsnøgler. Reservenøglen må aldrig anbringes i det opbevaringsmiddel, hvortil nøglen giver adgang.

Omlægning af pengeskabslåse udføres af Forsvarets Hovedværksteders Låsetjeneste.

Pengeskabslåse (nøgleslåse) omlægges/omstilles:

- ved tab, bortkomst el. kompromittering/formodet kompromittering af nøgler,
- ved brugerens afgang.

Omlægning/omstilling af pengeskabslåse skal fremgå af oversigt hos sikkerhedsofficeren.

7.2. Kodelåse.

Kodelåse (kombinationslåse) på opbevaringsmidler er ved leveringen indstillet på kodetallet 50. Ved brugende myndigheder mfl. skal enhver kodelås, der ikke er i anvendelse, stilles på kodetallet 50. Elektroniske kodelåse er indstillet 1, 2, 3, 4, 5, 6.

Tjenestestedets sikkerhedsofficer er ansvarlig for omstilling af kodelåse, og kodetallet må ikke noteres andre steder end i behørigt forseglet kuvert, der - med fornødne påtegninger - opbevares i et andet godkendt elektronisk overvåget opbevaringsmiddel efter tjenestestedets nærmere bestemmelse.

Kodelåse på opbevaringsmidler og kodehængelåse omstilles:

- halvårligt,
- ved kompromittering eller mistanke herom,
- ved afgang af personel med kendskab til kodetallet.

Omstilling af kodelåse skal fremgå af oversigt hos sikkerhedsofficeren.

Elektroniske kodelåse må ikke anvendes som primær aflåsning i ydre skallen indtil sikrede områder.

7.3. Fast monterede nøgleslåse.

Fast monterede nøgleslåse, der er primær aflåsning af lokaliteter, hvis indhold eller anvendelse kræver sikkerhedsbeskyttelse, bør - af hensyn til effektiv nøglekontrol - kun forsynes med det antal nøgler, der er absolut behov for.

Sikkerhedsgodkendte låse leveres med to nøgler, undtagelsesvis med tre nøgler efter særlig aftale. Der skal etableres et kvitteringssystem for udleverede brugsnøgler til sikkerhedsgodkendte låse.

Fortegnelse over sikkerhedsgodkendte låse samt fordeling af brugs- og reservenøgler skal bero hos sikkerhedsofficeren eller af en af ham udpeget person.

Sikkerhedsgodkendte låse omlægges/udskiftes

- ved tab, bortkomst eller kompromittering/formodet kompromittering af nøgler,
- ved afgang af personel, hvor særlige forhold taler herfor,

7.4. Ekstra nøgler.

Anskaffelse (rekvirering) af ekstra nøgler til sikkerhedsgodkendte låse kan kun finde sted med tjenestestedets bemyndigelse.

Omlægning/udskiftning af sikkerhedsgodkendte låse samt anskaffelse af ekstranøgler hertil skal fremgå af oversigt hos sikkerhedsofficeren. Hvis der ønskes mere end 3 nøgler skal FE give tilladelse til anvendelsen.

Et betydeligt antal lokaliteter, der indeholder materiel mv. af operativ og økonomisk værdi (garager, depoter, kontorer mv.), har ikke krav om sikkerhedsgodkendt aflåsning. Uagtet at der ikke er krav om sikkerhedsgodkendt aflåsning, bør det overvejes at anvende et sikkerhedsgodkendt låsesystem, hvor det er muligt at gennemføre effektiv kontrol af såvel

bruger- som reservenøgler samt for at undgå muligheden for ukontrolleret anskaffelse af ekstranøgler.

Anvendes ikke sikkerhedsgodkendt aflåsning bør det tilstræbes, at sådanne låse omlægges/udskiftes, når kontrollen med brugsnøgler vurderes sikkerhedsmæssigt ukontrollabelt. Fordeling og anskaffelse af nøgler samt omlægning/udskiftning af låse bør fremgå af oversigt ved etablisementsforvaltende myndighed og sikkerhedsofficeren.

7.5. Hængelåse.

Hængelåse (nøglehængelåse), der anvendes som primær aflåsning for materiale mv., der kræver sikkerhedsbeskyttelse, bør - af hensyn til effektiv nøglekontrol - kun forsynes med det antal nøgler, der er absolut behov for.

Sikkerhedsgodkendte hængelåse leveres med to nøgler.

Sikkerhedsgodkendte hængelåse, der anvendes som primær aflåsning for opbevaringsmidler mv. for klassificeret eller andet materiale, der kræver sikkerhedsbeskyttelse, omlægges/udskiftes/ ombyttes

- ved tab, bortkomst eller kompromittering/formodet kompromittering af nøgler,
- ved afgang af personel, hvor særlige forhold taler herfor,

Fordeling/omlægning/udskiftning/ombytning af sikkerhedsgodkendte hængelåse med tilhørende nøgler skal fremgå af oversigt hos sikkerhedsofficeren.

7.6. Tab, bortkomst eller kompromittering af nøgler.

Tab, bortkomst eller kompromittering af nøgler til sikkerhedsgodkendte hængelåse skal fremgå af oversigt hos SIKOF.

Det bør tilstræbes, at ikke-sikkerhedsgodkendte hængelåse, der anvendes som primær aflåsning af lokaliteter indeholdende materiel (garager, depoter mv.), udskiftes/ombyttes når kontrollen med brugsnøgler vurderes at være sikkerhedsmæssigt ukontrollabelt.

7.7. Fordeling af låse og nøgler.

Fordeling af låse og nøgler til sådanne lokaliteter bør fremgå af oversigt ved brugende myndighed (sikkerhedsofficeren).

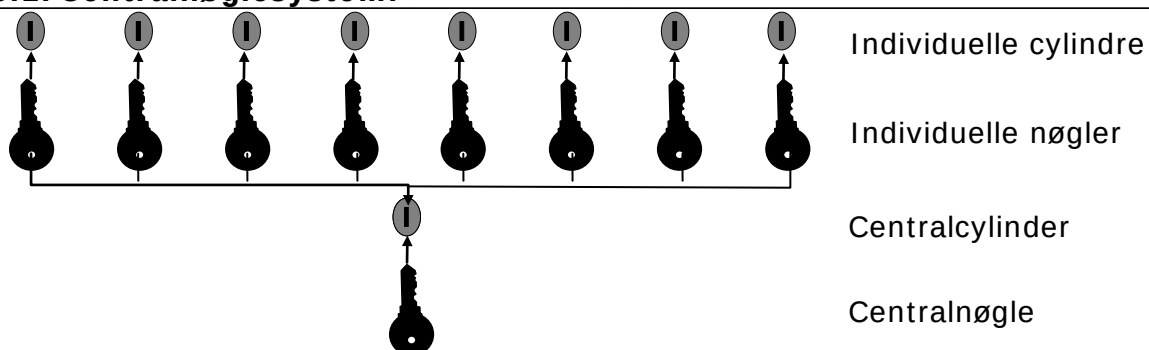
Eksempel på nøglekvittering fremgår af pkt. 9.2.

7.8. Mønstring af sikkerhedsgodkendte låse.

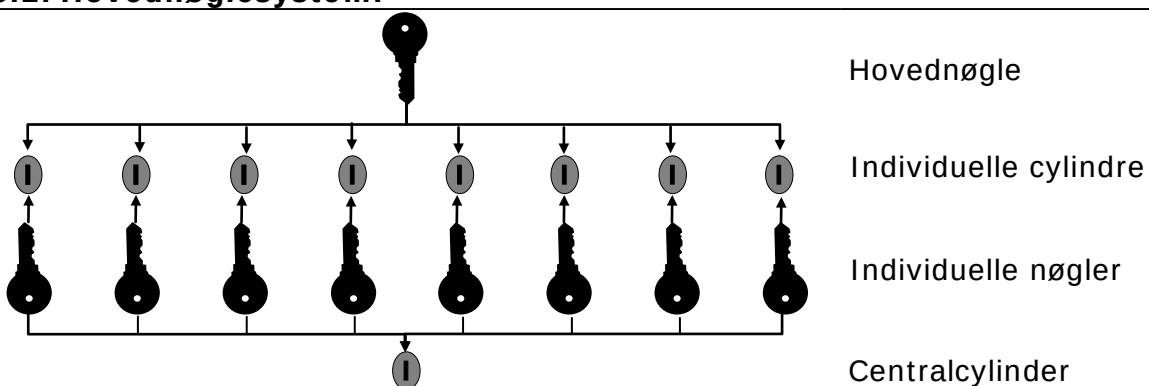
Mønstring af sikkerhedsgodkendte låse med tilhørende nøgler gennemføres årligt i.h.t. nøgleplaner og -kvitteringer. Mønstringsgrundlaget kan indhentes hos Forsvarets Låsetjeneste. De under mønstringen konstaterede uregelmæssigheder, herunder bortkomster, skal fremgå af mønstringsrapporten. Den skal forelægges myndighedens chef til underskrift og opbevares ved myndigheden i 10 år.

8. LÅSESYSTEMER

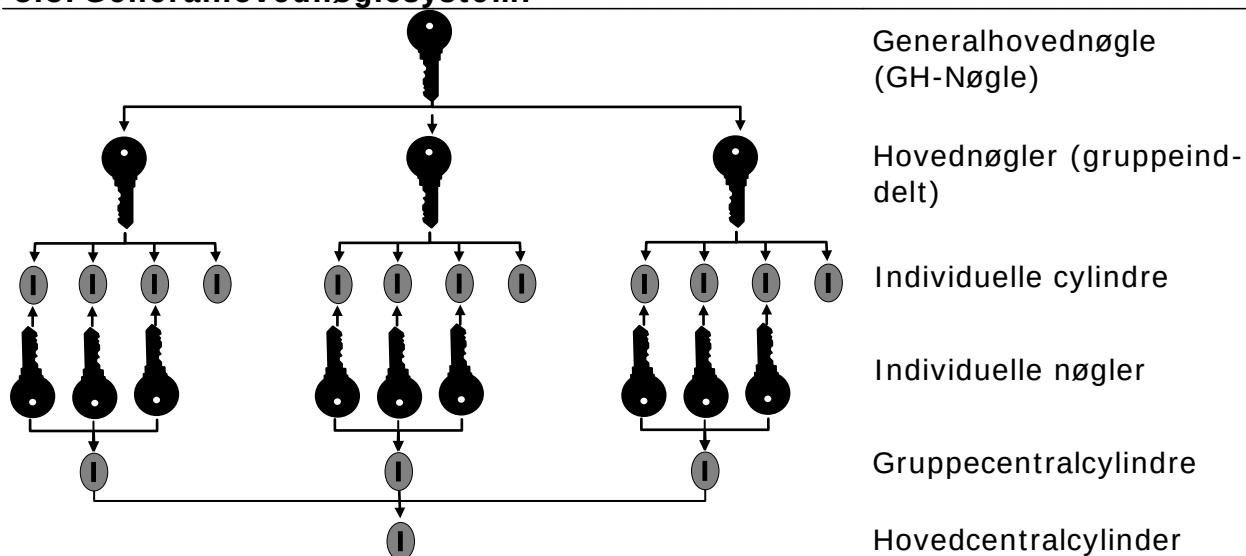
8.1. Centralnøglesystem.



8.2. Hovednøglesystem.



8.3. Generalhovednøglesystem.



9. FORMULARER, FORSVARETS HOVEDVÆRKSTEDERS LÅSETJENESTE

9.1. Nøgleplan.

 Forsvarets Hovedværksteders Låsetjeneste 		Husk monstring jf. FKOBST 358-1, Bilag til kapitel 7, bilag 4, underbilag 7, punkt 7.8 TIL TJENESTEBRUG Ændringer meddeles til FH Låsetjeneste (Når udfyldt)																																							
Nøgleplan for _____		BETEGNELSE RUM BYG CYL LAS																																							
System nr. _____																																									
Oprettelsesdato _____																																									
Godkendt af _____																																									
Underskrift																																									
Dato _____ Navn _____																																									
Revideret dato	Udført af	NØGLER	MRK	ST	I-NR	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32				

☐ Kopi Sikkerhedsofficer ☐ Kopi Etablisementsforvaltning VKH-08/17

SIKRINGSKRAV TIL VAGTLOKALER

1. VAGTLOKALER.

1.1. Mekanisk sikring

Vagtlokaler skal indrettes således, at vagtpersonellet sikres mulighed for selv at afværge et overfald eller at alarmere politi eller reaktionsstyrke. Vagtlokaler skal opfylde følgende minimumskrav:

- Ydervægge skal være udført i stabile bygningsdele.
- Adgangsdøre skal til stadighed være aflåste.
- Det skal være muligt at hindre indsigt udefra (f.eks. ved gardiner, rullegardiner eller skodder).
- Der skal være mulighed for at belyse adgangsveje til vagten. Betjeningen heraf skal kunne ske fra vagtlokalet.

1.2. Elektronisk overvågning

Hvis der i vagtlokalet terminerer alarmer eller anden elektronisk overvågning, der beskytter våben, ammunition, eksplosivstoffer, vitalt sensitivt materiel eller højt klassificerede informationer (FORTROLIGT og højere), skal følgende yderligere krav opfyldes:

- Adgangen til lokalet skal være kontrolleret ved enten et ADK-anlæg, der opfylder kravene til sikrede områder (underbilag 1 til bilag 7 til kapitel 7), eller ved en procedure, hvor adgangsdøren først kan åbnes, når den adgangssøgende er identificeret inde fra lokalet (f.eks. ved brug af dørspion eller videoovervågning).
- Der skal være etableret overfaldstryk (skal anskaffes gennem FES), der terminerer ved anden kontrolcentral eller politi.
- Lokalet skal som minimum indrettes som sikret område, kategori 2, sikringsniveau 40, hvis det ikke er døgnbemandet.

KRAV TIL KONTROLCENTRAL

1. PLACERING.

Kontrolcentralen skal placeres indenfor en bevogtet militær installation, og skal som minimum placeres mindst 200 meter fra et perimeterhegn.

Vagtstyrken på den militære installation skal være døgnbemandet og have en størrelse, der tilsikrer, at Kontrolcentralen også er operativ, når Forsvaret går op i bevogtningstrin. Kravet til vagtstyrken er jf. bilag 4 til kapitel 7.

2. MEKANISK SIKRING

Kontrolcentralen skal etableres i **sikringsniveau 40**. Kontrolcentralen skal opfylde følgende minimumskrav:

- Den mekaniske sikring skal opfylde EN 1627-30, RC 4 eller jf. EN 1143-1 grade 1.
- De stabile bygningsdele skal have en tilsvarende gennembrydningstid.
- Alle udvendige døre skal være aflåst med to godkendte og klassificerede låseenheder IV. Der skal anvendes to af Forsvarets sikkerhedsgodkendte låsecylindre (ABLOY). Dette gælder også døre ind til højere sikrede områder, sikringsniveau 50/60 samt døre ind til serverrum og lokaler til våbenopbevaring mm.
- Udvendige vinduespartier skal opfylde EN 356, P6B og EN 1522, FB 5.
- Der skal etableres sluse ind til kontrolcentralen.
- Det skal være muligt at hindre indsigt udefra.
- Rundt om Kontrolcentralen skal der i en afstand på mindst 8 meter etableres
- minimum et 2 meter højt perimeterhegn med tre rækker pigtråd eller spiralpigtråd på toppen.
- Der skal etableres ADK i perimetersikringen. ADK skal etableres med et samtaleanlæg og en kamerafunktion.

3. ELEKTRONISK OVERVÅGNING

- Skal opfylde kravene til sikringsniveau 40.
- Der skal etableres sluse ind til Kontrolcentralen. Der må ikke kunne være flere adgangsveje/døre åbne samtidig.
- Der skal etableres TVO, således at perimeterhegnet og arealet mellem kontrolcentralen og bygningen er overvåget.
- Det skal være muligt via TVO at identificere en person, som er i området omkring kontrolcentralen.
- Der skal etableres overfaldsalarmer/tryk. Overfaldstrykket skal gå til den lokale vagtcentral og til vagtcentralen ved Reservekontrolcentralen.
- Der skal være signalredundans mellem Kontrolcentral og Reservekontrolcentralen.

4. KRAV TIL ANDRE RUM ELLER LOKALER I KONTROLCENTRALEN

- Hvis der er højere klassificerede rum eller områder inde i Kontrolcentralen, skal de opfylde de respektive krav til henholdsvis den mekaniske sikring og den elektroniske overvågning.

5. ÅBNINGER I BYGNING

- Der må være følgende åbninger i bygningen: Slusen, nødudgangen, vinduespartier, "service åbninger", skuffe ind i det operative område samt ventilation.

6. SIKRING AF DRIFTEN

- Bygning skal sikres imod lynnedslag, oversvømmelse og vejr- og vindpåvirkninger.
- Der skal være toilet, bade- og køkkenfaciliteter inde i bygningen, men adskilt fra det operative område.
- Bygningen skal være koblet til en ekstern strømforsyning med 12 timers nonbreakable backsystem af UPS. Derudover skal Kontrolcentralen være tilkoblet et nødstrømsanlæg.
- Nødstrømsgeneratoren kan placeres inde i Kontrolcentralens område, alternativt i et andet sikret område (2-30 eller højere).

ELEKTRONISK OVERVÅGNING

FASTLÆGGELSE AF OVERVÅGNINGS- OG/ELLER KONTROLMETODER

Ref.: [Brancheorganisationen Forsikring & pensions hjemmeside](#)

Underbilag:

1. Systemdele i installationen, F&P klassificerede systemdele.
2. Transmission af elektroniske alarmer.

1. AUTOMATISKE INDBRUDSALARMANLÆG

Automatisk indbrudsalarmanlæg (AIA-anlæg) skal opbygges af centraludstyr, detektorer mv., der opfylder tekniske, kriminaltekniske og betjeningsmæssige krav anført i anerkendte normer eller standarder, der er relevante for den givne sikring, i henseende til følsomhed og modstandsdygtighed over for det aktuelle driftsmiljø mv.

AIA-anlæg skal opbygges som et fuldt adresserbar system, med mulighed for at kunne håndtere indbrudsalarm, verificeret indbrudsalarm, overfaldsalarm, sabotagealarm, system alarm, teknisk alarm, alarm for linjefejl, alarm for manglende tilkobling, alarm for uventet frakobling samt varsling for batterifejl.

Verificeret alarm er defineret som modtagelse af 2 af hinanden uafhængige indbrudsalarmer til kontrolcentral (standarden DS/EN518)/lokal vagtcentral fra sikringskomponenter inden for 10 min.

AIA-anlæg omfatter centraludstyr, som består af AIA- centraler og AIA- betjeningspaneler, som henholdsvis er den del af anlægget, der modtager, behandler og viderebringer signaler fra det øvrige udstyr, og den del der anvendes til betjening, og visning af alarmer mv.

AIA- centralen skal være anbragt i et sikringsniveau 40 område med mulighed for 24/7 adgang til bemyndiget teknisk personale.

Kontrolcentralen/den lokale vagtcentral er en modtagecentral for alarmsignaler til monitoring registrering og behandling af modtagne alarmer fra tilsluttede AIA-anlæg.

Kontrolcentral/lokale vagtcentraler skal være etableret i et sikret område.

I forbindelse med oprettelse af et elektronisk overvåget område skal forhold som sikringsniveau, gennembrudstid, reaktionstid, retablering af sikringsforholdene og forholdsordre for de forskellige alarmsignaler fastlægges.

F&P klassificerede systemdele indeholdt i en installation fremgår af ref.

2. AUTOMATISKE ADGANGSKONTROLANLÆG

Automatiske adgangskontrolanlæg (ADK-anlæg) skal opbygges af udstyr, der overholder krav til teknik, sikkerhed, drift og betjening anført i anerkendte normer eller standarder.

Ved oprettelse af ADK-anlægget skal databasen indeholde oplysninger om fysiske døre, og personlige adgangskort.

Adgangskort oprettes i databasen med et løbenummer (både et synlig og et skjult/krypteret identifikationsnummer). Adgangskortet udstedes til en person med brugers navn og medarbejdernummer samt en personlig krypteret kode.

Ved oprettelse af rettigheder til et personligt adgangskort, registreres de adgangsgivende døre med de tilhørende tidsintervaller i databasen.

Korrekt brug af et ADK- system indebærer korrekt brug af adgangs og personlig kode.

Ved anvendelse af et adgangskort på en ADK- kortlæser, kontrolleres kort og kode i systemets database for gyldig adgang, før dør frigives for adgang,

Kortet med navn og billede bruges til visuel opholdskontrol og visuel adgangskontrol.

Centraludstyret og dermed registreringsdatabasen og web klienter er de enheder som rummer, håndterer samt registrerer rettigheder og anvendes til kodeadministration. Centraludstyret og web klienter skal være etableret i et område, som sikres til sikringsniveau 40.

Elektroniske offline nøglesystemer (f.eks. SALTO) til ikke sikkerhedsbetydende døre:

Døre oprettes i offline databasen og efterfølgende programmeres adgangskortlæseren på dørene/langskiltene, således at hver dør har sin egen unikke identitet.

Medier oprettes i offline databasen med angivelse af løbenummer og bruger (navn og medarbejdersnummer).

Ved angivelse af rettigheder til et medie foretages det på en WEB klient med adgang til offline databasen, hvor der gives rettigheder til at kunne tilgå en eller flere offline døre. Mediet programmeres herefter ved at anvende et lokalt Hot Spot for indlæsning af rettigheder. Herefter kan mediet anvendes for adgang til de døre, som der er givet rettigheder til.

Indlæsningsenheden (adgangskortlæseren/langskiltet) foretager automatisk identifikation af data på brugerens medie for efterfølgende at åbne pågældende adgangsvej, ud fra at mediet indeholder gyldig rettighed for adgang.

Elektriske låse (langskilte, magnetlåse, el-slutblik) kan anvendes ved åbning og lukning af ikke sikkerhedsbetydende døre.

Mekanisk sikkerhedsgodkendte låseenheder og sikkerhedsgodkendte motorlåse kan anvendes på yderdøre (sikkerhedsbetydende døre).

3. TV- OG VIDEOOVERVÅGNINGSANLÆG

Anvendelse af TV- og videoovervågningsanlæg (TVO) (som overbygning på perimetersikring og adgangskontrol) har en god præventiv virkning og kan være til hjælp ved verifikation af en alarm samt i en evt. undersøgelse.

Kameraer skal placeres sådan, at hærværk, tyveri eller afdækning normalt ikke kan finde sted. Af præventive grunde bør kameraerne normalt opsættes synlige og videoovervågningen skiltes.

På baggrund af de lokale forhold kan det dog være hensigtsmæssigt at opsætte skjulte kameraer, således at disse beskyttes mod hærværk, tyveri eller afdækning.

Hvis denne løsning vælges, bør færrest mulig have kendskab til placeringen.

Der skal ske konstant optagelse, hvor optagelsen skal opbevares i mindst 29 døgn før data overskrives, og sletning bør først ske efter 30 døgn.

Et kamera er i stand til at foretage en intelligent videoanalyse, og dermed give en varslings baseret på de ændringer af billedet som algoritmerne har beregnet.

Pt. findes der ingen kameraer eller videosystemer, som er blevet klassificeret, således at TVO kan anvendes som sikringskomponent, da der fortsat er mange situationer, hvor videoanalysen fejler, eller hvor sigtbarheden ikke er til stede (tåge, regn, hagl, sne, sandstorm mv).

TVO vil derfor fortsat alene kunne anvendes som supplement til et sikringsanlæg, for verifikation og undersøgelse, såfremt billedkvaliteten tillader det.

Ved anvendelse af TVO skal systemet kunne fungerer 24/7, og såfremt der kræves identifikation ved eks. adgangsveje, skal der installeres supplerende hvidt lys.

Koncernens alarmbehandlingsplatform anvender og er integreret med en universal video-platform, således at der ved modtagelse af en AIA- alarm fra en given lokalitet automatisk kan hentes et kameras billeder frem fra den lokal video server for verifikation af AIA- alar-men.

Der bør opsættes kameraovervågning af kanaliserende adgangsveje som supplement til AIA for verifikation til lokaliteter, hvor der opbevares større mængder våben, ammunition og vitalt sensitivt materiel, herunder fx magasin- og depotområder samt våbenkamre. Overvågningen kan begrænses til steder med kanaliserende ind- og udpassage, hvor det vil være hensigtsmæssigt.

Videooptagelserne skal kvalitativt ved kanaliserende adgangsveje kunne anvendes til at verificere og identificere identiteten af køretøjer og personer.

4. OVERFALDSTRYK

Anvendelse af overfaldstryk (overfaldsalarmer) anvendes som sikring mod gidseltagning af bl.a. centralt placerede chefer i organisationer samt som sikring af personel i sensitive områder fx kontrolcentraler, indsatsstyrker, kurerer m.fl.

Styrelser, stabe og myndigheder fremsætter forslag til angivelse og definition af sensitive områder og anviser forslag til installation af overfaldstryk (overfaldsalarmer). FE skal godkende disse inden arbejdet iværksættes.

Overfaldsalarmeringsgrupper skal være tydeligt afmærket på kontrolcentralen og skal afprøves mindst halvårligt eller ved mistanke om fejl. Der skal forinden afprøvning tages kontakt med kontrolcentralen, så der ikke sker reaktion på afprøvningen. I særlige tilfælde kan overfaldsalarmer terminere direkte hos politiet.

SYSTEMDELE I INSTALLATIONEN - F&P KLASSIFICEREDE SYSTEMDELE

Ref.: [Brancheorganisationen Forsikring & pensions hjemmeside](#)

1. F&P GODKENDT SYSTEMDEL

En F&P godkendt systemdel er en systemdel, hvor et anerkendt prøvningslaboratorium har eftervist, at systemdelen opfylder disse forskrifters minimumskrav til:

- Funktion (virkemåde)
- Konstruktion (udførelse)
- Miljøimmunitet (funktionsdygtighed og pålidelighed i et nærmere angivet driftsmiljø)
- Sabotagesikkerhed
- Softwarekvalitet
- Datablad.

1.1. F&P registreret systemdel

En F&P registreret systemdel er en systemdel eller et forbindelseselement, hvor disse forskrifter ikke stiller prøvningskrav og hvor det tekniske dokumentationsmateriale efterviser, at enheden er af en kvalitet, der er egnet til formålet. Registreringen kan maksimalt opnås for 2 år.

2. ANVENDELSE AF SYSTEMDELE

Systemdele, der indgår i et F&P-godkendt anlæg, skal være godkendt eller registreret hertil jf. disse forskrifter.

Klassificerede systemdele skal anvendes således:

	SIKRINGSNIVEAU					
	10	20	30	40	50	60
Udstyrsklasse 4	X	X	X	X	X	X
Udstyrsklasse 3	X	X	X	X	X	X
Udstyrsklasse 2						
Udstyrsklasse 1	anvendes kun til "privat"					

2.1. Der anvendes alene systemdele i udstyrsklasse, 3 eller 4 i koncernen.

Ved ønske om anvendelse af lavere systemklasser end angivet ovenfor skal FE godkendelse være indhentet.

Udstyr der ikke har en udstyrsklasse, og dermed ikke er registreret som en sikringskomponent, skal altid være godkendt af FE inden brug.

TRANSMISSION AF ELEKTRONISKE ALARMER

1. ALARMNETTET¹

AlarmNettet (tidligere Det Offentlige Alarmsystem), er et overvåget transmissionssystem, der anvender det etablerede telefonnet som fremføringsvej for alarmer mv. Da transmissionen i AlarmNettet foregår ved udenbåndssignalering, kan datatransmission og telefonsamtale ved hjælp af frekvensfiltrering foregå samtidig uden at genere hinanden.

1.1. Anvendelse.

Koncernen anvender AlarmNettet til overføring af alarmer fra forskellige elektroniske overvågningssystemer som tyveri-, brand-, nødkaldeanlæg og overfaldsalarmer.

1.2. Selvkontrollerende.

Systemet kontrollerer sig selv hvert andet sekund, og mellem telefoncentralerne er der alternative fremføringsveje. Eventuelle fejl vil omgående blive registreret, og telefonselskaberne har forpligtet sig til at starte fejlretning inden for tre timer, fra fejlen er meldt.

2. KONCERNENS INTERNE ALARMNET BENÆVNT SIKKERHEDSNET

2.1. Formål.

Forsvarsministeriets Ejendomsstyrelse (FES) er systemansvarlig og har udarbejdet en fagbeskrivelse for sikkerhedsnettet, der i uddrag er beskrevet efterfølgende. Fagbeskrivelsen skal kunne bruges som en opgavebeskrivelse i forbindelse med indhentning af tilbud ved ekstern netværksleverandør, herunder etablering og drift. Fagbeskrivelsen skal samtidigt angive mindstekrav og forventninger til kommunikation imellem typegodkendte alarmtransmittere og Forsvarets Incident Managements System (IMS).

Sikkerhedsnettet har til formål at sammenkoble Forsvarets Kontrolcentraler og tilknyttede etableringer, herunder depoter og magasiner for overførsel af lokal Elektroniske Overvågning (EO).

I den Elektroniske Overvågning indgår Automatisk Indbruds Alarm (AIA), Automatisk Adgangskontrolanlæg (ADK), TV- og videoovervågning (TVO) og Automatisk Brand Alarmeringsanlæg (ABA).

2.2. Ansvar.

FES er ansvarlig for indkøb, etablering, drift, overvågning samt servicering af Sikkerhedsnet imellem Forsvarets kontrolcentraler og de underliggende systemer og anlæg, der skal sende informationer til kontrolcentraler.

FES er ansvarlig for, at Sikkerhedsnettet er tilgængeligt med mulighed for etablering af redundante forbindelser, således at Sikkerhedsnettet til enhver tid tilgodeser EN 50136 (angivet i F&P Sikringskatalog fane 160).

FES er ansvarlig for at tilsikre, at en installation mellem etableringerne og kontrolcentralerne er uafhængig af skiftende netværksudbydere.

Netværksudbyderen (TDC, Nianet m.fl.) er ansvarlig for, at Sikkerhedsnettet friholdes fra andre netværk, således at installation kan etableres med standard netværksudstyr uden yderligere konfiguration.

2.3. Omfang og afgrænsning.

Sikkerhedsnettet omfatter datatransmissionsnet for henholdsvis AIA, ADK, TVO og ABA.

¹ Pkt. 1 vil være gyldigt indtil år 2020. Derefter vil det blive ændret til ny teknologi.

2.4. Sikkerhedskrav.

Sikkerhedsnettets skal som minimum tilgodese de af F&P krav for alarmtransmissionssystemer herunder opfylde kravene til den europæiske standard for alarmtransmission som er angivet i EN 50136.

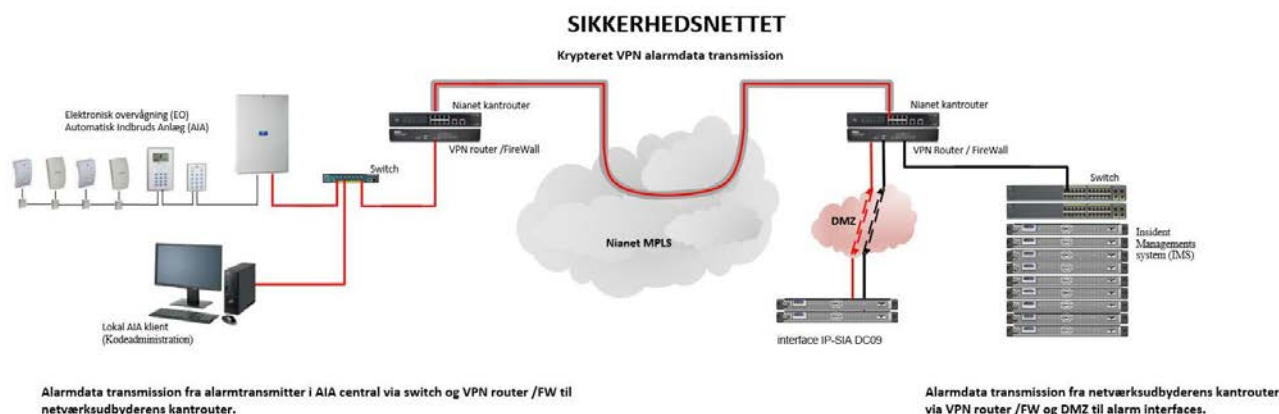
Design og implementering af Sikkerhedsnettets skal gøre det muligt, at:

- overvåge mod afbrydelse ved hjælp af poll- signaler², hvor en evt. afbrydelse skal medføre alarm på kontrolcentralen,
- overholde den maksimale alarmtransmissionstid jf. EN 50136,
- sikre beskyttelse af de transmitterede data ved kryptering samt transmittering via Virtuel Private Network (VPN),
- sikre fortsat drift ved strømsvigt, således det sikres, at alarmsignaler fortsat kan transmitteres til kontrolcentralen, i mindst det tidsrum som er angivet i EN 50131-1.

2.5. Løsning.

Sikkerhedsnettets skal forbinde overvågningssystemer på de enkelte etableringer, depoter og magasiner til Forsvarets kontrolcentraler.

Man kan ikke se på tværs af Sikkerhedsnettets, og dermed imellem Forsvarets lokationer med mindre, at den systemansvarlige ved FES accepterer en tværgående VPN forbindelse ud fra, at systemansvaret kan opretholdes uden at kompromittere systemet og sikkerheden.



2.6. Forudsætning

Forudsætning for at kunne blive tilsluttet Sikkerhedsnettets:

- Overdragelse af fuld ejerskab af lokal kabling og aktivt udstyr som indgår i Sikkerhedsnettets.
- Udlevering af dokumentation af de faktiske forhold vedrørende Sikkerhedsnettets.
- 24/7/365 adgang til FES personale/teknikere til sikret rum med FES rack skab med aktivt og passivt udstyr for tilslutning og opkobling af lokalt sikringsanlæg til kanrouter.

2.7. Supplerende info

Netværksudbyderens fiber og kanrouter fremføres og placeres i et af FES anvist sikret rum for sikringssystemer.

Aktivt og passivt udstyr monteres i et separat aflåseligt telerack, som placeres i særskilt rum, der sikres til sikringsniveau 40.

² Et poll-signal sendes kontinuerligt med et givet interval. Hvis poll-signalet ikke besvares et antal gange i træk, vil det udløse en alarm.

BEVOGTNING

RETNINGSLINIER FOR GENNEMFØRELSE AF BEVOGTNING

Underbilag:

1. Beføjelser for det i bevogtningstjenesten indsatte personel.
2. Uddrag af straffeloven.

1. INDLEDNING

1.1 Definitioner, formål og afgrænsninger

Dette bilag finder anvendelse på bevogtningsaktivitet, der udføres af styrelser, myndigheder og institutioner under Forsvarsministeriets koncernområde i Danmark, på Færøerne og i Grønland i fredstid.

Ved bevogtning forstås den del af den fysiske sikkerhed, der omfatter anvendelse af bevæbnet personel til overvågning, patruljering og reaktion på alarmer mv. samt ledsagelse af transportere. Bevogtningen har til formål at imødegå og hindre uvedkommendes indtrængen og adgang til personel og til vitalt og/eller sensitivt materiel, herunder klassificeret information, våben, ammunition og eksplosivstoffer. Bevogtning af de kongelige slotte og palæer, Rosenborg Slot, kongeskibet samt som bistand til politiet kan foretages som beskrevet i afsnit 2.3. og 2.4.

I afsnit 2 fastlægges retsgrundlaget for bevogtning. I afsnit 3 beskrives den bevogtningsudførende myndigheds ansvar for uddannelse og instruktion af bevogtningspersonellet. I afsnit 4 og 5 beskrives bevogtningspersonellet samt den indbyrdes rollefordeling under bevogtning på militært område, mens afsnit 6 omhandler bevogtning af militære transportere i civilt terræn.

Direktiver for bevogtning i udlandet udsendes øvelses-/ missionsspecifikt.

For nærmere gennemgang og beskrivelse af bevogtningspersonellets udrustning og beføjelser samt grænserne for magtanvendelse henvises til dette bilags underbilag 1.

2. SITUATIONER HVOR DER KAN UDFØRES BEVOGTNING

2.1 Retsgrundlag

Bemyndigelsen til bevogtning af militære områder udledes af de opgaver og beføjelser, som Forsvaret er tillagt i Forsvarsloven¹, i den militære områdelov² og i militær retsplejelov § 13³. Herudover kan bemyndigelsen udledes af den anerkendte ret for en offentlig myndighed til at udstede regler for ophold på myndighedens område, retssædvane⁴ samt principperne om nødværge og nødret i straffelovens §§ 13-14.

Den Kongelige Livgarde blev oprettet af Frederik III i henhold til kongelig resolution af den 30. juni 1658 bl.a. for at beskytte kongen. Amalienborg har været kongefamiliens hovedresidens siden 1794, Fredensborg Slot har været brugt siden 1863, Marselisborg Slot siden 1902 og Gråsten Slot siden 1935. Bemyndigelsen til bevogtning af de kongelige slotte og palæer samt Rosenborg Slot kan derfor ud over i Forsvarsloven findes i resolutionen.

¹ Lov nr. 122 af 27. februar 2001 om Forsvarets formål, opgaver og organisation m.v. med senere ændringer.

² Lov 336 af 6. juni 1991 om forbud mod ophold på og færdsel gennem skydeområder og andre militære områder, jf. også bkg. 73 af 30. januar 2002.

³ Lov nr. 531 af 24. juni 2005, militær retsplejelov, giver i § 13 ved indgang til og udgang fra et militært område adgang til uden retskendelse at foretage kontrol af tøj, bagage, tasker m.v. og af transportmidler.

⁴ En retssædvane er en handlemåde, der er benyttet af myndigheden almindeligt, stadigt og længe ud fra en opfattelse af, at der er tale om en ret- eller pligtmæssig handling. En retssædvane er på niveau med formel lovgivning og kan derfor kun ændres ved en ny lov, herunder også i henhold til grundlovens § 14, 2.pkt.

Forsvarets bistand til politiet, herunder også til bevogtning af samfundsvigtige institutioner, virksomheder eller anlæg med eller uden politimæssige beføjelser, samt adgang til oprettelse af midlertidige militære områder er særskilt reguleret i politilovens kapitel 6a.

2.2 Bevogtning af militære områder

Der kan udføres bevogtning af militære områder. Ved militært område forstås arealer og etablissementer, der benyttes af styrelser, myndigheder og institutioner inden for Forsvarsministeriets koncernområde. Militære områder omfatter bl.a. kaserner, flådestationer, skibe, flyvestationer, skoler, hovedkvarterer, værksteds- og depotområder, øvelsesområder og skydeterræner, men kan også omfatte isolerede stationære militære objekter i civilt terræn såsom kystradarer, hjemmевærnsgårde, depoter og lignende.

Afgrænsningen af det bevogtede område skal være markeret overfor offentligheden. Dette kan ske ved fysiske forhindringer (hegn, bomme mv.), men også fx ved skiltning, pæle-markering eller ved synlig patruljering⁵.

Hvis der skal foretages bevogtning af andet end det ovenfor beskrevne, kan dette kun ske i henhold til punkt 2.3. og 2.4.

2.3 Bevogtning af de kongelige slotte og palæer m.v. samt kongeskibet

Det overordnede ansvar for sikkerheden omkring den kongelige familie på de kongelige slotte og palæer samt Rosenborg Slot, hvor dele af Kongernes Samling⁶ opbevares, påhviler politiet. I forbindelse med kongefamiliens ophold på og sejlads med Kongeskibet Dannebrog påhviler sikkerheden ombord Søværnet.

2.3.1 Ydre bevogtning

Hendes Majestæt Dronningens Adjutantstab er med Den Kongelige Livgardes vagtkompagni ansvarlig for den ydre bevogtning og fysiske adgangskontrol ved Amalienborg samt ved de øvrige kongelige slotte Fredensborg Slot, Marselisborg Slot og Gråsten Slot, når disse er beboet eller benyttes af medlemmer af den kongelige familie⁷. Tilsvarende bevogter vagtkompagniet Rosenborg Slot.

2.3.2 Indre sikkerhed på de kongelige slotte samt Rosenborg Slot

I tilfælde af alarmer og andre akut opståede behov varetages sikkerheden indvendigt i slottene af Hendes Majestæt Dronningens Adjutantstab under evt. anvendelse af vagtkompagniet, indtil politiet når frem. For så vidt angår Rosenborg Slot varetages den indre sikkerhed af Slots- og Kulturstyrelsen, indtil politiet når frem.

2.4 Bevogtning på civilt område

Ved civilt område forstås steder, der ikke er militært område i henhold til afsnit 2.2.

Bevogtning i civilt område er som altovervejende udgangspunkt en politiopgave, og Forsvaret kan derfor i almindelighed kun udføre bevogtning og dermed beslægtede opgaver på civilt område som bistand til politiet⁸. Særlige undtagelser til dette udgangspunkt følger af nedennævnte punkter 2.4.2.-2.4.5.

⁵ Jf. Lov 1991-06-06 nr. 336 om forbud mod ophold på og færdsel gennem forsvarets skydeområder og andre militære områder (Militærømrådeloven).

⁶ Kongernes Samling opbevares på Rosenborg Slot og Amalienborg og har hjemmel i Kongelig Resolution nr. 16001 af den 14. juni 1854 om De Danske Kongers Kronologiske Samling. Resolutionen administreres af Kulturministeriet.

⁷ Jf. Forsvarsministeriets skrivelse til Hendes Majestæt Dronningens Adjutantstab og Forsvarskommandoen dateret den 20. januar 2005, journalnummer: 6. kt. 04-476-1, med bilag med overskriften: Administrationsgrundlag for forsvarets støtte til kongehuset (godkendt af Statsministeriet).

⁸ Forsvarets bistand til politiet er reguleret i lov nr. 708 af den 8. juni 2018 om ændring af lov om politiets virksomhed, herunder kapitel 6a vedrørende Forsvarets bistand til politiet, med tilhørende bekendtgørelse nr. 903 af den 26. august 2018 om Forsvarets bistand til politiet og etablering af midlertidige militære områder. Der henvises samtidig til de udfyldende bestemmelser i Hovedsamarbejdsaftalen mellem politiet og Forsvaret om Forsvarets bistand til politiet og etablering af midlertidige militære områder (med bilag) af den x.x.2019 (aftalen er endnu ikke indgået).

2.4.1 Bistand til politiet

Når bevogtning sker som bistand til politiet i henhold til politilovens § 24a, stk. 1, litra 4, skal formålet være at forebygge og afværge alvorlig kriminalitet og andre hændelser, der kan medføre fare for menneskers liv og helbred eller alvorlig skade på samfundsvigtige institutioner, virksomheder eller anlæg. Bistand vil typisk kunne ydes til bevogtning af truede objekter, som tryghedsskabende patruljeringer i det offentlige rum samt til afspærring og kontrol med særlige områder.

Bistand ydes efter anmodning fra politiet og under politiets operative ledelse i overensstemmelse med de regler, der gælder for politiets varetagelse af pågældende opgave. Det militære personel kan være tillagt særlige politimæssige beføjelser efter politiets nærmere bestemmelser herom. Politiet instruerer Forsvarets personel om rammerne for opgavens løsning samt eventuel anvendelse af magt og brug af magtmidler. Når Forsvaret yder bistand til politiet, undersøges og behandles evt. adfærdsklager over samt evt. strafbare forhold begået af Forsvarets personel af Den Uafhængige Politiklagemyndighed⁹.

2.4.2 Etablering af et midlertidigt militært område

Bevogtning på civilt område kan finde sted i forbindelse med etablering af et midlertidigt militært område, når det har til formål at forebygge og afværge fare for dansk og udenlandsk militært personel og materiel, der befinder sig uden for faste militære områder, jf. afsnit 2.2.

Medmindre særligt tungtvejende hensyn taler derfor, kan midlertidige militære områder alene oprettes i forbindelse med løsning af følgende opgaver:

1. ind- og udskibning af dansk eller udenlandsk militært personel og materiel fra civile havne, jernbaneterminaler og lufthavne,
2. ved besøg af udenlandske orlogsfartøjer i civile havne, hvis det skønnes fornødent at iagttage særlige sikkerhedsforanstaltninger,
3. ved oprettelse af sikkerhedszoner i forbindelse med ophold på jernbanenet og rastepladser m.v. ved transport af militært personel eller materiale,
4. ved oprettelse af sikkerhedszoner i forbindelse med midlertidig oprettelse af militært depot eller lejr,
5. ved oprettelse af sikkerhedszoner ved nedbrud eller lignende af militært materiel på civilt område, herunder også civil lufthavn.

Den stedlige politidirektørs skriftlige samtykke skal indhentes forud for etableringen af et hvert midlertidigt militært område. Ved hastende, uvarslede hændelser kan samtykket meddeles mundtligt.

Samtykket indhentes på baggrund af et oplæg, hvori der redegøres for den opgave, der tiltænkes løst med oprettelse af det midlertidige militære område, den geografiske afgrænsning af området samt det tidsmæssige behov for områdets opretholdelse, retningslinjer for varetagelse af sikkerhed og orden i området samt afmærkning. Politidirektøren kan anmode om yderligere oplysninger til brug for sin sagsbehandling.

Lodsejers accept skal foreligge, inden der indhentes samtykke fra den stedlige politidirektør. Ved hastende, uvarslede hændelser kan politidirektørens samtykke dog indhentes samtidig med indhentning af lodsejers samtykke¹⁰.

⁹ Jf. lovbekendtgørelse nr. 1284 af 14. november 2018, kapitel 93 b og 93 c.

¹⁰ Hvis lodsejers samtykke ikke kan indhentes, kan politiet med hjemmel i politilovens § 4, stk. 2, rydde og afspærre et område med henblik på at forebygge fare for forstyrrelse af den offentlige orden. Forsvaret kan i den forbindelse bistå politiet som beskrevet i punkt 2.4.1.

Så længe det midlertidige militære område er etableret, har det samme status som et fast militært område, og Forsvaret har ansvaret for at opretholde orden og sikkerhed på området. Som led heri kan der foretages ransagning efter militær retsplejelovs § 12, ligesom der kan foretages kontrol af indholdet af tøj, bagage, tasker m.v. og af transportmidler efter militær retsplejelovs § 13 uden retskendelse. Der henvises til punkt 3 i underbilag 1 til dette bilag.

Bevogtning af et midlertidigt militært område kan alene varetages af dansk militært personel, også selv om området anvendes af NATO/PfP-styrker¹¹.

2.4.3 Transporter

Forsvarets personel kan bevæbnet bevogte militære transportere, herunder også flytransporter, hvis der er saglige, sikkerhedsmæssige grunde til dette. Det vil primært kunne være tilfældet, hvor der er tale om transport af våben og ammunition eller af andet vitalt og/eller sensitivt materiel eller af dokumenter indeholdende sensitive oplysninger. Bevogtningen skal være passiv og må ikke under sin almindelige udførelse - udover eventuel påkrævet trafikregulering - medføre indgreb overfor civile, med mindre transporten udsættes for et angreb, tyveri- eller røveriforsøg. Bevogtningspersonellet skal ved standsning opholde sig i den umiddelbare nærhed af køretøjet m.v. For så vidt angår planlægning og udførelse henvises til afsnit 6.

2.4.4 Udrykning

Foretages bevogtning gennem udrykning - som en reaktion på en alarm - til en militær installation (fx et militært depot), kan der foretages undersøgelse af civilt terræn i umiddelbar nærhed af installationen, som fx udvendig inspektion af hegn, hvor dette ikke lader sig gøre inde fra det militære område. Der kan dog ikke medmindre betingelserne i punkt 2.4.1. eller 2.4.2. er opfyldt foretages afspærring eller udøves myndighed på civilt område.

2.4.5 Øvrig bevogtning på civilt område

Der kan undtagelsesvist foretages bevogtning af civile og militære objekter på civilt område, enten fordi den konkrete bevogtningsopgave er saglig i forhold til Forsvarets overordnede formål og opgaver, eller det følger af opståede nødrets-/nødværgemæssige omstændigheder som f.eks. havari, nød- eller sikkerhedslanding med Forsvarets fly m.v., og såfremt politiet ikke - evt. endnu - varetager opgaven. Bevogtning på civilt område skal foretages således, at den udgør det mindst mulige indgreb over for borgerne, hvilket kan sikres ved at indskrænke det bevogtede område omkring objektet så meget som muligt, herunder evt. med minestrimmel eller lignende. I tilfælde af sådanne opståede bevogtningsbehov kontaktes politiet altid hurtigst muligt med henblik på, at politiet kommer til stede og overtager bevogtningsopgaven, eller at der oprettes et midlertidigt militært område jf. ovenfor punkt 2.4.2.

3. ANSVAR, INSTRUKS OG UDDANNELSE

3.1 Ansvar

3.1.1. Den myndighed, som udfører bevogtning, og som har bevogtningspersonel under kommando (bevogtningsmyndigheden), er ansvarlig for, at bevogtningsleder og bevogtningspersonel er bekendt med deres opgaver og beføjelser som beskrevet i underbilag 1 til dette bilag.

3.1.2. Ved planlægning af bevogtningen skal bevogtningsmyndigheden sikre, at risikoen for personangreb samt ødelæggelse og tyveri af våben, ammunition og vitalt og/eller

¹¹ Dette gælder uanset NATO/PfP-statusoverenskomstens artikel VI, der tillader medlemmer af en fremmed styrke at besidde og bære våben i modtagerlandet i henhold til egne bestemmelser.

sensitivt materiel, herunder klassificerede informationer reduceres mest muligt, og således at eventuelle hændelser kan løses med mindst mulig anvendelse af magt.

3.1.3. Når Forsvaret yder bistand til politiet, jf. ovennævnte pkt. 2.4.1., foregår indsættelsen under politiets operative ledelse. Politiet instruerer Forsvarets personel om rammerne for opgavens løsning samt eventuel anvendelse af magt og brug af magtmidler.

3.2 Instruks

Bevogtningsmyndigheden skal udstede skriftlig instruks til bevogtningspersonellet, som udmønter relevante dele af dette bilags underbilag 1 og angiver konkrete forhold af relevans for bevogtningen på stedet¹². Skabeloner for "vagtens kort" er tilknyttet nævnte underbilag 1 som skabelon 1, 2 og 3. Ønsker bevogtningsmyndigheden at afvige fra de tilknyttede skabeloner til "vagtens kort" - udover det rent redaktionelle - skal det godkendes af den styrelse, som bevogtningsmyndigheden hører under.

3.3 Uddannelse

Bevogtningsmyndigheden er ansvarlig for, at bevogtningspersonellet modtager relevant uddannelse i magtanvendelse ved bevogtning. Det gælder både i konflikthåndtering og i korrekt håndtering af de magtmidler, personellet råder over.

4. BEVOGTNINGSSTYRKE

Bevogtning udføres med bevogtningsuddannet personel ansat ved koncernens styrelser, myndigheder og institutioner eller frivillige i Hjemmeværnet.

Alt personel, der deltager i bevogtning, skal være bevæbnet med skydevåben. Våbnet skal som udgangspunkt føres på personen under patruljering, ved indgriben over for konstaterede uregelmæssigheder samt ved ophold uden for vagtcentralen.

Når skydevåben føres på personen, skal det være ladet med patron i kammeret og sikret. Dette gælder dog ikke LMG M/62 og LMG M60E6, der føres sikret uden patron i kammeret.

5. LOKAL BEVOGTNING

5.1 Vagthavende

På de etableringer, hvor der i henhold til gældende bestemmelser befales en vagthavende, er denne uden for daglig tjenestetid chefens repræsentant på stedet og er som sådan overordnet for alt personel, der deltager i bevogtningstjenesten. Vagthavende skal, hvis tjenesten i øvrigt måtte tillade det, inspicere bevogtningstjenestens gennemførelse. Uregelmæssigheder, der konstateres af bevogtningsstyrken m.fl., skal straks meldes til vagthavende, der træffer beslutning om nødvendige foranstaltninger.

For så vidt angår den vagthavendes opgaver inden for bevogtningstjenesten kan en hjælper være befalet. Hjælperens betegnelse afhænger af værn og grad, men kan fx være vagtinspektør, vagtassistent eller inspektionshavende befalingsmand.

På etableringer, hvor en vagthavende ikke befales, varetages dennes opgaver for så vidt angår bevogtningstjenesten af en vagtinspektør/vagtassistent/inspektionshavende befalingsmand eller tilsvarende.

5.2 Tilsynshavende

Tilsynshavende med hjælpere ved indkvarterede enheder kan efter omstændighederne assistere ved bevogtningstjenestens udførelse.

¹² Se VFKPLAN OP 120-1 for nærmere information om, hvem der er bevogtningsmyndighed på de forskellige bevogtningstrin.

5.3 Lokale vagtcentraler (LVC)

Etablissementets tekniske sikrings-/overvågningsanlæg terminerer i en lokal vagtcentral, hvor den centrale betjening af bevogtningstjenestens kommunikationsmidler foretages.

En lokal vagtcentral har sit eget udpegede ansvarsområde, som ofte er defineret ved myndighedens perimeterhegn men det kan også omfatte områder og depoter mv. uden for perimeterhegnet.

Vagtkommandøren opholder sig normalt i vagtcentralen. Ved fravær skal en afløser fra bevogtningsstyrken udpeges. Vagtkommandøren skal umiddelbart kunne kontaktes over disponible kommunikationsmidler, således at han kan lede indgriben over for konstaterede uregelmæssigheder.

Vagthavende indsætter lokale indsatsstyrker (LIS).

Udover reaktion på alarmer kan bevogtningsstyrken varetage følgende funktioner:

- portnerfunktionen/adgangs- og udgangskontrol, jf. pkt. 5.5.,
- patruljering, herunder opholdskontrol jf. punkt 5.6. og
- indgriben overfor konstaterede uregelmæssigheder.

5.4 Lokal indsatsstyrke (LIS)

En lokal indsatsstyrke er et bevæbnet hold bestående af mindst 2 mand, der på instruks fra den lokale vagtcentral kan rykke ud til verificerede alarmer på og omkring etablermentet inden for den fastsatte reaktionstid. Indsatsstyrken er normalt en del af den lokale vagtcentralens bemanning.

5.5 Portnerfunktionen/adgangs- og udgangskontrol.

Adgangssøgende, der er i besiddelse af gyldigt adgangskort eller militært identitetskort, kan ved forevisning heraf passere til kontrolleret område ad hovedadgangsvejen, idet det dog i lokale bestemmelser kan fastsættes, at der skal være stikprøvevis kontrol. I henhold til skiltning ved indgangen til etablermentet skal adgangssøgende, der ikke er i besiddelse af gyldigt adgangskort/militært identitetskort, eller som ønsker at besøge sikrede områder, henvises til vagten, for dér at opnå tilladelse til at passere og få udleveret adgangskort/passerseddel.

Adgangssøgende vejledes i fornødent omfang i overensstemmelse med etablermentets sikkerhedsbestemmelser og blivende bestemmelser. Kørende trafik dirigeres ved trafiklys; gående enkeltpersoner henvises til passage forbi portnerloge eller tilsvarende kontrolsted.

Andre adgangsveje må normalt kun benyttes til tjenstlig trafik. Besøgende henvises ved skiltning til hovedadgangsvejen.

Uden for daglig arbejdstid lukkes/spærres alle adgangsveje, hvor dette er muligt. Al færdsel til og fra etablermentet kontrolleres. Kontrollens art afhænger af de passerendes mulighed for at få adgang til sikrede områder.

Passage ud fra et etablerment sker under iagttagelse af tilsvarende regler som for passage ind i etablermentet.

Militær retsplejelovs § 13 tillader vagter at foretage generel kontrol af indholdet af tøj, bagage, tasker m.v. og af transportmidler ved indgang til- og udgang fra – et militært område. Kontrollen udføres med henblik på at sikre, at der ikke ind- eller udføres genstande mv. i strid med interne forskrifter eller gældende lov i øvrigt. Kontrollen kan udføres mod

en bred personkreds eller som stikprøvekontrol. Det skal over for de besøgende ved skilting eller på anden måde tilkendegives, at der kan forekomme kontrol. Kontrollen kan iværksættes af den pågældende myndigheds chef og personel, der af denne er bemyndiget hertil, og den kan alene gennemføres af bevogtningsmyndighedens eget personel. Der henvises i øvrigt til nærværende bilags underbilag 1.

5.6 Patruljering.

Der udsendes periodisk patruljer som supplement til den øvrige fysiske sikkerhed (mekanisk sikring og elektronisk overvågning) for at konstatere og hindre,

- ulovligt ophold på området,
- ødelæggelse og hærværk,
- tyveri og indbrud,
- brand mv.

Patruljerne, der skal udrustes med radio, alarmerer øjeblikkeligt, når uregelmæssigheder konstateres, og imødegår om muligt sådanne.

Patruljer kan efter omstændighederne også udsendes til fjernt beliggende militære bygninger eller anlæg.

Patruljeringen tilrettelægges således, at intensiteten kan varieres under hensyn til områdernes sårbarhed og de tidsrum, hvor sandsynligheden for uregelmæssigheder er størst.

Hvor patruljen er udrustet med hund, tilrettelægges patruljeringen således, at hundens evner kan udnyttes maksimalt i forhold til vejrlig og terræn¹³.

6. BEVOGTNING AF MILITÆRE TRANSPORTER I CIVILT TERRÆN

6.1 Ansvar for planlægning mv.

Den for transporten ansvarlige chef skal sikre, at alle relevante informationer indgår i planlægningen og gennemførelsen af transporter af våben, ammunition og andet vitalt og/eller sensitivt materiel herunder klassificerede informationer, således at risikoen for tyveri og ødelæggelse reduceres mest muligt, og således at eventuelle situationer kan løses med mindst mulig anvendelse af magt.

Ved planlægningen af transporter skal der tages hensyn til kategoriseringen i bilag 1 til kapitel 3 (omfang af våben, ammunition og vitalt og/eller sensitivt materiel og klassificeret information, der kræver særlig sikkerhedsbeskyttelse). Transport af funktionsduelige våben (eller samtidig transport af alle dele heraf) eller ammunition skal generelt ske som fastsat i bestemmelserne for den militære sikkerhedstjeneste, jf. bilag 3 til kapitel 3.

Håndvåben transporteres så vidt muligt med vitale våbendele udtaget og opbevaret særskilt fra håndvåbnets hoveddel. Våben og tilhørende ammunition bør ligeledes søges opbevaret adskilt. Bevogtningspersonellet skal være bekendt med, hvilke dele af transporten der indeholder mere eller mindre vitalt og/eller sensitivt materiel.

På baggrund af en samlet vurdering af den generelle og konkrete trusselvurdering, transportens indhold (farlighed og mængde) og andre relevante forhold træffer den for transporten ansvarlige chef beslutning om behovet for bevogtning (eksempelvis om bevogtning

¹³ Anvendelse af bevogtningshunde og krav til egenskaber og uddannelse fremgår af RFLV 206-2-1 Bevogtningstjeneste i Flyvevåbnet og VFKBST F.667-1 Bestemmelser for Forsvarets hundetjeneste

kan gennemføres alene af det personel, der gennemfører selve transporten, eller om der er behov for tilgang af ledsagepersonel) samt hvilke magtmidler, der skal medbringes og autoriseres, herunder at magtmidlerne står mål med det, der beskyttes. Chefen skal endvidere vurdere, hvilke kommunikationsmidler der skal stilles til rådighed for eventuelt bevogtningspersonel og for transportens personel i øvrigt.

Chefen skal sikre, at bevogtningspersonellet har modtaget den påkrævede uddannelse og tilstrækkelige instrukser, herunder instruks vedrørende rammerne for magtanvendelse under den konkrete transport, jf. pkt. 3.2.

6.2 Koordination med politiet i forbindelse med transporter.

Politiet skal altid informeres om bevogtede, militære transporter i civilt terræn. Politiet informeres om den planlagte rute med henblik på koordination og for at sikre, at såvel bevogtningspersonel som de involverede politikredse er varslet og bedst muligt forberedt. Behovet for politieskorte og evt. supplerende forholdsregler drøftes i den forbindelse med politiet forud for transporten. Der kan bl.a. søges aftalt et direkte telefonnummer til vagthavende i politiet og til transportens personel/bevogtningspersonellet, således at der kan opnås hurtig forbindelse.

6.3 Udpegning og instruktion af bevogtningspersonel.

Anvendelse af skydevåben til beskyttelse af transporter på offentlig vej indebærer særlig fare for skade på udenforstående. Det er derfor vigtigt, at udpegningen af personel til bevogtning af transporter sker under nøje hensyntagen til den pågældendes viden, erfaring, træning og uddannelse.

Der skal forud for hver transport, normalt ved marchbefalingen, gives instruks vedrørende grænserne for magtanvendelse under den konkrete transport, herunder om skydevåben kun må benyttes i selvforsvar eller også til at hindre, at det bevogtede ødelægges/fjernes. Der skal udarbejdes vagtens kort til støtte for bevogtningspersonellets opgaveløsning, jf. dette bilags underbilag 1.

6.4 Tilkaldelse af politiet.

Politiet skal tilkaldes så hurtigt som muligt, hvis en militærtransport med våben, ammunition samt vitalt og/eller sensitivt materiel herunder klassificerede informationer bliver angrebet eller udsat for anden kriminell handling, eller hvis der er mistanke om, at dette vil ske. Såfremt det ikke er muligt at kontakte politiet, før et angreb indtræder, skal politiet tilkaldes snarest herefter. Forsvarets Auditørkorps orienteres efterfølgende om forholdet.

BEFØJELSER FOR DET I BEVOGTNINGSTJENESTEN INDSATTE PERSONEL**1. INDLEDNING**

I dette underbilag beskrives bevogtningspersonellets bevæbning og beføjelser.

2. BEVÆBNING

Alt personel, der deltager i bevogtning, skal være bevæbnet med skydevåben. Våbnet skal som udgangspunkt føres på personen under patruljering, ved indgriben over for konstaterede uregelmæssigheder samt ved ophold uden for vagtcentralen.

Når skydevåben føres på personen, skal det være ladet med patron i kammeret og sikret (gælder ikke LMG M/62 og LMG M60E6, der føres sikret uden patron i kammeret).

3. BEFØJELSER UNDER BEVOGTNING AF MILITÆRT OMRÅDE**3.1 Bevogtningspersonellets generelle beføjelser**

3.1.1. Bevogtningspersonellet er at anse som vagter og skal i forbindelse med bevogtningens udførelse adlydes og respekteres som overordnet i forhold til det øvrige personel¹. Det skal fremgå af lokale vagtbestemmelser og/eller vagtens kort, om bevogtningspersonellet har beføjelse til at udstede ordrer som led i varetagelsen af deres opgaver. Ordre, som bevogtningspersonellet udsteder, skal være sagligt begrundet i den opgave, de er sat til at varetage.

3.1.2. Bevogtningspersonellet kan overfor *alle* personer give påbud om, at ordens- eller sikkerhedsbestemmelser på området skal følges. Såfremt sådanne bestemmelser har været tydeligt bekendtgjort for de pågældende, f.eks. ved opslag ved indgangen til området eller ved vagtens tidligere mundtlige tilkendegivelser, kan bevogtningspersonellet ved overtrædelse bortvise personen fra området. Såfremt overtrædelsen af bestemmelserne tillige vurderes at udgøre et strafbart forhold, eksempelvis fordi militært personel undlader at efterkomme en tjenstlig ordre og dermed udviser grov ulydighed² eller ved ord eller handling i øvrigt udviser grov respektstridig opførsel³, således at anholdelse skønnes nødvendig af hensyn til disciplinen, kan bevogtningspersonellet foretage anholdelse i henhold til punkt 3.3.3.⁴

3.1.3. Ordens- eller sikkerhedsbestemmelser for området kan f.eks. indeholde regler for:

- hvor og hvornår man må opholde sig i et bestemt område,
- hvem der må opholde sig i området,
- hvilken adfærd der er tilladt (f.eks. fotografering, støj, alkoholindtagelse), og
- hvad personer på vagtens forlangende er forpligtet til at gøre, f.eks. at legitimere sig eller oplyse årsagen til sit ophold på området.

¹ Cirkulære nr. 9036 af 20.1.2006 (tjenestebestemmelser for Forsvarets militære og civile personel) fastlægger i § 3 en overordnet som den, der i henhold til bestemmelse eller ordre er bemyndiget til at udstede ordrer til andre inden for et nærmere fastsat tjenesteområde. Funktionen som vagt forudsætter bl.a., at pågældende er tillagt et særligt ansvar, og at der foreligger en konkret instruks eller ordre, jf. Betænkning 1435/2004, s. 260. Cirkulære 9036/2006 anvendes som fortolkningsbidrag i forhold til kvalifikationen af begrebet "overordnet" i militær retsplejelov § 10, jf. nedenfor note 4.

² Jf. militær straffelov nr. 530 af den 24.6.2005 § 11.

³ Jf. militær straffelov nr. 530 af den 24.6.2005 § 13.

⁴ I henhold til militær retsplejelov nr. 531 af den 24.6.2005 § 10, kan en overordnet anholde en underordnet, der udviser grov ulydighed eller groft respektstridig opførsel, hvis anholdelse skønnes nødvendig af hensyn til disciplinen.

3.1.4. En bortvisning, jf. punkt 3.1.2, fra militært område kan gennemføres under anvendelse af magt, såfremt vedkommende ikke frivilligt ønsker at forlade området. Vurderes det, at der ikke er blevet begået et strafbart forhold, vil der alene kunne anvendes håndkraft (uden våbenbrug) ved bortvisningen. Er der tale om en reaktion på en strafbar handling, kan magt i henhold til reglerne punkt 3.3.2 anvendes.

3.2 Kontrol ved indgang til og udgang fra militært område

3.2.1. Militær retsplejelovs § 13 tillader vagter uden retskendelse at foretage generel kontrol af indholdet af tøj, bagage, tasker m.v. og af transportmidler ved indgang til og udgang fra militært område. Kontrollen udføres ud fra et sikkerhedsmæssigt synspunkt med henblik på at sikre, at der ikke ind- eller udføres genstande mv. i strid med interne forskrifter eller gældende lov. Kontrollen kan udføres mod en bred personkreds eller som stikprøvekontrol.

3.2.2. Kontrollen kan omfatte enhver form for håndbagage, herunder tasker, mapper, rygsække, indkøbsposer etc. samt alle former for transportmidler, herunder navnlig motor-drevne køretøjer. Er bagagen låst, f.eks. en mappe eller taske, eller er bilen, herunder dens bagagerum, låst, kan det kræves, at den, der har rådighed over bagagen eller bilen, låser op, så kontrollen kan foretages. Undersøgelse af tøj og fodtøj bør ske ved, at vedkommende anmodes om selv at tømme sine lommer og aftage fodtøj, hvorefter vagten mærker efter uden på tøjet og undersøger fodtøjet indvendigt efter gemte genstande.

Klassificeret materiale, der medbringes i henhold til gyldigt kurércertifikat, må alene underkastes kontrol, hvis det efter omstændighederne skønnes nødvendigt og kuréren indvilliger heri. Hvis kuréren ikke vil tillade kontrol, skal han afvises. Ved kontrol med kurérens tilladelse, skal følgende iagttages,

- åbning af emballagen foretages af kuréren selv,
- emballagen åbnes et sted, hvor det ikke er synligt for uvedkommende,
- kontrollen gennemføres af ældste tilstedeværende og denne besejrer kun det klassificerede materiale i absolut nødvendigt omfang, og
- der gives kvittering for åbningen af materialet og oplysning om, hvilken person, der har foretaget eftersynet.

3.2.3. Militært personel er på grund af kommandoforholdet forpligtet til at deltage i kontrollen både ved indgang til og udgang fra området.

3.2.4. Civile er forpligtet til at deltage i kontrollen i forbindelse med udgang fra området. Ved indgang til området kan civile afvise at lade sig kontrollere. I givet fald kan vagten dog nægte dem adgang til området.

3.2.5. Såfremt personer, der er forpligtet til at deltage i kontrollen, nægter at medvirke til denne, kan vagten om nødvendigt tilbageholde genstande eller personer, og i yderste fald tvinge vedkommende til at tåle kontrollen. Vagten kan anvende den nødvendige magt for at gennemføre kontrollen og kan om nødvendigt anmode om politiets hjælp hertil. Tilbageholdelse må alene omfatte den genstand m.v., som skal undersøges, eller den person, hvis tøj skal undersøges. Tilbageholdelsen må ikke vare længere, end formålet med undersøgelsen tilsiger.

3.2.6. Vagten må kun tvinge nogen til at tåle kontrollen, hvis mindre indgribende foranstaltninger ikke er tilstrækkelige, og hvis indgrebet står i rimeligt forhold til formålet med indgrebet.

3.2.7. Kontrollen skal foretages så skånsomt, som omstændighederne tillader, herunder uden så vidt muligt at forårsage ødelæggelse eller beskadigelse.

3.2.8. Udførelse af adgangskontrol må ikke foretages overfor en person, såfremt der er en konkret mistanke om, at pågældende har begået et strafbart forhold, og såfremt formålet

med kontrollen er at tilvejebringe oplysninger om dette forhold⁵. Denne kompetence tilfalder Auditørkorpset eller politiet. Vagten vil dog kunne foretage en anholdelse, såfremt betingelserne under punkt 3.3.3 er opfyldt.

3.3 Beføjelser ved strafbart forhold

3.3.1 Strafbart forhold

3.3.1.1. Vagten kan skride ind overfor et umiddelbart forestående eller påbegyndt angreb på person, hvad enten det er vagten selv eller andre.

3.3.1.2. Vagten kan skride ind overfor et strafbart forhold rettet mod det eller de objekter, der beskyttes. Typiske forhold, der kan skrides ind overfor, kan være:

- **Ulovlig indtrængen:** Omfatter situationer, hvor en person uden tilladelse er trængt ind på afspærret område, eller hvor en person er trængt ind på ikke-afspærret, men ikke offentligt tilgængeligt område og ikke efter opfordring vil forlade dette.
- **Hærværk:** Omfatter ødelæggelse af ejendom. Om ødelæggelsen er omfattende eller om genstanden, der udsættes for hærværk, er af stor eller lille værdi, er uden betydning.
- **Tyveri:** Omfatter tyveri af genstande samt indbrud i bygninger eller køretøjer med henblik på at stjæle genstande af værdi. Om værdien er høj eller lav er uden betydning.
- **Spionage:** Omfatter tilegnelse af klassificerede oplysninger med henblik på overdragelse til fremmede stater eller organisationer. Det kan være svært at afgøre i situationen, om der er tale om spionage, idet det afhænger af gerningsmandens hensigt med at gøre sig bekendt med de klassificerede oplysninger. Indikationer, på at der er tale om spionage, kan f.eks. være ubegrundet ophold ved eller fotografering af hemmelige dokumenter/oplysninger/udstyr.

3.3.1.3. Vagten skal i sin vurdering af, om der er tale om et strafbart forhold, forholde sig til egne iagttagelser og viden om lokaliteter, trusler mv. Vagten må handle ud fra egen overbevisning i situationen. Ved tvivl, om hvorvidt forholdet er strafbart, må situationen undersøges nærmere.

3.3.2 Fælles betingelser for magtanvendelse ved indskriden overfor strafbart forhold

3.3.2.1. Vagten kan anvende magt, når der skrives ind for at stoppe eller forhindre et overhængende eller påbegyndt angreb/strafbart forhold.

Det vil sige, at vagten kan anvende magt i nødværge, når et angreb er igangværende (her standser vagten angrebet) samt i situationer, hvor angrebet endnu ikke er gået i gang, men er overhængende (her forhindrer vagten angrebet). Sidstnævnte betyder, at vagten kan skride ind, inden angrebet begynder. Det afgørende er, at vagten vurderer, at angrebet med sikkerhed rent faktisk vil indtræde, idet det ikke er tilstrækkeligt, at angrebet kun er en mulighed. Denne vurdering er vagtens, og der tillægges vagten et skøn i situationen.

Hvis et angreb er afsluttet, kan der kun ske magtanvendelse, hvis det er nødvendigt for at gennemføre anholdelse, (se nærmere punkt 3.3.3.), eller hvis dette sker i forlængelse af angrebet med henblik på at genvinde et retsgode, f.eks. tilbagetage frastjålne genstande.

3.3.2.2. Vagten må kun anvende den nødvendige magt.

Det betyder, at vagten kun må anvende det mindst indgribende magtmiddel, som er egnet til at stoppe hændelsen.

⁵ Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter (Retssikkerhedsloven) § 9, stk. 1.

3.3.2.3. Vagten må derudover kun anvende den magt, som vurderes forsvarlig. Når forsvarligheden af en magtanvendelse skal vurderes, skal truslen fra angrebet vurderes i forhold til den påtænkte anvendelse af magt. Der skal ved forsvarlighedsvurderingen navnlig lægges vægt på:

- Hvor farlig/ødelæggende er hændelsen? Jo større risiko, der er for personskade eller store materielle skader, desto mere magt må anvendes. Der må generelt altid anvendes mere magt overfor angreb på person end overfor angreb på materielle ting. Dødbringende magt må som altovervejende udgangspunkt kun anvendes mod livsfarlige angreb. Der henvises til reglerne for brug af skydevåben under punkt 3.3.4.11.
- Hvem er hændelsens person? Anvendelse af magt overfor børn, påvirkede eller sindsforvirrede personer skal søges begrænset.
- Hvad er hændelsens genstand? Jo større operative, sikkerhedsmæssige konsekvenser angrebet kan medføre, eller jo større betydning, det kan have for Forsvarets eller andre myndigheders samfundsvigtige opgaveløsning, jo mere magt må anvendes.

3.3.2.4. Vagten skal foretage en konkret vurdering af, hvad der udgør den nødvendige og forsvarlige magtanvendelse i den givne situation.

Det er vigtigt at vurdere både nødvendigheden og forsvarligheden af en modhandling, da begreberne ikke omfatter det samme. En konkret magtanvendelse kan være nødvendig uden samtidig at være forsvarlig og må derfor ikke anvendes. Det gælder især ved de mest indgribende magtmidler overfor mindre lovovertrædelser. Hvis eksempelvis et igangværende hærværk eller indbrud alene vil kunne stoppes under anvendelse af skydevåben, vil dette kunne ske i overensstemmelse med kravet om nødvendighed, men det vil aldrig være "forsvarligt" i nødværgereglens forstand. Det betyder, at der i princippet kan forekomme situationer, hvor det ikke vil være forsvarligt at afværge angrebet med det nødvendige magtmiddel, og hvor man derfor må opgive at standse lovovertrædelser. Dette forhindrer ikke, at der må foretages anholdelse, hvis betingelserne herfor er opfyldt.

3.3.3 Anholdelse

3.3.3.1. Såfremt en person træffes under eller i umiddelbar tilknytning til udøvelsen af et strafbart forhold, kan vagten anholde vedkommende⁶.

At anholdelse kun kan foretages, såfremt gerningsmanden træffes under eller i umiddelbar tilknytning til det strafbare forhold, betyder, at vagten skal have en høj grad af sikkerhed for at den, der anholdes, rent faktisk også har begået en strafbar handling. Dette vil f.eks. være tilfældet, såfremt gerningsmanden træffes på fersk gerning eller på vej væk fra et gerningssted. Kravet vil ikke være opfyldt, hvis vedkommende først træffes på et senere tidspunkt.

3.3.3.2. Anholdelse kan kun ske, hvis mindst en af følgende betingelser er opfyldt:

- det er nødvendigt at anholde vedkommende, for at forhindre vedkommende i at begå yderligere strafbare forhold, eller
- det er nødvendigt at anholde vedkommende, for at sikre at han forbliver på stedet, indtil politiet ankommer, eller
- det er nødvendigt at anholde vedkommende for at hindre hans samkvem med andre (f.eks. medgerningsmænd eller vidner).

Ovenstående betyder, at hvis en person indvilliger i at blive på stedet eller følge med frivilligt, er det ikke nødvendigt at anholde vedkommende.

3.3.3.3 Anholdelse må ikke foretages, hvis frihedsberøvelse efter sagens art eller omstændighederne i øvrigt vil være et uforholdsmæssigt indgreb.

⁶ Beføjelsen følger af retsplejelovens § 755, stk. 2, vedrørende privat anholdelse

Almindeligvis vil strafbare forhold som nævnt i punkt 3.3.1.1. og 3.3.1.2. opfylde kravet om forholdsmæssighed.

3.3.3.4. Den anholdte skal snarest muligt overgives til politiet med oplysning om tidspunktet og grundlaget for anholdelsen. Hvis den anholdte er militært ansat, skal denne i visse tilfælde overgives til Forsvarets Auditørkorps⁷. Er vagten i tvivl, overdrages den anholdte til politiet, og Forsvarets Auditørkorps orienteres om forholdet.

3.3.3.5. Unge under 15 år kan ikke ifalde straf og kan derfor heller ikke anholdes, men derimod tilbageholdes under samme betingelser som en anholdt. Ved en beslutning om tilbageholdelse skal den efterforskningsmæssige interesse i tilbageholdelsen afvejes over for de særlige hensyn, der skal tages på grund af den mindreåriges unge alder. Tilbageholdelse af mindreårige skal foretages så skånsomt og kortvarigt som muligt, men vil oftest kunne udstrækkes i det omfang, tungtvejende efterforskningsmæssige hensyn kræver det – f.eks. i forbindelse med sporsikring.

Tilbageholdelse kan f.eks. undlades, hvis den mindreårige frivilligt oplyser kontaktoplysninger eller på anden måde vil kunne identificeres efterfølgende.

3.3.3.6. En anholdelse kan om nødvendigt gennemføres ved brug af magt. Magtanvendelse vil kun være påkrævet i tilfælde, hvor den anholdte flygter eller ikke ønsker at forblive frivilligt på stedet.

Det er kun den nødvendige og forsvarlige magt, der kan anvendes for at anholde en person.

3.3.3.7. I forbindelse med anholdelsen kan der foretages sikkerhedsmæssig visitation af den pågældende (strygning og tryk). Den anholdte skal fratages genstande, som kan anvendes til vold, undvigelse eller som bevis, eller hvis genstanden er frataget nogen, der kan kræve den tilbage⁸.

Ud over den sikkerhedsmæssige visitation må civile ikke underkastes personlig ransagning, herunder undersøgelse af tøj, som den pågældende er iført. Militært personel må kun underkastes personlig ransagning, hvis den militære chef på tjenestestedet eller Forsvarets Auditørkorps i det konkrete tilfælde har givet sin bemyndigelse⁹.

Effekter, der er taget i forvaring, afleveres til den myndighed, der overtager sagens videre behandling (dvs. til politiet eller Forsvarets Auditørkorps). Indeholder effekterne klassificerede informationer, skal der gøres opmærksom herpå ved afleveringen, således at effekterne kan blive beskyttet og behandlet efter gældende bestemmelser.

Er den videre behandling overdraget til politiet, og indeholder effekterne klassificerede informationer, rettes der omgående henvendelse til Forsvarets Efterretningstjeneste.

Såfremt Forsvarets Auditørkorps beslutter, at en militær anholdt skal frigives, noteres tidspunktet og årsagen hertil. Den anholdtes identitet skal søges afklaret forud for frigivelsen. Dette kan ske ved almindelig udspørgning, notering af signalement, bevarelse af genstande med pågældendes fingeraftryk og/eller DNA, frivillig billedoptagelse mv. Enhver anholdelse og frigivelse skal rapporteres skriftligt.

⁷ Forsvarets Auditørkorps har påtalekompetencen i sager, hvor militært personel overtræder militær straffelov, den civile straffelov eller andre strafbelagte bestemmelser. I de to sidstnævnte tilfælde skal overtrædelsen dog vedrøre tjenesten eller være begået i anledning af tjenesten eller på militært område mv.

⁸ Jf. retsplejeloven § 807a, jf. § 802, stk. 1, nr. 2.

⁹ Bekendtgørelse nr. 1109 af 4. november 2005 om militære myndigheders adgang til at foretage uopsættelige efterforskningskridt i tilfælde, hvor auditørens afgørelse ikke kan indhentes.

3.3.4 Magtmidler

3.3.4.1. Vagten skal altid anvende det mindst indgribende magtmiddel til rådighed, som vurderes egnet til at stoppe hændelsen i overensstemmelse med de fælles betingelser for magtanvendelse beskrevet ovenfor under 3.3.2.

3.3.4.2. De enkelte magtmidler må kun anvendes af personel, der har modtaget den fornødne uddannelse i korrekt brug heraf og i håndtering af de skader, som de enkelte magtmidler vil kunne resultere i.

3.3.4.3. De enkelte magtmidler skal anvendes med besindighed og størst mulig skånsomhed.

3.3.4.4. Anvendelse af magtmidlet omfatter både den reelle anvendelse samt det at true med at anvende magtmidlet, advare om brugen samt i skydevåbens tilfælde at affyre varselsskud. Anvendes et skydevåben som slagvåben, falder det ikke ind under anvendelse af skydevåben, men af stav.

3.3.4.5. Talens brug (anråb). Anvendes til at give ordre/påbud om, at en bestemt adfærd skal ophøre og kan bruges uden begrænsninger. Trues der med anvendelse af et magtmiddel, f.eks. "stands eller jeg skyder", skal betingelserne for at bruge det pågældende magtmiddel være opfyldt.

3.3.4.6. Håndkraft. Magtanvendelse uden våben. Kan f.eks. være førergreb eller anden fysisk håndtering af en person. Håndkraft kan altid anvendes som magtmiddel, hvor talens brug ikke resulterer i, at vagtens lovlige påbud efterkommes. Graden af håndkraft skal være afpasset situationen og skal altid anvendes, så personen udsættes for mindst mulig skade eller fare herfor. I den forbindelse skal der udvises særlig forsigtighed med at fastholde personer i positioner, hvor der er risiko for kvælning eller hjertestop, som f.eks. liggende på maven med hænderne fikseret på ryggen.

3.3.4.7. Håndjern. Brug af håndjern, strips eller andet middel, som fikserer hænder eller fødder. Anvendes alene på anholdte/tilbageholdte personer, når der er risiko for vold, flugt eller selvbeskadigelse.

3.3.4.8. Peberspray. Peberspray anvendes til pacificering af en gerningsmand. Peberspray anvendes kun, indtil personen er under kontrol. Peberspray kan altid anvendes som magtmiddel, hvor mindre indgribende magtmidler (tale og håndkraft) ikke vurderes egnet, også selv om gerningsmanden ikke er bevæbnet. Forinden brug bør vagten så vidt muligt tilkendegive, at peberspray vil blive anvendt. Efter brug bør vagten sørge for øjenskyllning af den, der har været eksponeret for peberspray.

3.3.4.9. Stav. Stav må kun rettes mod arme, ben, ryg og sæde. Det bør i videst muligt omfang undgås at anvende staven mod knæ, albuer og andre led. Staven må ikke rettes mod hoved, hals, nakke, kraveben, bryst, mave, nyrer, skridt eller rygsøjle. Staven må ikke anvendes som stødvåben. Stav kan altid anvendes som magtmiddel, hvor mindre indgribende magtmidler (tale, håndkraft og peberspray) ikke vurderes egnet, også selv om gerningsmanden ikke er bevæbnet. Forinden brug bør vagten så vidt muligt tilkendegive, at han har til hensigt at anvende stav.

3.3.4.10. Hund. Hund kan alene anvendes som alternativ til skydevåben i overensstemmelse med retningslinjerne nedenfor pkt. 3.3.4.11. Forinden brug bør vagten så vidt det er muligt tilkendegive, at han har til hensigt til at anvende hunden.

3.3.4.11. Skydevåben. Skydevåben må kun anvendes, hvor andre magtmidler til rådighed ikke findes tilstrækkelige. Skydevåben må kun anvendes i følgende situationer:

- a) Ved farlige angreb på vagten selv eller andre. Et angreb er farligt, når det indebærer fare for liv eller førlighed, hvilket navnlig vil være tilfældet, hvor angriberen er bevæbnet med skyde-, stik- eller slagvåben.

- b) Ved anholdelse kun i de tilfælde, hvor der efter et angreb omfattet af a) er en overhængende risiko for, at den pågældende på ny vil foretage et farligt angreb på person.
- c) I forbindelse med et forsøg på ødelæggelse eller tilegnelse af materiel eller information, hvor bevogtningsmyndigheden har vurderet, at det kan have kritiske konsekvenser for Forsvarets operative opgaveløsning eller/og rigets sikkerhed, såfremt gerningsmanden lykkes med sit forehavende.

Hvilket materiel og hvilken information, der vil kunne føre til anvendelse af skydevåben i beskyttelsen heraf, skal vurderes i forbindelse med udfærdigelsen af hver enkelt vagtinstruks. Bevogtningsmyndigheden skal sikre, at sådant materiel og oplysninger er udpeget og identificeret, således at vagten har de oplysninger, der er nødvendige for, at denne kan vurdere evt. ødelæggelses- eller tilegnelsesforsøg på et kvalificeret grundlag.

Forsøg på at ødelægge eller tilegne sig håndvåben eller håndvåbenammunition kan ikke i sig selv føre til anvendelse af skydevåben mod gerningsmanden, med mindre situationen samtidigt er omfattet af pkt. a. eller b. ovenfor.

Er vagten i tvivl om, hvorvidt materiel eller oplysninger er udpeget og identificeret som beskyttet efter dette pkt. c, gælder en formodning imod, at dette er tilfældet.

Skud mod person skal afgives således, at skader søges begrænset til et minimum og således, at skuddene ikke udgør en risiko for andre. Er der nærliggende fare for, at udenforstående kan blive ramt, må skud kun afgives i yderste nødstilfælde. Før skud afgives, skal der så vidt muligt advares herom ved advarselsråb og dernæst ved varselsskud, som om muligt afgives i ufarlig retning.

3.3.4.12. Hvis en eller flere gerningsmænd kommer til skade ved vagtens anvendelse af magt, skal der ydes nødvendig førstehjælp, og ambulance skal om nødvendigt tilkaldes.

4. VAGTERS BEFØJELSER UNDER BEVOGTNING AF DE KONGELIGE SLOTTE

4.1. Forsvaret kan udføre bevogtning af de kongelige slotte og Rosenborg Slot som beskrevet i bilag 4, punkt 2.3.

4.2. Der kan anvendes magt i overensstemmelse med reglerne i punkt 3 med følgende undtagelser:

4.2.1. Vagten skal udføre adgangskontrol og afvise personer, der ikke har fornøden adgangsligitation og/eller lovligt ærinde. Vagten har ikke de øvrige beføjelser nævnt under punkt 3.2., idet disse specifikt er rettet mod militært område.

4.2.2. Skydevåben vil ikke kunne anvendes i henhold til punkt 3.3.4.11., litra c, idet det på forhånd vurderes, at der ikke på kongelige slotte og palæer findes militært materiel af en sådan operativ vigtighed, at anvendelse af skydevåben er berettiget.

5. VAGTERS BEFØJELSER VED BEVOGTNING SOM LED I FORSVARETS BISTAND TIL POLITIET

5.1. Vagtinstruks samt vagters magtbeføjelser som led i Forsvarets bistand til politiet udarbejdes af politiet til brug for den pågældende opgave. Der henvises i øvrigt til bilag 4, punkt 2.4.1. og 3.1.3.

6. VAGTERS BEFØJELSER UNDER BEVOGTNING AF MILITÆRE TRANSPORTER I CIVILT TERRÆN

6.1. Militære transportere i civilt terræn kan bevogtes som beskrevet i bilag 4, punkt 2.4.3.

6.2. Der kan anvendes magt i overensstemmelse med reglerne i punkt 3.3. med følgende undtagelse:

6.2.1. I det omfang transporter foregår i civilt terræn, må magt i selvforsvar kun anvendes, når angrebet ikke kan afværges på mindre indgribende måde, som f.eks. ved at køre væk.

6.3. Politiet skal altid informeres om den bevogtede transport og den planlagte rute med henblik på koordination og for at sikre, at såvel bevogtningspersonellet som de involverede politikredse er varslet og bedst muligt forberedt i forhold til evt. trusler. Behovet for politiskorte og evt. supplerende forholdsregler skal i den forbindelse drøftes med politiet forud for transporten.

6.4. Politiet skal tilkaldes så hurtigt som muligt, hvis en transport bliver angrebet eller udsat for anden kriminell handling, eller hvis der er mistanke om, at dette vil ske. Såfremt det ikke er muligt at kontakte politiet, før et angreb indtræder, skal politiet tilkaldes snarest herefter. Forsvarets Auditørkorps orienteres efterfølgende om forholdet.

7. VAGTERS BEFØJELSER UNDER BEVOGTNING I CIVILT OMRÅDE

7.1. Der kan udføres bevogtning i civilt område som beskrevet under punkt 2.3. og 2.4. i bilag 4.

7.2. Såfremt der foretages bevogtning på civilt område, skal denne tilstræbes gennemført, så borgere påvirkes mindst muligt.

7.3. Politiet skal kontaktes, når behovet for bevogtning opstår, og bevogtningsopgaven vil kun kunne opretholdes, indtil politiet ankommer og evt. overtager opgaven.

7.4. Vagten må bruge den nødvendige og forsvarlige magt til at hindre folk i at ødelægge eller borttage Forsvarets genstande. For at etablere et bevogtet område om genstandene, skal reglerne om midlertidige militære områder følges.

7.5. Magt kan anvendes i overensstemmelse med reglerne i punkt 3.3.

8. RAPPORTERING MV.

8.1. Enhver anvendelse af magt i henhold til dette underbilag skal rapporteres som en hændelse vedrørende fysisk sikkerhed, jf. FKOBST 358-1, kapitel 10, og VFKBST O.305-1.

8.2. Hurtigst muligt efter anvendelse af magt i henhold til punkt 3.3. skal politiet tilkaldes, og Forsvarets Auditørkorps orienteres om sagen. Hvor magt alene er anvendt over for militært personel, tilkaldes politiet ikke.

9. IKRAFTTRÆDELSE

De ved FKO skrivelse af 8. oktober 2010 udsendte "midlertidige retningslinjer for anvendelse af magt i forbindelse med bevogtning af våben- og ammunitionstransporter" ophæves.

Skabelon A

Skabelon for bevogtning af militære områder. Kun de dele, der er relevante for opgaven og i forhold til udleverede magtmidler, medtages. Der kan indlægges begrænsninger i magt-anvendelse i forhold til det angivne, men ikke udvidelser, medmindre dette er godkendt af den styrelse, som bevogtningsmyndigheden henhører under. Markerede klammer skal i nødvendigt omfang udfyldes.

VAGTENS KORT BEVOGTNING AF MILITÆRE OMRÅDER

1. Opgave

Du skal på [beskriv det militære område/bevogtningsområdet] forhindre eller stoppe personangreb og tyveri/ødelæggelse af militær ejendom. Du skal gennemføre adgangskontrol og sørge for, at kun folk med lovligt ærinde er på området.

2. Adgangskontrol

2.1. Du skal afvise personer, der ikke har adgangslegitimation eller lovligt ærinde.

2.2. Du kan foretage kontrol af indholdet af tøj, bagage, tasker mv. samt transportmidler ved indgangen til og udgangen fra militært område.

2.3. Militært personel er forpligtet til at deltage i kontrollen både ved indgang til og udgang fra området.

2.4. Civile er forpligtet til at deltage i kontrollen i forbindelse med udgang fra området. Ved indgang til området, kan civile afvise at lade sig kontrollere. I givet fald kan du nægte dem adgang til området.

2.5. Du skal foretage kontrollen så skånsomt som muligt og kan om nødvendigt tilbageholde genstande og personer.

3. Beføjelser ved overtrædelse af ordensforskrifter

3.1. Du kan overfor alle personer på området give påbud, om at ordens- eller sikkerhedsbestemmelser på det militære område skal følges og om at fremvise legitimation. Du kan bortvise personer, der ikke ønsker at efterleve påbuddet; om nødvendigt ved brug af håndkraft (uden brug af våben).

[**3.2.** Indskriv konkrete ordens-/sikkerhedsforskrifter, som gælder på området, og som det ønskes, at vagten skal håndhæve]

4. Beføjelser overfor strafbare forhold

Hvis du konstaterer strafbare forhold i form af vold, ulovlig indtrængen, hærværk, indbrud eller spionage på området, skal du reagere på følgende måde:

- Hvis tiden tillader det, skal du melde om forholdet og afvente ordre fra din overordnede.
- Hvis tiden ikke tillader indhentning af ordre, skal du skride ind og forsøge at stoppe det strafbare forhold. Du må bruge den magt, som er nødvendig for at stoppe handlingen, og som står mål med handlingens farlighed.
- Hvis du udsætter dig for fare ved at gribe ind, eller hvis det strafbare forhold ikke er personfarligt eller ikke er rettet mod særligt udpeget ejendom, er du alene forpligtet til at observere, så du kan bistå politiet ved den efterfølgende efterforskning. [Indsæt beskrivelse af evt. særligt udpeget ejendom]

5. Efterfølgende magtanvendelse

5.1. Du kan eftersætte og bruge den fornødne magt for at anholde en person, som træffes i forbindelse med udøvelsen af et strafbart forhold.

5.2. Du må bruge den magt, som er nødvendig for at foretage anholdelsen, og som står mål med vigtigheden af anholdelsen. Du må i den forbindelse fratage den anholdte genstande, som kan bruges til vold eller undvigelse eller som er tyvekoster.

6. Magtmidler

6.1. Du skal altid anvende det mindst indgribende magtmiddel, som er egnet til situationen.

6.2. Du skal altid anvende magtmidlet med besindighed og størst mulig skånsomhed.

6.3. Du kan anvende følgende magtmidler som beskrevet i eskalationsrækkefølgen med det mindst indgribende magtmiddel først og det mest indgribende til sidst:

Talens brug (anråb). Anvendes til at give ordre/påbud om, at en bestemt adfærd skal ophøre, og kan bruges uden begrænsninger, idet der dog ikke må trues med anvendelse af magtmidler, som ikke vil være lovlige at anvende.

Peberspray. Kan anvendes i alle situationer. Peberspray anvendes til pacificering af en gerningsmand og anvendes kun, indtil personen er under kontrol. Forinden brug skal du om muligt advare om, at du har til hensigt at anvende peberspray.

Håndkraft (førergreb og lignende). Kan anvendes i alle situationer. Graden af håndkraft skal være afpasset situationen og skal altid anvendes, så den angribende udsættes for mindst mulig skade eller fare. I den forbindelse skal du særligt udvise forsigtighed med at fastholde personer i positioner, hvor der er risiko for kvælning eller hjertestop

Håndjern. Anvendes alene ved risiko for vold, flugt eller selvmord.

Stav. Kan anvendes i alle situationer. Du må kun rette stav mod arme, ben, ryg og sæde. Du bør i videst muligt omfang undgå at anvende staven mod knæ, albuer og andre led. Staven må ikke rettes mod hoved, hals, nakke, kraveben, bryst, mave, nyrer, skridt eller rygsøjle. Forinden brug skal du om muligt advare om, at du har til hensigt at anvende stav.

Hund. Hund kan alene anvendes som alternativ til skydevåben i overensstemmelse med retningslinjerne for anvendelse af skydevåben. Forinden brug skal du om muligt advare om, at du har til hensigt at anvende hund.

Skydevåben. Du må kun anvende skydevåben i følgende situationer:

Ved angreb på person: Ved farligt angreb på dig selv eller andre. Farligt angreb betyder i denne sammenhæng, at der skal være fare for liv eller alvorlig helbredsskade.

Ved anholdelse: Når du skal anholde en person, der har gennemført et personfarligt angreb, og der er overhængende risiko for, at personen udfører endnu et personfarligt angreb.

[Ved angreb på ejendom: Du må kun anvende skydevåben ved et angreb på følgende på forhånd udpeget ejendom: *[her indsættes den på forhånd udpegede og af bevogtningsmyndigheden godkendte ejendom på tjenestestedet, hvor det vurderes, at et angreb kan have kritiske konsekvenser for den operative opgaveløsning og/eller rigets forsvar]*].

Du skal om muligt følge følgende eskalationstrin ved brug af skydevåben:

- 1) Afgive advarsel om brug af skydevåben
- 2) Afgive advarsel og indtage skydestilling
- 3) Afgive varselsskud
- 4) Afgive sigtet skud

Skud mod person skal afgives således, at følgeskader søges begrænset til et minimum, og således at skuddene ikke udgør en risiko for andre. Er der nærliggende risiko for at udenforstående kan blive ramt, må skud kun afgives i yderste nødstilfælde.

7. Meldepligt

Du skal straks melde til din overordnede, og politiet skal hurtigst muligt kontaktes, hvis du har anvendt magt, eller hvis du har konstateret et strafbart forhold på området. Forsvarets Auditørkorps orienteres efterfølgende om forholdet.

Skabelon B

Skabelon for bevogtning af kongelige slotte og palæer samt Rosenborg Slot. Kun de dele, der er *relevante for opgaven og i forhold til udleverede magtmidler, medtages. Der kan indlægges begrænsninger i magtanvendelse i forhold til det angivne, men ikke udvidelser, medmindre dette er godkendt af Forsvarskommandoen. Markerede klammer skal i nødvendigt omfang udfyldes.*

VAGTENS KORT BEVOGTNING AF KONGELIGE SLOTTE

1. Opgave

Du skal forhindre eller stoppe personangreb og tyveri fra eller ødelæggelse på *[beskriv bevogtningsområdet]*. Du skal gennemføre adgangskontrol og sørge for, at kun folk med lovligt ærinde er på området.

2. Adgangskontrol

Du skal afvise personer, der ikke har ID-kort eller lovligt ærinde.

3. Beføjelser ved overtrædelse af ordensforskrifter

3.1. Du kan overfor alle personer på området give påbud, om at ordens- eller sikkerhedsbestemmelser på *[angiv område]* skal følges og om at fremvise legitimation. Du kan bortvise personer, der ikke ønsker at efterleve påbuddene om nødvendigt ved brug af håndkraft (uden brug af våben).

[3.2. Indskriv konkrete ordens-/sikkerheds forskrifter, som gælder på området, og som ønskes, at vagten skal håndhæve]

4. Beføjelser overfor strafbare forhold

Hvis du konstaterer strafbare forhold i form af vold, ulovlig indtrængen, hærværk, tyveri eller spionage på området, skal du reagere på følgende måde:

- Hvis tiden tillader det, skal du melde om forholdet og afvente ordre fra din overordnede.
- Hvis tiden ikke tillader det, skal du skride ind, og forsøge at stoppe det strafbare forhold. Du må bruge den magt, som er nødvendig for at stoppe det strafbare forhold, og som står mål med angrebets farlighed.
- Hvis du udsætter dig for fare ved at gribe ind, eller hvis det strafbare forhold ikke er personfarligt, er du alene forpligtet til at observere, så du kan bistå politiet ved den efterfølgende efterforskning.

5. Efterfølgende magtanvendelse

5.1. Du kan eftersætte og bruge den fornødne magt for at anholde en person, som træffes i forbindelse med udøvelsen af et strafbart forhold.

5.2. Du må bruge den magt, som er nødvendig for at foretage anholdelsen, og som står mål med vigtigheden af anholdelsen. Du må i den forbindelse fratage den anholdte stjålne genstande samt genstande, som kan bruges til vold eller undvigelse.

6. Magtmidler

6.1. Du skal altid anvende det mindst indgribende magtmiddel, som er egnet til situationen.

6.2. Du skal altid anvende magtmidlet med besindighed og størst mulig skånsomhed.

6.3. Du kan anvende følgende magtmidler som beskrevet i eskalationsrækkefølgen med det mindst indgribende magtmiddel først og det mest indgribende til sidst:

Talens brug (anråb). Anvendes til at give ordre/påbud om, at en bestemt adfærd skal ophøre, og kan bruges uden begrænsninger, idet der dog ikke må trues med anvendelse af magtmidler, som ikke vil være lovlige at anvende.

Håndkraft (førergreb og lignende). Kan anvendes i alle situationer. Graden af håndkraft skal være afpasset situationen og skal altid anvendes, så den angribende udsættes for mindst mulig skade eller fare. I den forbindelse skal du særligt udvise forsigtighed med at fastholde personer i positioner, hvor der er risiko for kvælning eller hjertestop.

Skydevåben. Du må kun anvende skydevåben i følgende situationer:

Ved angreb på person: Ved farlige angreb på dig selv eller andre. Farligt angreb betyder i denne sammenhæng, at der skal være fare for liv eller alvorlig helbredsskade.

Ved anholdelse: Når du skal anholde en person, der har gennemført et personfarligt angreb, og der er overhængende risiko for, at personen udfører endnu et personfarligt angreb.

Du skal om muligt følge følgende eskalationstrin ved brug af skydevåben:

- 1) Afgive advarsel om brug af skydevåben
- 2) Afgive advarsel og indtage skydestilling
- 3) Afgive varselsskud
- 4) Afgive sigtet skud

Skud mod person skal afgives således, at følgeskader søges begrænset til et minimum, og således at skuddene ikke udgør en risiko for andre. Er der nærliggende risiko for, at udenforstående kan blive ramt, må skud kun afgives i yderste nødstilfælde.

7. Meldepligt

Du skal straks melde til din overordnede, og politiet skal hurtigst muligt kontaktes, hvis du har anvendt magt, eller hvis du har konstateret et strafbart forhold på området. Forsvarets Auditørkorps orienteres efterfølgende om forholdet.

Skabelon C

Skabelon for bevogtning af transport. Kun de dele, der er relevante for opgaven og i forhold til udleverede magtmidler, medtages. Der kan indlægges begrænsninger i magtanvendelse i forhold til det angivne, men ikke udvidelser, medmindre dette er godkendt af den styrelse, som bevogtningsmyndigheden henhører under. Markerede klammer skal i nødvendigt omfang udfyldes.

VAGTENS KORT BEVOGTNING AF TRANSPORTER

1. Opgave

Du skal under transport af *[beskriv transportopgaven]* forhindre eller stoppe personangreb, røveri, tyveri eller hærværk rettet mod transporten.

2. Beføjelser overfor strafbare forhold

Hvis du konstaterer strafbare forhold i form af vold, røveri, tyveri eller hærværk mod transporten, skal du reagere på følgende måde:

- Hvis tiden tillader det, skal du melde om forholdet og afvente ordre fra din overordnede.
- Hvis tiden ikke tillader det, skal du skride ind, men du skal så vidt muligt forsøge at afværge angrebet passivt, f.eks. ved at køre væk. Kun hvis dette ikke er muligt, skal du forsøge at stoppe angrebet ved en aktiv indskriden.
- Du må bruge den magt, som er nødvendig for at stoppe angrebet, og som står mål med angrebets farlighed.
- Hvis du udsætter dig for fare ved at gribe ind, eller hvis angrebet ikke er personfarligt eller ikke er rettet mod særligt udpeget gods/dokumenter, er du alene forpligtet til at observere, så du kan bistå politiet ved den efterfølgende efterforskning. *[Indsæt beskrivelse af evt. særligt udpeget gods/dokumenter]*

3. Efterfølgende magtanvendelse

3.1. Du kan eftersætte og anholde en person, som træffes i forbindelse med udøvelsen af et strafbart forhold.

3.2. Du må bruge den magt, som er nødvendig for at foretage anholdelsen, og som står mål med vigtigheden af anholdelsen. Du må i den forbindelse fratage den anholdte stjålne genstande samt genstande, som kan bruges til vold eller undvigelse.

4. Magtmidler

4.1. Du skal altid anvende det mindst indgribende magtmiddel, som er egnet til situationen.

4.2. Du skal altid anvende magtmidlet med besindighed og størst mulig skånsomhed.

4.3. Du kan anvende følgende magtmidler som beskrevet i eskalationsrækkefølgen med det mindst indgribende magtmiddel først og det mest indgribende til sidst *[kun magtmidler, der er udleveret, medtages]*:

Talens brug (anråb). Anvendes til at give ordre/påbud om, at en bestemt adfærd skal ophøre, og kan bruges uden begrænsninger, idet der dog ikke må trues med anvendelse af magtmidler, som ikke vil være lovlige at anvende.

Håndkraft (førergreb og lignende). Kan anvendes i alle situationer. Graden af håndkraft skal være afpasset situationen og skal altid anvendes, så den angribende udsættes for

mindst mulig skade eller fare. I den forbindelse skal du særligt udvise forsigtighed med at fastholde personer i positioner, hvor der er risiko for kvælning eller hjertestop

[Håndjern. Anvendes alene ved risiko for vold, flugt eller selvmord.]

[Peberspray. Kan anvendes i alle situationer. Peberspray anvendes til pacificering af en gerningsmand og anvendes kun, indtil personen er under kontrol. Forinden brug skal du om muligt advare om, at du har til hensigt at anvende peberspray]

[Stav. Kan anvendes i alle situationer. Du må kun rette stav mod arme, ben, ryg og sæde. Du bør i videst muligt omfang undgå at anvende staven mod knæ, albuer og andre led. Staven må ikke rettes mod hoved, hals, nakke, kraveben, bryst, mave, nyrer, skridt eller rygsøjle. Forinden brug skal du om muligt advare om, at du har til hensigt at anvende stav.]

[Hund. Hund kan alene anvendes som alternativ til skydevåben i overensstemmelse med retningslinjerne for skydevåben. Forinden brug skal du om muligt advare om, at du har til hensigt at anvende hund.

Skydevåben. Du må kun anvende skydevåben i følgende situationer:

Ved angreb på person: Ved farlige angreb på dig selv eller andre. Farligt angreb betyder i denne sammenhæng, at der skal være risiko for liv eller alvorlig helbredsskade.

Ved anholdelse: For at anholde en person, der har gennemført et personfarligt angreb og er på vej til at gøre det igen.

[Ved angreb på forsvarets ejendom: Du må kun anvende skydevåben ved et angreb på følgende på forhånd udpeget gods: *[her indsættes den på forhånd udpegede og det af styrelse/kommando/region godkendte transportgods, hvor det vurderes, at et angreb kan have kritiske konsekvenser for Forsvarets operative opgaveløsning]*.

Du skal om muligt følge følgende eskalationstrin ved brug af skydevåben:

- 1) Afgive advarsel om brug af skydevåben
- 2) Afgive advarsel og indtage skydestilling
- 3) Afgive varselsskud
- 4) Afgive sigtet skud

Skud mod person skal afgives således, at følgeskader søges begrænset til et minimum, og således at skuddene ikke udgør en risiko for andre. Er der nærliggende risiko for, at udenforstående kan blive ramt, må skud kun afgives i yderste nødstilfælde.

5. Meldepligt

Du skal straks melde til din overordnede, og politiet skal hurtigst muligt kontaktes, hvis du har anvendt magt, eller hvis du har konstateret et strafbart forhold på området. Forsvarets Auditørkorps orienteres efterfølgende om forholdet.

UDDRAG AF STRAFFELOVEN

§ 13. Handlinger foretagne i nødværge er straffri, for så vidt de har været nødvendige for at modstå eller afværge et påbegyndt eller overhængende uretmæssigt angreb og ikke åbenbart går ud over, hvad der under hensyn til angrebets farlighed, angriberens person og det angrebne retsgodes betydning er forsvarligt.

Stk. 2. Overskrider nogen grænserne for lovligt nødværge, bliver han dog straffri, hvis overskridelsen er rimeligt begrundet i den ved angrebet fremkaldte skræk eller ophidselse.

Stk. 3. Tilsvarende regler finder anvendelse på handlinger, som er nødvendige for på retmæssig måde at skaffe lovlige påbud adlydt, iværksætte en lovlig pågribelse eller hindre en fanges eller tvangsanbragt persons rømning.

§ 107. Den, som i fremmed magts eller organisations tjeneste eller til brug for personer, der virker i sådan tjeneste, udforsker eller giver meddelelse om forhold, som af hensyn til danske stats- eller samfundsinteresser skal holdes hemmelige, straffes, hvad enten meddelelsen er rigtig eller ej, for spionage med fængsel indtil 16 år.

Stk. 2. Såfremt det drejer sig om de i § 109 nævnte forhold, eller handlingen finder sted under krig eller besættelse, kan straffen stige indtil fængsel på livstid.

§ 108. Den, som uden at forholdet falder ind under § 107, i øvrigt foretager noget, hvorved fremmed efterretningsvæsen sættes i stand til eller hjælpes til umiddelbart eller middelbart at virke indenfor den danske stats område, straffes med fængsel indtil 6 år.

Stk. 2. Såfremt det drejer sig om efterretninger vedrørende militære anliggender, eller virksomheden finder sted under krig eller besættelse, kan straffen stige indtil fængsel i 12 år.

§ 109. Den, som røber eller videregiver meddelelse om statens hemmelige underhandlinger, rådslagninger eller beslutninger i sager, hvorpå statens sikkerhed eller rettigheder i forhold til fremmede stater beror, eller som angår betydelige samfundsøkonomiske interesser overfor udlandet, straffes med fængsel indtil 12 år.

Stk. 2. Foretages de nævnte handlinger uagtsomt, er straffen fængsel indtil 3 år eller under formildende omstændigheder bøde.

§ 110. Den, som forfalsker, ødelægger eller bortskaffer noget dokument eller anden genstand, der er af betydning for statens sikkerhed eller rettigheder i forhold til fremmede stater, straffes med fængsel indtil 16 år.

Stk. 2. Foretages de nævnte handlinger uagtsomt, er straffen fængsel indtil 3 år eller under formildende omstændigheder bøde.

§ 110 a. Med bøde eller fængsel indtil 3 år straffes den, som forsætligt eller uagtsomt uden behørig tilladelse

1. beskriver, fotograferer eller på anden måde afbilder danske ikke almentilgængelige militære forsvarsanlæg, depoter, enheder, våben, materiel el.lign., eller som mangfoldiggør eller offentliggør sådanne beskrivelser eller afbildninger,
2. offentliggør bestemmelser, der vedrører danske stridskræfters mobilisering og andet krigsberedskab.

Stk. 2. Med bøde straffes den, som forsætligt eller uagtsomt uden behørig tilladelse optager fotografier fra luftfartøj over dansk statsområde eller offentliggør sådanne ulovligt optagne fotografier.

§ 119. Den, som øver vold, truer med at øve vold eller offentligt eller med forsæt til udbredelse i en videre kreds fremsætter trussel om vold mod nogen, hvem det påhviler at handle i medfør af offentlig tjeneste eller hverv, under udførelsen af tjenesten eller hvervet eller i anledning af samme, eller som på lige måde søger at hindre en sådan person i at foretage en lovlig tjenestehandling eller at tvinge ham til at foretage en tjenestehandling, straffes med bøde eller fængsel indtil 8 år. Ved fastsættelse af straffen skal det indgå som en skærpende omstændighed, at forholdet er begået, mens eller i umiddelbar forlængelse af at der i området foregår grov forstyrrelse af ro og orden på offentligt sted, eller at forholdet er begået mod den pågældende i dennes fritid.

Stk. 2. På samme måde straffes den, som, uden at forholdet falder ind under stk. 1, fremsætter trusler om vold, om frihedsberøvelse eller om sigtelse for strafbart eller ærerørigt forhold mod nogen, der af det offentlige er tillagt domsmyndighed eller myndighed til at træffe afgørelse vedrørende retsforhold eller vedrørende håndhævelse af statens straffemyndighed, i anledning af udførelsen af tjenesten eller hvervet, eller som på lige måde søger at hindre en sådan person i at foretage en lovlig tjenestehandling eller at tvinge ham til at foretage en tjenestehandling.

Stk. 3. Lægger nogen ellers de nævnte personer hindringer i vejen for udførelsen af deres tjeneste eller hverv, straffes han med bøde eller fængsel indtil 1 år og 6 måneder. Ved fastsættelse af straffen skal det indgå som en skærpende omstændighed, at forholdet er begået, mens eller i umiddelbar forlængelse af at der i området foregår grov forstyrrelse af ro og orden på offentligt sted

§ 121. Den, som med hån, skældsord eller anden fornærmelig tiltale overfalder nogen af de i § 119 nævnte personer under udførelsen af hans tjeneste eller hverv eller i anledning af samme, straffes med bøde eller fængsel indtil 1 år.

BESTEMMELSER FOR ADGANGS-, OPHOLDS- OG UDGANGSKONTROL

Underbilag:

1. Tekniske krav til elektroniske adgangskontrolanlæg for sikrede områder.
2. Bestemmelser vedrørende fotografering.

1. ETABLISSEMENTETS BRUGSMØNSTER

I de sikringsmæssige overvejelser omkring koncernens bygningers brugsmønster er adgangskontrollen et væsentligt led i planlægning og udførelse af de samlede sikringsløsninger.

Typisk vil der være tale om flere personkategorier, som på forskellige tidspunkter skal have adgang til og ophold i forskellige områder og lokaliteter.

Som eksempler på personkategorier med behov for adgang til koncernens styrelser, stabe og myndigheder anføres følgende:

- Tjenstgørende militært og civilt personel,
- frivillige i Hjemmeværnet i fm. uddannelse, øvelser, tjeneste m.v.,
- rådighedspersonel i fm. uddannelse, øvelser, indkommandering mv.,
- traditionsbærende foreninger og klubber,
- leverandører,
- kunder,
- besøgende,
- pressefolk,
- offentlige kontrolmyndigheder,
- offentlige og civile servicemyndigheder,
- konsulenter
- håndværkere,
- rengøringspersonale, og
- vagtpersonale.

Personer, der ikke kan henføres til ovennævnte kategorier, er generelt uvedkommende på koncernens etableringer.

Til hver af disse personkategorier kan der gives adgangstilladelse til områder under hensyntagen til styrelsens, stabens eller myndighedens mønster for så vidt angår den daglige tjeneste.

Besøgskort skal udleveres ved adgangskontrollen og skal afleveres ved udgang.

For så vidt angår ledsagelse af konsulenter, besøgende, håndværkere og rengøringspersonale i områder, der kræver ledsagelse, er det adgangsberettigede personer fra myndigheden, der dagligt arbejder i pågældende områder, der skal ledsage de besøgende, håndværkere eller rengøringspersonale henset til kendskab til områdets sikkerhedsmæssige karakteristika. Varsling om opgaven og behov for ledsagelse skal ske så betids, at gennemførelse af ledsageopgaven kan ske med rimelig planlægningshorisont. Ved større projekter, f.eks. ombygninger, nybyggeri mv. bør det som udgangspunkt være koncernens projektleverandør, der varetager ledsageopgaven, efter koordination med myndighedschefen eller garnisonskommandanten.

Såfremt der undtagelsesvis af chefen for myndigheden eller dennes sikkerhedsofficer gives tilladelse til uledsaget adgang til sikret område, kategori 2, bør det defineres, hvilket kon-

kret område ved myndigheden, som der er givet tilladelse til at arbejde og opholde sig uledsaget i. Endvidere bør det fastlægges, om den undtagelsesvisse tilladelse til uledsaget adgang tillige omfatter færdsel fra vagtområdet og videre til og fra det definerede arbejds- og opholdsområde, eller om dette skal ske ledsaget

2. ADGANGSKONTROL OG ADGANGSBERETTIGEDE

2.1 Sikret område

2.1.1 Kategori 1 område

Til kategori 1 områder kan chefen for myndigheden eller sikkerhedsofficeren bemyndige fast tjenstgørende personel uledsaget adgang i området. Fast tjenstgørende personel defineres her som personer, der er ansat i koncernen og dagligt arbejder i det sikrede kategori 1 område. De pågældende skal være sikkerhedsgodkendt til det rette niveau. For kategori 1 område, sikringsniveau 50-60 er det HEMMELIGT/YDERST HEMMELIGT.

Øvrige personer har ikke adgang uden konstant ledsagelse af en adgangsberettiget person.

I efterfølgende skema er anført, hvem der, efter bemyndigelse fra chefen for myndigheden eller sikkerhedsofficeren, kan have uledsaget adgang til et kategori 1 område, sikringsniveau 50-60.

Fast personel ved myndigheden				
Områdekategorier ved myndigheden	YHM/HEM-godkendt ved myndighedsområdet. (Fast tjenstgørende i rummet/cellen/arkivet)	HEM-godkendt ved myndigheden	FTR-godkendt ved myndigheden	TTJ-godkendt ved myndigheden
Områdekategori 1, sikringsniveau 50-60	Ja	Nej	Nej	Nej

Fast personel i koncernen			
Områdekategorier ved myndigheden	YHM/HEM-godkendt i koncernen	FTR-godkendt i koncernen	TTJ-godkendt i koncernen
Områdekategori 1, sikringsniveau 50-60	Nej	Nej	Nej

Konsulenter, håndværkere og rengøringspersonale				
Områdekategorier ved myndigheden	HEM-godkendt	FTR-godkendt	TTJ-godkendt	Ikke-godkendt
Områdekategori 1, sikringsniveau 50-60	Nej	Nej	Nej	Nej

Adgangskontrol skal foregå ved indsats af personel eller anvendelse af automatiske adgangskontrolanlæg.

2.1.2 Kategori 2 område

Til kategori 2 områder kan chefen for myndigheden eller sikkerhedsofficeren bemyndige tjenstgørende personel uledsaget adgang i området. Tjenstgørende personel betyder i denne sammenhæng personer, der er ansat i koncernen. De pågældende skal være sikkerhedsgodkendt til det rette niveau. For kategori 2 område, sikringsområde 30-40 er det HEMMELIGT.

Personer, der forretter tjeneste ved myndigheden/etablissementet og er sikkerhedsgodkendt til FORTROLIGT, kan, efter bemyndigelse fra chefen for myndigheden eller sikkerhedsofficeren, meddeles uledsaget adgang i kategori 2 området. Det skal i denne forbindelse sikres, at der ikke gives mulighed for indsigt i HEM sager.

Øvrige personer har, som udgangspunkt, ikke adgang uden at være under opsyn (ledsaget) af en adgangsberettiget person.

Chefen for myndigheden eller sikkerhedsofficeren kan dog undtagelsesvis tillade, at konsulenter, håndværkere og rengøringspersonale kan arbejde uden ledsagelse, såfremt det er nødvendigt og anses for sikkerhedsmæssigt forsvarligt. De skal dog være sikkerhedsgodkendt til det sikkerhedsniveau, som de utilsigtet kan komme til at få indblik i. Med henblik på at sikre dokumentation for en sådan tilladelse skal beslutningen, inkl. sikkerhedsmæssig vurdering og begrundelse, herom føres i risikologgen.

I efterfølgende skema er anført, hvem der, efter bemyndigelse fra chefen for myndigheden eller sikkerhedsofficeren, kan have uledsaget adgang til et kategori 2 område, sikringsniveau 30-40:

Fast personel ved myndigheden				
Områdekategorier ved myndigheden	YHM/HEM-godkendt ved myndighedsområdet. (Fast tjenstgørende i rummet/cellen/arkivet)	HEM-godkendt ved myndigheden	FTR-godkendt ved myndigheden	TTJ-godkendt ved myndigheden
Områdekategori 2, sikringsniveau 30-40	Ja	Ja	Ja, men der må ikke gives indsigt i HEM sager	Nej

Fast personel i koncernen			
Områdekategorier ved myndigheden	YHM/HEM-godkendt i koncernen	FTR-godkendt i koncernen	TTJ-godkendt i koncernen
Områdekategori 2, sikringsniveau 30-40	1	Nej	Nej
1: Efter en generel bemyndigelse fra myndighedens chef eller sikkerhedsofficer. Når først adgang er givet, kan man bevæge sig rundt uledsaget i det anviste arbejdsområde			

Konsulenter, håndværkere og rengøringspersonale				
Områdekategorier ved myndigheden	HEM-godkendt	FTR-godkendt	TTJ-godkendt	Ikke-godkendt
Områdekategori 2, sikringsniveau 30-40	2	Nej	Nej	Nej
2: Bør altid være ledsaget. Såfremt det undtagelsesvis er nødvendigt og anses for sikkerhedsmæssigt forsvarligt, kan myndighedenschefen eller dennes sikkerhedsofficer lade de pågældende arbejde uden ledsagelse. De skal dog være godkendt til det sikkerhedsniveau, som de utilsigtet kan komme til at få indblik i. I sikret område, kategori 2, sikringsniveau 30/40 er det HEM. En tilladelse til uledsaget adgang skal dokumenteres i risikologgen.				

Adgangskontrol skal foregå ved indsats af personel eller anvendelse af automatisk adgangskontrolanlæg.

2.2 Kontrolleret område

2.2.1 Kategori 3 område

Til kategori 3 områder etableres normalt adgangskontrol for at kontrollere eller overvåge ind passage af personer og køretøjer.

Adgangsberettigede er personel med koncernens identitetskort eller adgangskort til etablissementet.

Efter garnisonskommandantens, chefen for myndigheden eller dennes sikkerhedsofficers bestemmelse, jf. skema nedenfor, skal øvrige personer have udstedt midlertidigt adgangskort til etablisementet eller afhentes ved indgangen og være under periodevis opsyn under opholdet. Det midlertidige adgangskort skal bæres synligt og som minimum fornys årligt.

Adgangssøgende vejledes i fornødent omfang ved vagtens foranstaltning i overensstemmelse med etablisementets sikkerhedsinstruks og lokale bestemmelser.

I efterfølgende skema er anført, hvem der kan have uledsaget adgang til et kategori 3 område, sikringsniveau 10 eller åbent areal:

Fast personel ved myndigheden				
Områdekategorier ved myndigheden	YHM/HEM-godkendt ved myndighedsområdet. (Fast tjenstgørende i rummet/cellen/arkivet)	HEM-godkendt ved myndigheden	FTR-godkendt ved myndigheden	TTJ-godkendt ved myndigheden
Områdekategori 3, sikringsniveau 10	Ja	Ja	Ja	Ja
Områdekategori 3, åbent areal	Ja	Ja	Ja	Ja

Fast personel i koncernen			
Områdekategorier ved myndigheden	YHM/HEM godkendt i koncernen	FTR-godkendt i koncernen	TTJ-godkendt i koncernen
Områdekategori 3, sikringsniveau 10	Ja	Ja	Ja
Områdekategori 3, åbent areal	Ja	Ja	Ja

Konsulenter, håndværkere og rengøringspersonale				
Områdekategorier ved myndigheden	HEM-godkendt	FTR-godkendt	TTJ-godkendt	Ikke-godkendt
Områdekategori 3, sikringsniveau 10	1	1	1	1
Områdekategori 3, åbent areal	2	2	2	2

1: Efter bemyndigelse fra chefen for myndigheden eller sikkerhedsofficeren, og det sikres, at der ikke gives indsigt i klassificerede sager.

2: Efter bemyndigelse fra garnisonskommandanten.

Adgangskontrollen kan foretages ved indsats af personel eller ved anvendelse af automatisk adgangskontrolanlæg under anvendelse af medie (kort eller brik) og korrekt personlig pin-kode.

2.3 Overvåget område, (periodisk)

2.3.1 Kategori 4 område

Til kategori 4 områder er tjenstgørende personel ved myndigheden (etablisementet) adgangsberechtigt efter bemyndigelse fra chefen for myndigheden eller sikkerhedsofficeren.

3. OPHOLDSKONTROL

Opholdskontrol har til formål at registrere oplysninger om hvilke personer og hvor mange personer, der befinder sig i områder, hvor klassificeret materiale opbevares. Der skal etableres kontrol for identifikation af adgangsberettigede med henblik på udførelse af opholdskontrol ved anvendelse af adgangskort, der skal bæres synligt. Kortet skal som minimum indeholde billede og navn på den adgangsberettigede. Dette gælder dog ikke besøgskort.

Ved den interne opholdskontrol skal uvedkommendes indsigt i eller aflytning af klassificerede informationer søges hindret. Desuden tager opholdskontrollen sigte på at hindre spionage - ved installering/placering af aflytningsudstyr eller ved uretmæssigt indgreb i udstyr, installationer mv. - samt at hindre sabotage, hærværk og tyveri.

Alt tjenstgørende personel skal medvirke ved den interne opholdskontrol og hindre eller rapportere ulovlig færden eller mistænkelig adfærd.

4. UDGANGSKONTROL

Udgangskontrol har til formål at kontrollere, at alle personer, der er indpasseret til sikrede og kontrollerede områder ud passerer ved tjenestetids ophør.

Automatiske adgangskontrolanlæg er en væsentlig støtte i udgangskontrollen.

Såfremt styrelsen, staben eller myndigheden har mistanke om kompromittering af klassificerede materiale eller mistanke om, at materiel e.l. uretmæssigt fjernes fra sikrede eller kontrollerede områder eller etablisementets område, kan kontrol af køretøjer og personel gennemføres efter chefens nærmere bestemmelse evt. bistået af politiet.

Forsvarets Auditørkorps orienteres om kontrollen.

TEKNISKE KRAV TIL ELEKTRONISKE ADGANGSKONTROLANLÆG FOR SIKREDE OMRÅDER.

1. INDLEDNING

Ved gennemførelse af adgangskontrol til sikrede områder er det ofte ønskeligt at erstatte vagtpersonel med elektroniske adgangskontrolanlæg (ADK). Sådanne anlæg kan anvendes, når følgende sikkerhedsmæssige minimumskrav er tilgodeset.

2. ANLÆGGETS ADGANGSKRITERIER

ADK må først give adgang, når to på hinanden følgende adgangskriterier er opfyldt, sædvanligvis gyldigt adgangskort og korrekt personlig identifikationskode. Anlægget skal rumme mulighed for let og hurtigt at ændre kredsen af adgangsberettigede.

Forsvarsministeriets Ejendomsstyrelses (FES) fagbeskrivelser for ADK skal følges.

Adgangen til sikret område skal ske via et kontrolleret område. Samme adgangskontrolanlæg kan betjene adgangskontrollen fra kontrolleret område til sikret område, men kontrollen skal ske i to forskellige trin, fx første trin ved indgang til en sluse fra kontrolleret til sikret område og andet trin fra slusen til det sikrede område.

Adgangskort skal udformes visuelt således, at det ikke umiddelbart lader sig kopiere. Ud over brugerens navn og billede skal kortets løbenummer være synligt på adgangskortet.

En neutral returadresse ved bortkomst accepteres, men er ikke nødvendig, da et tabt kort altid annulleres fra anlægget.

Den personlige identifikations-kode skal bestå af mindst fire cifre.

Forsynes anlægget med overfaldskode, skal denne have samme antal cifre som øvrige personlige koder.

Adgangskortet skal overholde ISO credit card format.

Alle nye kortlæsere skal kunne læse kort/brikker af typen NXP Mifare DESfire EV1, hvor data på kort/brikker er krypteret med 128 Bit AES kryptering.

3. ANLÆGGETS SIKRING OG REAKTION

ADK skal udføres som selvstændige anlæg. Adgangskontrolanlægget skal tilkobles et alarmanlæg for sabotageovervågning og må ikke være integreret med sikringsanlæg (AIA). FES fagbeskrivelse på området skal følges.

4. INSTALLATION

Adgangskontrolanlægget skal installeres således, at kontrolparametrene ikke kompromitteres. Kompromittering kan ske enten visuelt (personlig kode) eller ved kompromitterende udstråling (personlig kode og/eller adgangskortoplysninger).

Kortlæsere kan eventuelt være placeret sammen med kodetastaturet. Kortlæsere skal være mekanisk robuste og afvise vand og snavs. Kortlæsere skal mekanisk og elektrisk (alarmsløjfe) sikres mod uvedkommendes indgreb og/eller manipulation.

Ved læsning og bearbejdning af de på kort indlagte informationer må en kortlæsesers kompromitterende udstråling ikke være læsbar mere end 1 m fra kortlæseren. Dette krav gælder ikke krypteret information. Tilladelig feltstyrke er angivet i NATO publikationen AMSG 720.

Kodetastaturer skal anbringes således, at uvedkommendes indseende forhindres. Tastaturer forsøges anbragt ca. 1,1 m over gulv og på en sådan måde, at uvedkommendes mulighed for at aflæse PIN-koden begrænses mest muligt. Indseende forhindres evt. ved supplerende afskærmning eller indsnævring af rummet, hvor tastaturet er anbragt. Kodetastaturet skal mekanisk og elektrisk (alarmsløjfe) sikres mod uvedkommendes indgreb og/eller manipulation.

Centralenheder og printere mv., der indgår i ADK-anlægget, skal placeres i sikret område således, at kun de systemansvarlige har adgang hertil.

Kompromitterende udstråling fra centralenheder, printere mv. skal begrænses mest muligt. Valg af udstyr og installation skal foregå i henhold til Kapitel 6,

5. YDERLIGERE SIKRINGSTILTAG

Adgangsveje skal forsynes med sikkerhedsgodkendte, mekaniske låse eller spærringer, der kan anvendes uden for normal arbejdstid og i nødsituationer.

Adgangskontrolanlæg skal forsynes med automatisk tilkobling af nødstrøm.

6. LOGNING AF ADGANG / ADGANGSFORSØG

ADK-anlæg skal registrere/logge såvel autoriseret adgang som uautoriserede adgangsforsøg. Registreringen skal angive tid, sted og brugeridentifikation.

Registreringen/logningen skal opbevares ved myndigheden i mindst 1 år og må tidligst destrueres efter gennemført årlig mønstring af informationsbærende klassificeret materiale af klassifikationsgraderne YDERST HEMMELIGT og HEMMELIGT.

BESTEMMELSER VEDRØRENDE FOTOGRAFERING

1. GENERELT

Under henvisning til [Straffeloven](#) § 110 a stk. 1 er der forbud mod at fotografere ikke alment tilgængelige militære etablissementer mv. Forbuddet håndhæves således:

- Fotografering inde på ikke alment tilgængelige militære etablissementer må ikke finde sted, med mindre der af etablisementets chef er givet tilladelse hertil.
- Fotografering fra standpladser uden for etablissementerne tillades i almindelighed. Chefen for et etablisement kan bestemme, at der ikke skrives ind over for fotografering mv., som foretages fra bestemte strækninger uden for området, såfremt fotografier optaget fra disse strækninger skønnes at være uden sikkerheds- eller efterretningsmæssig værdi.

Skærpelse af fotoforbud eller overvågning af fotografering af militære etablissementer, installationer, enheder mv. iværksættes ved [FKOPLAN OP 120-1](#).

2. SKILTNING

Skiltning om fotoforbud skal være i overensstemmelse med det i pkt. 1 anførte.

3. PERSONELLETS PLIGTER

Enhver vagt og befalingsmand har pligt til at skride ind overfor fotografering, afbildning mv. af anlæg, enheder, materiel, våben mv., medmindre den stedlige chef har givet speciel tilladelse til fotografering eller afbildning af det pågældende objekt eller har truffet beslutning om, at en foretagen fotografering eller afbildning kan tillades.

4. FORHOLD VED INDSKRIDEN

I tilfælde af indskriden gøres den pågældende opmærksom på, at fotografering, afbildning mv. af det omhandlede objekt er forbudt i medfør af Straffeloven § 110 a, og anmodes om at udlevere filmen eller opbevaringsmediet (smartphone, digitalt kamera mv.) samt at udtale sig om formålet med fotograferingen/optagelse herunder filmens fabrikat, beskaffenhed, type og øvrige data.

Endvidere sikres den pågældendes navn og adresse samt, så vidt det er muligt, hans stilling, fødselsdato og fødested ved passende legitimation.

Politiet skal omgående tilkaldes, såfremt:

- Den pågældende nægter at udlevere filmen eller opbevaringsmediet eller nægter at legitimere sig på fyldestgørende måde,
- vedkommendes adfærd giver anledning til særlig mistanke,
- overtrædelsen i øvrigt er af en sådan karakter, at det ikke ganske klart fremgår, om forholdet er undskyldeligt, og om videre forfølgning derfor er påkrævet.

I de nævnte tilfælde varetages sagens videre behandling af politiet.

Melding om episoden afgives straks jf. kapitel 10.

I de tilfælde, hvor politiet ikke har været tilkaldt, udfærdiges indberetning med oplysning om den pågældendes identitet samt forklaring vedrørende formålet med fotograferingen og de nærmere omstændigheder ved udførelsen heraf.

Indberetningen fremsendes til FE direkte, iht. kapitel 10.

KAPITEL 8

INDUSTRISIKKERHED

AFSNIT I - GENERELLE FORHOLD

1. INDLEDNING

Industrisikkerhed omfatter foranstaltninger inden for områderne personelsikkerhed, materisikkerhed, dokumentisikkerhed, informationssikkerhed samt fysiske sikkerhed, til beskyttelse af civile virksomheder, der udfører klassificeret arbejde. Bestemmelserne er gældende i såvel udbuds-, produktions- som afleveringsfasen.

2. FORMÅL

Formålet med dette kapitel er at beskrive den sikkerhedspolitik og de principper og minimumskrav, som ligger til grund for sikkerheden ved virksomheder, der udfører klassificeret arbejde for forsvaret, NATO og EU eller de lande med hvilke, der er indgået bilaterale industrisikkerhedsaftaler.

Kapitlet indeholder de særlige sikkerhedsmæssige bestemmelser, som gælder for sikkerhedsgodkendte virksomheder, og som ikke fremgår af de øvrige kapitler. Bestemmelserne vedrører alene rent sikkerhedsmæssige aspekter og ikke forhold vedrørende eksportkontrol. Den enkelte virksomhed er selv ansvarlig for tilladelser til eksport og import af klassificerede produkter.

Endelig indeholder kapitlet bestemmelser for samarbejdet mellem danske virksomheder og forsvarets myndigheder på det sikkerhedsmæssige område.

3. GRUNDLAG

Forsvarets Efterretningstjeneste (FE), Sektionen for Sikkerhedsgodkendelser, gennemfører på Forsvarsministeriets (FMN) vegne godkendelse, uddannelse og kontrol af sikkerheden ved alle virksomheder, der udfører klassificeret arbejde for forsvaret, NATO, EU eller de lande med hvilke, der er indgået bilaterale industrisikkerhedsaftaler. Dette forhold er også gældende i de tilfælde, hvor der er tale om en multinational virksomhed.

Følgende kan indstille en virksomhed til sikkerhedsgodkendelse:

- Forsvarsministeriet
- Forsvarskommandoen (FKO)
- Hjemmeværnskommandoen (HJK)
- Forsvarsministeriets Materiel- og Indkøbsstyrelse (FMI)
- Forsvarsministeriets Ejendomsstyrelse (FES)
- Organisationen Dansk Industri
- Sikkerhedsgodkendte virksomheder kan indstille om godkendelse af deres underleverandører

De indstillende myndigheder har ansvaret for at:

- Der så tidligt som muligt i projekteringsfasen udarbejdes sikkerhedsinstruks for projektet, og at denne ajourføres løbende gennem projektet.

- Der kun anvendes sikkerhedsgodkendte virksomheder til udførelse af klassificerede opgaver eller arbejder.
- Indstille virksomheder til sikkerhedsgodkendelse i de tilfælde, hvor et uklassificeret projekt udvikler sig til et klassificeret projekt.

Sikkerhedsgodkendelse af virksomheder gennemføres efter indstilling fra ovenstående myndigheder og udføres på baggrund af følgende bestemmelser:

- [Stasministeriets sikkerhedscirkulære](#). Cirkulæret vedrørende sikkerhedsbeskyttelse af informationer, der er af fælles interesse for NATO/EU, andre klassificerede informationer, samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt.
- Nærværende bestemmelser for Den militære Sikkerhedstjeneste,
- NATO eller EU direktiver og bestemmelser.
- Bestemmelser vedtaget af Multinational Industrial Security Working Group (MISWG).

4. STRUKTUR

For at lette læseligheden er kapitlet opdelt i følgende emneområder:

- Afsnit I Generelle forhold.
- Afsnit II Godkendelsesprocedure.
- Afsnit III International procedure.

5. ORDFORKLARING

Hvor begreberne "Sikkerhedsgodkendende myndighed", "Godkendende Sikkerhedsmyndighed" og "Sikkerhedsmyndigheden" anvendes, vil det normalt betyde FE..

I forbindelse med NATO eller EU -projekter eller projekter i internationalt regi (joint venture projekter), hvor lande, med hvilke der er truffet bilaterale aftaler, deltager, kan andre landes sikkerhedsmyndigheder være involveret.

6. RISIKOSTYRING

Dansk industrisikkerhedspolitik bygger på Statsministeriets cirkulære [nr. 10338 af 17 december 2014](#) og NATO industrisikkerhedspolitik, som i væsentlig grad understøttes af MISWG standarder.

FE foretager, på baggrund af myndighedens indstilling, en risikovurdering, baseret på klassifikationen af det materiale, der skal opbevares eller bearbejdes i virksomheden.

En virksomhed skal kun sikkerhedsgodkendes, såfremt der i virksomheden skal opbevares klassificerede informationer/materiale.

Arbejder virksomheden udelukkende som konsulent for de indstillende myndigheder, og de klassificerede informationer opbevares hos den aktuelle myndighed, sikkerhedsgodkendes det nødvendige antal medarbejdere, som derefter knyttes sikkerhedsmæssigt til den aktuelle myndighed.

Arbejdet må ikke iværksættes, før konsulenterne er sikkerhedsgodkendt.

Virksomheden skal sikkerhedsgodkendes, hvis den i forbindelse med tilbudsgivning, kontraktforhandlinger, gennemførelse af et projekt eller udførelse af vedligeholdelsesarbejder, skal opbevare klassificerede informationer.

Sikkerhedsgodkendelsesproceduren tager ofte længere tid end tidsforskellen mellem udbud og tilbud. Dette medfører, at en virksomhed, som på udbudstidspunktet ikke er sikkerhedsgodkendt, ikke kan deltage i tilbudsgivningen.

For udbudsmateriale, der er klassificeret TIL TJENESTEBRUG, kan indstillende myndighed udlevere udbudsmaterialet under henvisning til cirkulære [nr. 10338 af 17 december 2014](#)

Ved udsendelse af udbudsmateriale, klassificeret TIL TJENESTEBRUG, til virksomheder, der ikke har den fornødne sikkerhedsgodkendelse, skal teksten i bilag 1 indgå i ledsageskrivelsen. Indstillende myndighed har ansvaret for, at tilbudsgiveren lever op til og overholder bestemmelsen om, at materialet afleveres efter endt brug, og efterfølgende indstiller virksomheden til sikkerhedsgodkendelse.

Indstillende myndighed skal gøre tilbudsgiveren opmærksom på, at der i forbindelse med eventuel kontrakt eller arbejde kan komme udgifter i forbindelse med sikkerhedsgodkendelse af virksomheden, så som etablering af hegn, adgangskontrolanlæg, alarmanlæg samt anskaffelse af godkendt opbevaringsmiddel m.m.

For udbudsmateriale, der er klassificeret FORTROLIGT og højere, skal virksomheden og de medarbejdere, som skal arbejde med materialet, være sikkerhedsgodkendt til den aktuelle klassifikation, før udbudsmaterialet udleveres.

7. ANSVAR OG SIKKERHEDSORGANISATION

7.1. Ansvarlig myndighed.

FE udøver på Forsvarschefens (FC) vegne den daglige ledelse af og kontrol med den militære sikkerhedstjeneste. FE har tillige på FMN vegne, ansvaret for industrisikkerhed i forhold til de civile virksomheder, der udfører klassificeret arbejde for forsvaret og NATO samt i forhold til de lande, med hvilke der er indgået bi- eller multilaterale aftaler.

Indstillende myndighed har ansvaret for, at alle virksomheder, der arbejder med klassificerede informationer inden for eget ansvarsområde, er sikkerhedsgodkendt.

7.2. Chefen.

Virksomhedens chef er ansvarlig for planlægning og udførelse af samt kontrol med den militære sikkerhedstjeneste inden for eget ansvarsområde. Det påhviler chefen at udgive en sikkerhedsinstruks omfattende lokale bestemmelser i forhold til det sikkerhedsmiljø, han pålægges af indstillende myndighed og/eller Virksomhedssikkerhedssektionen.

7.3. Sikkerhedschefen.

Ved alle myndigheder og institutioner samt virksomheder, der udfører klassificeret arbejde, skal virksomhedens chef udpege en sikkerhedschef. (Chefen kan selv varetage opgaven). Sikkerhedschefen har ansvaret for udøvelse af den militære sikkerhedstjeneste, herunder udarbejdelse og vedligeholdelse af sikkerhedsinstruksen, og for at virksomhedens personel sikkerhedsgodkendes og afmeldes, når der ikke længere er brug for sikkerhedsgodkendelsen.

Sikkerhedschefen skal have direkte adgang til virksomhedens chef. Sikkerhedschefen i mindre virksomheder kan samtidig bestride stillingen som informatiksikkerhedschef. Sikkerhedschefen bør have så tæt kontakt til Virksomhedssikkerhedssektionen, at det er naturligt at søge spørgsmål af sikkerhedsmæssig karakter løst her.

7.4. Informationssikkerhedschefen.

Ved alle myndigheder, institutioner og tjenestesteder samt virksomheder, hvor der er elektronisk udstyr, hvorpå der udføres klassificeret arbejde, skal chefen udpege en informati-

onssikkerhedschef. Hans ansvarsområde dækker alle på stedet værende elektroniske systemer. Opgaven kan i mindre virksomheder varetages af chefen selv.

7.5. Personligt ansvar.

Alt personel har ansvaret for at følge sikkerhedsinstruksen, samt pligt til at medvirke til en effektiv sikkerhedstjeneste.

7.6. Interessekonflikter.

Interessekonflikter skal undgås ved valg af sikkerhedspersonel. Sikkerhedschefen bør fx ikke være projektansvarlig og informatiksikkerhedschefen bør ikke være informatikchefen, idet disses arbejdsområder i visse situationer kan være modsat rettede.

8. SIKKERHEDSCHEFENS RAPPORTERINGSPLIGT

Sikkerhedschefen bør jævnligt have kontakt med Virksomhedssikkerhedssektionen, og det er påkrævet, at der **omgående** meldes til sektionen, såfremt der på virksomheden opstår:

- Mistanke om eller konstatering af spionage, sabotage, subversion, terrorvirksomhed samt lignende skadevoldende virksomhed,
- Hændelser, der skønnes af sikkerhedsmæssig betydning, indbrudsforsøg, indbrud, tyveri, tab/bortkomst af materiel eller materielgenstande, komponenter m.v.
- Kompromittering eller anden form for sikkerhedsbrud.
- Mistænkelig adfærd.
- Brud på eller mistanke om brud på den etablerede fortroligheds-, integritets- eller tilgængelighedssikkerhed i informationssystemer.

Sikkerhedschefen skal søge oplyst hos Virksomhedssikkerhedssektionen, om der er særlige hensyn at tage, eller om yderligere foranstaltninger skal iværksættes, fx øjeblikkelig melding til politiet.

Meldepligten må ikke forhindre sikkerhedschefen i omgående indgriben, hvor en person træffes på fersk gerning under udførelse af en forbrydelse eller på friske spor, eller hvor øjeblikkelig indgriben er nødvendig for at hindre skade i at opstå, brand eller lignende som følge af en forbrydelse.

En skriftlig rapport skal umiddelbart efter enhver mistanke eller konstatering af sikkerhedsbrud fremsendes til Virksomhedssikkerhedssektionen. Rapporten skal indeholde så mange af nedennævnte punkter som muligt (se kapitel 10):

- Hvad der er sket (kompromittering, tab eller lignende).
- Hvad der er tabt og/eller kompromitteret.
- Hvor det er sket.
- Hvornår det er sket; kan tidspunktet for tab eller kompromittering ikke angives nøjagtigt, angives tidspunkterne for, hvornår sagen med sikkerhed senest er konstateret værende til stede, og hvornår den først er meldt eller konstateret savnet.
- Hvorledes det er sket; er dette ikke klarlagt, da hvorledes det kan formodes at være sket.
- Hvilke personer, der har tjenstlig adgang til det bortkomne eller kompromitterede materiale, og hvilke personer, der kan tænkes at have haft uretmæssig adgang til materialet.
- Hvilke meldinger og ordrer, der i sagens anledning er afgivet og modtaget, hvilke undersøgelser, der i øvrigt er foretaget - herunder om politi har været tilkaldt.

- Hvilken risiko, tabet eller kompromitteringen skønnes at frembyde.
- Hvilke forholdsregler, der er taget dels til at afbøde den skete skade, dels til imødegåelse af eventuelle lignende tilfælde i fremtiden.
- Eventuel mistanke.

Grundlaget for sikkerhedschefens rapportering er ofte information fra medarbejderne, hvorfor det er nødvendigt, at denne nyder almen tillid i alle medarbejderkredse. Den enkelte medarbejder skal trygt kunne henvende sig til sikkerhedschefen, ligesom denne skal kunne henvende sig til enhver medarbejder, uden at der derved opstår misforståelse, ængstelse, rygtedannelse eller lignende.

9. TRANSPORT AF KLASSIFICERET MATERIALE

9.1. HEM/NS og FTR/NC materiale.

9.1.1. Generelt

- Ved transport af klassificeret materiale skal bestemmelserne i kapitel 4 vedrørende pakning og emballering til forsendelse/transport være gennemført.
- Tilladelse til transport skal gives af den ansvarlige myndighed.
- Der skal foreligge en fortegnelse over materialet, der skal transporteres.
- Personer, der gennemfører transporten, skal være sikkerhedsgodkendt til samme klassifikationsgrad som transportens indhold.
- Alt materiale uanset rumfang skal transporteres i godkendt transportmiddel.

9.1.2. Udland

Under transport til/fra udland skal Courier Certificate (se bilag 2) og/eller (se bilag 3) samt Certificate of Security Clearance (se bilag 4) medbringes. Begge certifikater udstedes af Sektionen for Sikkerhedsgodkendelser ved FE. Efter transportens gennemførelse returneres bilag 2 og/eller bilag 3 i udfyldt stand til Virksomhedssikkerhedssektionen.

9.1.3. Indland

Ved transport inden for landets grænser skal Certificate of Security Clearance (bilag 4) og/eller (se bilag 5) medbringes. Certifikatet udstedes af Sektionen for Sikkerhedsgodkendelser ved FE.

9.2. TTJ/NR og NU materiale.

Materiale, der er klassificeret TTJ/NR eller NU, kan umiddelbart transporteres i ind- og udland af personer, der er sikkerhedsgodkendt til TTJ/NR.

**SIKKERHEDSGODKENDELSE I FORBINDELSE MED UDBUDSFORRETNINGER
(AFSKRIFT)**

TIL TJENESTEBRUG

**FORSVARETS
EFTERRETNINGSTJENESTE**

Kastellet 30, 2100 København Ø
Telefon 33 32 55 66
Telefax 33 14 62 60
E-mail fe@fe-mail.dk

SEKTIONEN FOR SIKKERHEDSGODKENDELSE

Nr.	B.358.8/BV-
Dato	

(Bedes anført ved henvendelser)

Til :

Emne : SIKKERHEDSGODKENDELSE AF FIRMAER I FORBINDELSE
MED UDBUDSFORRETNINGER.

1. Forsvarets Efterretningstjeneste (FE) har bemærket, at adressaterne ofte udsender udbudsmateriale til ikke sikkerhedsgodkendte firmaer, hvorefter der senere tilgår FE en skrivelse med anmodning om sikkerhedsgodkendelse af de aktuelle firmaer eller af enkeltpersoner.

2. Tiden mellem udsendelsestidspunktet og licitationstidspunktet er ofte så kort, at en endelig sikkerhedsgodkendelse ikke kan gennemføres. FE har derfor bestemt, at ved udsendelse af udbudsmaterialer med klassifikationsgraden TIL TJENESTEBRUG skal nedennævnte tekst indgå i ledsageskrivelsen til de firmaer, der ikke har den fornødne sikkerhedsgodkendelse.

Opmærksomheden skal henledes på

“Cirkulære nr. 204 af 7. december 2001 vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt”.

Neden for følger en afskrift af de væsentligste sikkerhedsaspekter, der bør tilgodeses ved behandling af sager, klassificeret til TIL TJENESTEBRUG.

- TIL TJENESTEBRUG anvendes på dokumenter, der ikke må offentliggøres eller komme til uvedkommendes kundskab.

TIL TJENESTEBRUG

TIL TJENESTEBRUG

- Enhver, som har klassificerede dokumenter til behandling, har pligt til at udvise den største omhu for at sikre, at uvedkommende ikke bliver bekendt med dokumenternes indhold.
- Indsigt i klassificerede dokumenter må kun gives personer, for hvem en sådan indsigt er tjenstligt nødvendigt.
- Ingen er berettiget til at gøre sig bekendt med klassificerede dokumenter, der ikke er forelagt den pågældende til behandling eller gennemsyn.
- Et klassificeret dokument må ikke udlånes eller udleveres til nogen anden person, der ikke af vedkommendes nærmeste chef er bemyndiget til at behandle dokumenter af den pågældende klassifikationsgrad.
- Opbevaring af dokumenter, når disse ikke umiddelbart anvendes, skal finde sted i aflåst skrivebordsskuffe, pengeskab og lignende.

På grund af tidsfaktoren kan FE ikke nå at sikkerhedsgodkende Deres firma og de medarbejdere, som nødvendigvis skal have indsigt i dokumenter, tegninger m.m.

De anmodes derfor om at leve op til bestemmelserne om indsigt og opbevaring.

Får Deres firma det udbudte arbejde, melder udbyderen dette til FE, som derefter gennemfører en egentlig "godkendelsesforretning" i nødvendigt omfang.

Eventuelle spørgsmål i forbindelse med ovenstående kan rettes til Sektionen for Sikkerhedsgodkendelser ved Forsvarets Efterretningstjeneste, tlf. 3332 5566.

3. For udbudsmateriale, der er klassificeret FORTROLIGT og højere, henledes opmærksomheden på kapitel 4 i FKOBST 358-1, hvori det bestemmes, at sikkerhedsgodkendelse skal være gennemført, før materialet udleveres.

Underskrift

TIL TJENESTEBRUG

COURIER CERTIFICATE (AFSKRIFT)DANISH DEFENCE
INTELLIGENCE SERVICEKastellet 30
DK-2100 Copenhagen
Tel: 33 32 55 66
milsik@fe-ddis.dk
www.fe-ddis.dk08 June 2016
Document no.:

COURIER CERTIFICATE No. XX/201x

**FOR THE HAND-CARRIAGE
OF CLASSIFIED INFORMATION**

This is to certify that the bearer:

[fulde navn]

born on [dd. mmm åååå] in [land]

a national of Denmark

holder of passport no.: [pasnr.]

issued by: [pasudstedende myndighed]

expiry: [dd. mmm åååå]

employed with: [firmanavn]

is authorized to act as courier on the journey detailed below for the following consignment:

(Number and particulars of the consignment in detail, i.e. No. of packages, weight and dimensions of each package and other identification data as in shipping documents)

The attention of Customs, Police, and/or Immigration Officials is drawn to the following:

- The material comprising this consignment is classified in the interests of the National Security of: The Kingdom of Denmark and The United States of America.
- It is requested that the consignment will not be inspected by other than properly authorized persons or those having special permission.
- If an inspection is deemed necessary, it is requested that it be carried out in an area to which persons not belonging to these services do not have access, and in the presence of the courier.
- It is requested that the package, if opened for inspection, and in order to authenticate this opening, be marked after reclosing by a seal and signature, and that the shipping documents (if any) be annotated to the effect that the consignment has been opened.
- Customs, Police, and/or Immigration officials of countries to be transmitted, entered or exited are requested to give assistance if necessary to ensure successful and secure delivery of the consignment.

□

ITINERARY

From: [land hvor rejsen begyndes]

To: [land hvor rejsen slutter]

Through: [lande der passeres]

2/6

Authorized stops: [list steder – f.eks. lufthavne]

Date of beginning of journey [dd. mmm åååå]

Signature of the
Security Officer of
[firmanavn]

Signature of the Danish National Security
Authority

.....
[navn]

.....
[navn]

Stamp

stamp

NOTE: To be signed on completion of journey:

I declare in good faith that, during the journey covered by this Courier Certificate, I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment.

Couriers's Signature:

Witnessed by (signature of the Security Officer of the Company):

Date of return of the Courier Certificate: (day/month/year)

I

Annex to Courier Certificate no. x/201x

NOTES FOR COURIERS

1. You have been appointed to act as a courier. Your Courier Certificate has been provided. Before starting the journey, you will be briefed on the security regulations governing the escort of the classified consignments and on your security obligations during the specific journey (behavior, itinerary, schedule, etc.). You will also be requested to sign a declaration that you have read and understand and will comply with prescribed security obligations.
2. The following general points are brought to your attention:
 - (a) you will be held liable and responsible for the consignment described in the Courier Certificate;
 - (b) throughout the journey, the classified consignment must stay under your personal control;
 - (c) the consignment will not be opened en route except in the circumstances described in sub-paragraph (j) below;
 - (d) the classified consignment is not to be discussed or disclosed in any public place;
 - (e) the classified consignment is not, under any circumstances, to be left unattended. You are to be instructed on this matter by your company Security Officer;
 - (f) while escorting a classified consignment, you are forbidden to deviate from the travel schedule provided;
 - (g) in cases of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your personal control; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as listed in sub-paragraph (i) below. If you have not received these details, ask for them from your company Security officer;
 - (h) you and the company Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc) are complete, valid and current;

-
- (i) if unforeseen circumstances make it necessary to transfer the consignment to other than the designated representatives of the government you are to visit, you will give it only to authorised employees of one of the points of contact listed in subparagraph (1);

- (j) there is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials inquire into the contents of the consignment, show them your Courier Certificate and this note and insist on showing them to the actual senior Customs, Police and/or Immigration Official; this action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police and/or Immigration Official demands to see the actual contents of the consignments you may, open it in his presence, but should be done in an area out of sight of the general public.
You should take precautions to show officials only as much of the contents as will satisfy them that the consignment does not contain any other item and ask the official to repack or assist in repacking it immediately upon completion of the examination.

You should request the senior Customs, Police and/or Immigration Official to provide evidence of the opening and inspection of the package s by signing and sealing them when closed and confirming in the shipping documents that the consignment has been opened.

If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving company Security Officer and the dispatching company Security Officer, who should be requested to inform the NSA/DSA of their respective governments.

- I (k) Upon your return, you must produce a bona fide receipt for the consignment signed by the Security Officer of the company or agency receiving the consignment or by the NSA/DSA of the receiving government.

(I) Along the route you may contact the following officials to request assistance:

US official: [fulde navn og kontaktoplysninger for den amerikanske virksomheds sikkerhedsofficer]

Danish official: [fulde navn og kontaktoplysninger for danske virksomheds sikkerhedschef]

DECLARATION

The Security Officer of [dansk virksomheds navn] handed to me the Notes concerning the handling and custody of classified equipment and components to be escorted by me.
I have read and understood their contents.

I shall always retain en route the classified information and shall not open the consignment unless required by the Customs Authorities etc.

Upon arrival, I shall hand over the classified equipment intended for the receiving organization against receipt, to the designated consignee.

(Place and date)

(signature of escort)

Witnessed by (Company Security Officer's signature)

CERTIFICATE OF SECURITY CLEARANCE (AFSKRIFT)**CERTIFICATE OF SECURITY CLEARANCE**

Issued by
(member nation or EU/WEU/NATO civil or military body)

Date and Place of Issue

..... Valid until

This is to certify that:

Full Name

Date of Birth

Place of Birth

Nationality

Where employed

Purpose and Duration of Visit

.....

.....

Holder of Passport/Identity Card No.

Issued at Dated

Military Rank and Number (where applicable)

.....

has been granted access to EU, WEU or NATO information classified up to and including
..... in accordance with
current EU, WEU or NATO security regulations (NATO including the Security Annex to C-M(64)39,
and has been briefed accordingly by
.....

Signed:

Title:

Official government stamp (Optional)

Date:

NOTE : This certificate must be handled in accordance with the provisions of NATO Security Policy and its supporting directives.

AFSNIT II - GODKENDELSESPROCEDURE

1. INDLEDNING

Sikkerhedsgodkendelse af en virksomhed er en forudsætning for deltagelse i klassificeret arbejde. Dette er gældende for såvel nationalt som internationalt samarbejde. I forbindelse med udbud, tilbud og virksomhedsbesøg samt besøg på militære installationer i ind- og udland er der aftalt særlige procedurer. Disse procedurer og tilhørende dokumenter er beskrevet i afsnit III.

2. FORMÅL

Formålet med afsnit II er at fastlægge godkendelsesproceduren for virksomheder, der indstilles til at arbejde med klassificerede projekter, samt sikkerhedsgodkendte virksomheder, der ønsker at give tilbud på udbudte NATO og WEU projekter eller ønsker at indgå i internationalt sikkerhedsklassificeret samarbejde.

3. INDSTILLING

En virksomhed, der ønsker at udføre klassificeret arbejde, kan lade sig indstille til sikkerhedsgodkendelse af en af følgende indstillende myndigheder:

- Forsvarsministeriet
- Forsvarskommandoen (FKO)
- Hjemmeværnskommandoen (HJK)
- Forsvarsministeriets Materiel- og Indkøbsstyrelsen (FMI)
- Forsvarsministeriets Ejendomsstyrelse (FES)
- Dansk Industri
- Sikkerhedsgodkendte virksomheder.

4. PROCEDURE

Ved indstilling til sikkerhedsgodkendelse anvendes det i bilag 1 (se bilag 1) viste skema. Det er væsentligt, at indstillende myndighed har afklaret med virksomheden (hovedkontraktholderen), om det påregnes, at der skal indgå underleverandører i projektet.

Kan den indstillede virksomhed forudse, at der skal anvendes underleverandører, skal virksomheden indhente tilladelse hos ejeren af de klassificerede informationer, før disse frigives til underleverandøren.

Hovedkontraktholderen har ligeledes ansvaret for at underleverandøren er sikkerhedsgodkendt til den aktuelle klassifikationsgrad. Er underleverandøren ikke sikkerhedsgodkendt, er det hovedkontraktholderens ansvar, at indstilling foretages via den projektansvarlige myndighed. Intet klassificeret materiale må udleveres til underleverandøren, før hovedkontraktholderen har modtaget en skrivelse fra Sektionen for Sikkerhedsgodkendelser om, at underleverandøren er sikkerhedsgodkendt.

Hovedkontraktholderen har således ansvar for, at underleverandøren er sikkerhedsgodkendt til den nødvendige klassifikationsgrad, og at indehaveren af ophavsretten til informationerne har givet tilladelse til frigivelse af de fornødne informationer.

Militære myndigheder indstiller via respektive sikkerhedsofficer direkte til Virksomhedssikkerhedssektionen om sikkerhedsgodkendelse af virksomheder, som de pågældende militære myndigheder har udpeget til at udføre en aktuel opgave. Nødvendige virksomhedsoplysninger fremgår af bilag 1.

Der må ikke udleveres klassificerede informationer til den pågældende virksomhed, før der foreligger en sikkerhedsgodkendelse, se afsnit I, pkt. 6.

5. INDLEDENDE UNDERSØGELSE

Med baggrund i det modtagne skema, eller en skrivelse med tilsvarende indhold, vil virksomheden blive kontaktet af Sektionen for Sikkerhedsgodkendelser for aftale om et besøg, så sektionen kan skabe sig et overblik over virksomhedens fysiske beliggenhed, indretning m.m.

Dette første besøg danner grundlag for en vurdering af virksomhedens sikkerhedsniveau i forhold til den ønskede klassifikation. På mødet aftales eventuelt justering af sikkerhedsniveauet, så dette kan leve op til nærværende bestemmelser.

Sektionen for Sikkerhedsgodkendelser kan i særlige tilfælde lade sammensætte en arbejdsgruppe til vurdering af den fysiske sikkerhed og informatiksikkerheden.

Ved dette første møde skal virksomheden fremlægge et sammenskrevet resumé fra Erhvervs- og Selskabsstyrelsen, så ejerforhold og økonomiske forhold bliver oplyst. I forbindelse med mødet udleveres oplysningsskema I eller II til anvendelse i forbindelse med sikkerhedsgodkendelse af personel.

6. GODKENDELSE

I forbindelse med en virksomhedsgodkendelse skal virksomhedslederen, bestyrelsesformanden og samtlige bestyrelsesmedlemmer, sikkerhedschefen og en eventuel stedfortrædende sikkerhedschef være godkendt til virksomhedens klassifikationsgrad, dog som minimum FORTROLIGT.

Hvis en person, der er indstillet til sikkerhedsgodkendelse, ikke kan godkendes til den nødvendige klassifikationsgrad, vil Virksomhedssikkerhedssektionen rette henvendelse til sikkerhedschefen og anmode virksomheden om at trække ansøgningen om sikkerhedsgodkendelse tilbage og indstille en anden medarbejder.

National sikkerhedsdeklaration udstedes, når virksomhedens personel er sikkerhedsgodkendt og de oven for nævnte sikkerhedstiltag er udført og kontrolleret.

Virksomheden tilsendes en skrivelse, hvoraf det fremgår, hvilken klassifikation virksomheden er godkendt til, og i hvilket tidsrum godkendelsen gælder. Skrivelsen er bilagt en national sikkerhedsdeklaration, bilag 8-II-2 (se bilag 2), i to eksemplarer, hvoraf det ene beholdes ved virksomheden og det andet tilsendes Virksomhedssikkerhedssektionen i underskrevet stand. Når underskrevet eksemplar er modtaget i Virksomhedssikkerhedssektionen, er virksomheden sikkerhedsgodkendt og skrivelse herom vil tilgå virksomheden.

Virksomhedssikkerhedssektionen vil efterfølgende tillige underrette den indstillende myndighed om resultatet.

I virksomheder, der kun skal sikkerhedsgodkendes til klassifikationsgraden TIL TJENESTEBRUG vil sikkerhedschefen modtage en kopi af cirkulære af 7. december 2001, nærværende kapitel 8, samt uddrag af den øvrige del af de militære sikkerhedsbestemmelser.

Cirkulæret og kapitel 8 vil, sammen med grunduddannelse (se pkt. 11) og aflæggelse af konsulentbesøg, danne basis for sikkerheden i virksomheden.

I virksomheder, der skal sikkerhedsgodkendes til klassifikationsgraden FORTROLIGT og højere, vil sikkerhedschefen i forbindelse med godkendelsesproceduren modtage og få gennemgået nærværende sikkerhedsbestemmelser.

7. AFMELDELSE

Sikkerhedsgodkendelser skal afmeldes ved fratrædelse af den stilling, hvortil godkendelse er nødvendig. Dette har gyldighed ved såvel internt som eksternt arbejdsskifte. Såfremt der om en person, der er sikkerhedsgodkendt, opstår tvivl om dennes sikkerhedsmæssige kvalifikationer og forståelse, skal sikkerhedschefen eller den ansvarlige leder efter forholdene begrænse den pågældendes adgang til klassificeret materiale og klassificerede eller sikrede områder og derefter indberette forholdet til Sektionen for Sikkerhedsgodkendelser.

8. EJERSKIFTE

Planlægges ejerskifte eller fusion skal virksomheden snarest underrette Sektionen for Sikkerhedsgodkendelser om det kommende ejerforhold. Er ejerskiftet så langt fremskredet, at det allerede er registreret i Erhvervs- og Selskabsstyrelsen, medsendes et resumé.

9. FRATRÆDELSERKLÆRING

Forlader en sikkerhedsgodkendt medarbejder virksomheden eller skifter til en anden funktion, der ikke kræver sikkerhedsgodkendelse, skal den pågældende underskrive en fratrædelseserklæring, se bilag 3 (se bilag 3).

Fratrædelseserklæringen skal opbevares i virksomheden i 5 år, efter at den pågældende medarbejder er ophørt med at være beskæftiget med klassificeret materiale, og skal derefter destrueres. Erklæringen tjener to formål: At sikre, at medarbejderen har forpligtet sig til ikke at videregive klassificerede informationer efter fratrædelse, og at medarbejderen ved sin underskrift har erklæret ikke at være i besiddelse af klassificeret materiale.

10. DATABESKYTTELSE

Virksomheden skal ved sin behandling af personoplysninger overholde de forpligtelser, der følger af EU's persondataforordning og anden lovgivning.

Oplysningerne i et udfyldt oplysningsskema og eventuelle bilag hertil indhentes udelukkende med henblik på FE's behandling af sagen om sikkerhedsgodkendelse og må ikke benyttes til andre formål. De udfyldte skemaer mv. og oplysninger herfra må således ikke kopieres, lagres elektronisk eller underkastes nogen anden behandling hos virksomheden end 1) **gennemlæsning** med henblik på at konstatere evt. fejlagtig udfyldelse, 2) **påtegning** med virksomhedens indstilling, og 3) **videresendelse** til FE.

Skrivelser og andre meddelelser fra FE vedrørende sikkerhedsgodkendte medarbejdere, må opbevares, så længe det tjener et sagligt formål for virksomheden, men skal normalt slettes senest 5 år efter medarbejderens fratræden.

Udfyldte oplysningsskemaer må alene behandles af sikkerhedschefen og de evt. andre medarbejdere i virksomheden, som sikkerhedschefen særligt har autoriseret hertil. Antallet af autoriserede medarbejdere skal begrænses til færrest muligt, og de pågældende skal være orienteret om deres pligt til at beskytte oplysningerne og skal være sikkerhedsgod-

kendt til mindst TIL TJENESTEBRUG eller indstillet hertil.

Oplysningerne skal opbevares efter de regler, der gælder for TIL TJENESTEBRUG klassificeret information. Det vil sige i aflåst gemme (sikringsskab eller almindeligt kontormøbel).

Udfyldte oplysningsskemaer og bilag hertil skal sendes til FE i lukkede, uigennemsigtige kuverter. Der må ikke ske forsendelse i ukrypteret form på internettet.

Sikkerhedschefen skal omgående underrette FE om brud på persondatasikkerheden, der sker i forbindelse med virksomhedens behandling af oplysninger vedrørende sikkerhedsgodkendelse.

Alvorlige eller gentagne brud på persondatasikkerheden kan få konsekvenser for virksomhedens sikkerhedsgodkendelse.

11. LUKNING ELLER KONKURS

Det er virksomhedens ansvar snarest muligt at underrette Sektionen for Sikkerhedsgodkendelser, indstillende myndighed og eventuel hovedleverandør i tilfælde af lukning af virksomheden eller konkurs, således at inddragelse af klassificeret materiale samt udleverede militære bestemmelser mv. kan finde sted.

I tilfælde af lukning af virksomheden, konkurs eller afmelding afleveres samtlige fratrædelseserklæringer til Virksomhedssikkerhedssektionen.

12. UDDANNELSE

Sektionen for Sikkerhedsgodkendelser afholder to gange om året et kursus for nye sikkerhedschefer, normalt i marts og oktober. Kursus er obligatorisk for alle sikkerhedsgodkendte virksomheder.

INDSTILLING OM SIKKERHEDSGODKENDELSEINDSTILLING OM SIKKERHEDSGODKENDELSE

Firma navn:		
Firma adresse:		
Firma ledelse Virksomhedsleder:	Telefon nr.:	Telefax nr.:
	Kontaktperson:	
Bestyrelsesformand:	Leverandør:	[]
	Underleverandør:	[]
Klassifikation, projekt/opgave (hvis kendt):		
Projektnavn og -reference nr. (militære projektansvarlige):		
Beskrivelse af projekt/arbejde (arbejdets omfang eller projektindhold: materieltype/-system):		
Navn og adresse på hovedleverandør (udfyldes kun af underleverandør):		
Navn og adresse på underleverandør med klassificeret arbejde/opgave:		

SIKKERHEDSDEKLARATION NATO (AFSKRIFT)

Kastellet 30
2100 København Ø
Telefon: 33 32 55 66
godkendelser@fe-ddis.dk
www.fe-ddis.dk

4. februar 2016
Sagsnr. 1234567890

Sikkerhedsdeklaration
vedrørende
beskyttelse af *nationale* og *NATO* klassificerede sager

Virksomheden

Navn:

Adresse:

Leder af virksomheden:

Fulde navn:

Stilling:

Virksomheden erklærer herved at have gjort sig bekendt med bestemmelserne vedrørende sikkerhedsbeskyttelse af klassificerede sager, og at de sikkerhedsforskrifter, der er gældende, vil blive overholdt i forbindelse med sådanne sagers behandling.

Virksomheden er indforstået med at give Forsvarets Efterretningstjeneste adgang til virksomheden, med henblik på at kontrollere sikkerhedsforskrifternes overholdelse.

Forbindelser til udlandet

	Nej	Ja (anføres nærmere)
1. Ejers nogen del af virksomhedens kapital af udlændinge? ¹⁾		
2. Er virksomheden organiseret på en sådan måde, at aktieselskaber eller lign., der er tilknyttet virksomheden, drives af udlændinge? ¹⁾		
3. Har virksomheden overenskomst med udlændinge vedrørende udveksling af licenser, patenter eller fabrikationshemmeligheder?		
4. Har virksomheden nogen aftale med agentur, kompagniskab eller lign., med udlændinge? ¹⁾		
5. Har virksomheden gæld til eller modtager økonomisk støtte fra udlændinge? ¹⁾		
¹⁾ Ved udlændinge forstås: a) Enhver person som ikke er dansk statsborger. b) Enhver form for forretningsvirksomhed, som befinder sig uden for landets grænser. c) Enhver form for forretningsvirksomhed her i landet, som ejes af eller kontrolleres af udlændinge eller et udenlandsk firma.	NATO oplysninger, uanset art, må ikke videregives til statsborgere fra ikke-NATO lande uden skriftlig tilladelse fra Forsvarets Efterretningstjeneste, Virksomhedssikkerhedssektionen.	
(Virksomhedens stempel)		
_____ (Dato) _____ (Underskrift)		

FRATRÆDELSESERKLÆRING

TIL TJENESTEBRUG

FRATRÆDELSESERKLÆRING

for

Fulde navn:

CPR-nummer og fødested:

Stilling:

Bopæl:

Under Deres ansættelse ved virksomheden har De været beskæftiget med sager, der har været klassificeret

.....
(klassifikationsgrad)

De er i fremtiden forpligtet til ikke at videregive de klassificerede oplysninger, som De under Deres ansættelse i virksomheden har fået kendskab til.

Brud på tavshedsloftet kan medføre straf efter straffeloven.

Undertegnede erklærer herved, at jeg har forstået ovenstående, samt at jeg ved min afgang fra virksomheden ikke er i besiddelse af klassificerede sager.

.....
(underskrift)

TIL TJENESTEBRUG

AFSNIT III - INTERNATIONAL PROCEDURE

1. INDLEDNING

Der er i ovennævnte bestemmelser fastlagt retningslinier og procedurer for besøg ved NATO og WEU etablissementer, militære installationer og virksomheder i udlandet, der udfører klassificeret produktion for NATO/WEU. På tilsvarende vis er der fastsat bestemmelser for besøg hos udenlandske virksomheder, hvormed danske virksomheder ønsker at indgå samarbejde om udførelse af klassificeret arbejde.

Fælles for disse besøg er, at såvel besøgsmodtager som den besøgende skal være sikkerhedsgodkendt til den aktuelle klassifikationsgrad.

Virksomhedssikkerhedssektionen ved FE udfærdiger de nødvendige dokumenter i forbindelse med besøg. Der kan være tale om et antal besøg inden for en defineret periode (max 1 år), eller et pludseligt opstået behov.

2. FORMÅL

Formålet med afsnit III er at gennemgå procedurer og de tilhørende dokumenter, som anvendes i forbindelse med deltagelse i internationalt samarbejde, hvor klassificeret materiale behandles.

Afsnittet beskriver arbejdsgange og dokumenter. Proceduren og beskrivelsen er primært baseret på anvendelse i NATO og WEU lande og de lande, hvormed Danmark har indgået industrisikkerhedsaftaler.

Procedurerne støtter sig til NATO og WEU direktiver og bestemmelser samt procedurer vedtaget af Multinational Industrial Security Working Group (MISWG).

3. PERSONEL

Sikkerhedsgodkendt personel, der skal besøge de i pkt. 1. nævnte institutioner, indsender en udfyldt REQUEST FOR VISIT formular (bilag 1 (se bilag 1) og/eller bilag 2 (se bilag 2)). Det udfyldte bilag fremsendes til Sektionen for Sikkerhedsgodkendelser pr. mail, telefax eller brev.

Bilag 1 består af 4 sider og bilag 2 af 8 sider, som kan kombineres. Side 1 og 2 skal altid udfyldes og gælder for én persons besøg ved én virksomhed. Side 3 anvendes, hvis denne person skal besøge flere virksomheder inden for samme nation på samme rejse. Side 4 anvendes hvis personen, nævnt på side 1 og 2, skal ledsages af en eller flere medarbejdere fra samme virksomhed på rejsen.

Den udfyldte REQUEST FOR VISIT formular skal som minimum indeholde:

- Besøgets forventede klassifikationsgrad *)

Besøgsmodtager

- Virksomhedens navn
- Virksomhedens adresse
- Virksomhedens telefon nr.
- Virksomhedens kontaktpersoner

Besøgende

- Fulde navn
- Fødselsdato
- Fødested
- Nationalitet
- Sikkerhedsgodkendelse
- Pasnummer og eventuel ID-kort nr.

Egen virksomhed

- Årsag til besøg
- Kopi af en eventuel invitation.
- Besøgsperiode (fra/til).

*)Sektionen for Sikkerhedsgodkendelser undersøger, om firmaet er sikkerhedsgodkendt til den krævede klassifikation.

Den ansøgende virksomhed eller person vil fra Sektionen for Sikkerhedsgodkendelser modtage en bekræftelse på godkendelse af besøg.

4. FACILITY SECURITY CLEARANCE CERTIFICATE/ INFORMATION SHEET (FIS)

Hvis en virksomhed ønsker at give tilbud på eller skal udføre klassificeret arbejde i forbindelse med NATO og WEU projekter, eller deltage i multinationalt samarbejde, skal virksomheden dokumentere sin sikkerhedsgodkendelse. Dertil anvendes Facility Security Clearance Certificate. Facility Security Clearance Certificate findes i to udgaver, vist i bilag 3 (se bilag 3) og bilag 4 (se bilag 4). Disse anvendes i forbindelse med klassificerede NATO og WEU projekter. Facility Security Clearance Information Sheet (FIS), bilag 5 (se bilag 5) og/eller bilag 6 (se bilag 6) bruges i forbindelse med andre klassificerede, multinationale projekter.

Anmodning om udstedelse af Facility Security Clearance Information Sheet kan komme fra besøgsmodtageren via modtagerlandets sikkerhedsmyndighed eller den tilbudsgivende virksomhed. Sektionen for Sikkerhedsgodkendelser vil udstede og fremsende kopi til modtagerlandets sikkerhedsmyndighed.

Den besøgende vil selv modtage originalen fra Sektionen for Sikkerhedsgodkendelser og skal medbringe denne ved besøg hos modtageren.

5. KONTAKT MED UDLÆNDINGE.

Medarbejdere i virksomheder, som udfører klassificeret arbejde, udgør uanset stilling eller sikkerhedsgodkendelse potentielle mål for fremmede efterretningstjenester. Det påhviler derfor alle sikkerhedsgodkendte medarbejdere at melde til sikkerhedschefen om enhver kontakt med personer, hvis oprindelse eller adfærd kan give anledning til mistanke om efterretningsaktivitet.

Såfremt mistanke opstår, afgiver sikkerhedschefen indledningsvis telefonisk melding til Sektionen for Sikkerhedsgodkendelser, jf. afsnit I pkt. 8.

6. REJSER TIL OG OPHOLD I UDLANDET.

Såfremt en sikkerhedsgodkendt medarbejder skal foretage rejse til udlandet, skal den rejssende orienteres om de risici, der kan være forbundet med rejse i det pågældende land samt de forholdsregler, der bør træffes.

Efter hjemkomsten skal sikkerhedschefen indhente oplysninger om, hvorvidt den pågældende har været udsat for hændelser af sikkerhedsmæssig karakter eller af usædvanlig art. Disse oplysninger sendes til Sektionen for Sikkerhedsgodkendelser ved FE.

REQUEST FOR VISIT (NATO) (AFSKRIFT)**REQUEST FOR VISIT**

- ☐ ONE TIME
☐ RECURRING
☐ EMERGENCY

ADMINISTRATIVE DATA	
1. REQUESTOR:	
Date:	
To:	
Visit to:	
2. REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY	
Name:	
Postal address:	
Telex/Fax nr.:	Telephone nr.:
3. GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED	
Name:	
Address:	
Telex/Fax nr.:	Telephone nr.:
Point of contact:	
4. DATES OF VISIT: / / to / /	
5. TYPE OF VISIT: (Select one from each column)	
☐ Government initiative	☐ Initiated by requestor
☐ Commercial initiative	☐ By invitation/facility
6. SUBJECT TO BE DISCUSSED/JUSTIFICATION	
7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED:	
8. IS THE VISIT PERTINENT TO: SPECIFY:	
A specific equipment/weapon	☐
Foreign military sales/export license	☐
A programme or agreement	☐
A defence acquisition process	☐
Other	☐

REQUEST FOR VISIT (CONTINUATION)

9. PARTICULARS OF VISITORS		Enclosure	()
Name:			
Date of birth:		Place of birth:	
Security clearance:		PP number:	
Position:		Nationality: DA	
Company/Agency			
10. THE SECURITY OFFICER OF THE REQUESTING AGENCY/FACILITY			
Name:		Telephone:	
Signature:			
11. CERTIFICATION OF SECURITY CLEARANCE		STAMP	
Name:			
Address:			
Telephone:			
Signature:			
12. REQUESTING NATIONAL SECURITY AUTHORITY			
Name:			
Address:			
Telephone:			
Signature			
13. REMARKS:			

REQUEST FOR VISIT

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED

1. Name:
Address:

Telefax/Fax No.:
Point of Contact: Telephone No.:
2. Name:
Address:

Telefax/Fax No.:
Point of Contact: Telephone No.:
3. Name:
Address:

Telefax/Fax No.:
Point of Contact: Telephone No.:
4. Name:
Address:

Telefax/Fax No.:
Point of Contact: Telephone No.:
5. Name:
Address:

Telefax/Fax No.:
Point of Contact: Telephone No.:
6. Name:
Address:

Telefax/Fax No.:
Point of Contact: Telephone No.:

REQUEST FOR VISIT

1.	Name: Date of birth: Security clearance: Position: Company/Agency:	Place of birth: PP number: Nationality: DA
2.	Name: Date of birth: Security clearance: Position: Company/Agency:	Place of birth: PP number: Nationality: DA
3.	Name: Date of birth: Security clearance: Position: Company/Agency:	Place of birth: PP number: Nationality: DA
4.	Name: Date of birth: Security clearance: Position: Company/Agency:	Place of birth: PP number: Nationality: DA
5.	Name: Date of birth: Security clearance: Position: Company/Agency:	Place of birth: PP number: Nationality: DA
6.	Name: Date of birth: Security clearance: Position: Company/Agency:	Place of birth: PP number: Nationality: DA
7.	Name: Date of birth: Security clearance: Position: Company/Agency:	Place of birth: PP number: Nationality: DA

REQUEST FOR VISIT (WEU) (afskrift)

Udgået

FACILITY SECURITY CLEARANCE CERTIFICATE (FSCC) (AFSKRIFT)**Facility Security Clearance Certificate (FSCC)**

1. This is to certify that on (date), the National Security Authority of **Denmark** granted to the
(name of facility) located at (address of facility) a
NATO (classification) security clearance in accordance
with the provisions of the Industrial Security Directive 4 to the NATO Security
Policy, C-M (2002)49, valid until (date).
2. The National Security Authority of **Denmark** confirms that the facility referred
to in paragraph 1 above :
 - (a) * possesses storage capabilities approved for the safeguarding of
classified information up to the NATO level;
 - (b) * possesses NO storage capabilities approved for the safeguarding of
NATO classified information.

.....

(Signature)

.....

(Stamp or seal of Issuing Authority)

* Delete (a) or (b) as applicable.

WEU FACILITY SECURITY CLEARANCE CERTIFICATE (AFSKRIFT)

Udgået

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FIS NATO) (AFSKRIFT)

FACILITY SECURITY CELARANCE INFORMATION SHEET (FIS)

REQUEST

- Please ☐ provide a FSC assurance of the facility listed below.
☐ start initiating a FSC up to and including the level of ... if the facility does not hold a current FSC.
☐ confirm the FSC up to and including the level of ... as provided on (ddmmyy)
☒ provide the correct and complete information, if applicable.

1. Full facility name : / Corrections/additions :
 2. Full facility address : /
 3. Mailing address (if different from 2) /
 4. Zip code/city/country : /
 5. Name of the security officer (optional) : /
 6. The request is made for the following reason(s):
(indicate particulars of the precontractual stage, contract, sub-contract, programme/project)
.....
.....
.....
- Requesting NSA/DSA** Name: Date:

REPLY

1. This is to inform you that the above mentioned facility :
☐ holds a FSC up to and including the level of: ☐ S ☐ NS ☐ C ☐ NC
☐ does not hold a FSC.
☐ does not hold a FSC, but, on your above mentioned request, the FSC is in progress. You will be informed when the FSC has been established.
Expected date ../. (mm/yy). (if known)
 2. Safeguarding of classified documents: ☐ yes, level : .. ☐ no.
Safeguarding of classified material: ☐ yes, level : .. ☐ no.
 3. This FSC certification expires on : (ddmmyy).
In case of an earlier invalidation or in case of any change of the information listed above, you will be informed.
 4. Should any contract be let or classified information be transferred in relation to this certification, please inform us on all relevant data including security classification.
 5. Remarks :
.....
.....
- Issuing NSA/DSA** Name: Date:

Kapitel 9**RISIKOSTYRING**

Indhold	Kapitel 9.....	1
	RISIKOSTYRING	1
	1. INDLEDNING	2
	2. FORMÅL	2
	3. OVERORDNET STYRING AF DEN MILITÆRE SIKKERHED.....	2
	4. RISIKOVURDERING	4
	5. SIKKERHEDSINSTRUKSER	4
	5.1. Generel sikkerhedsinstruks	4
	6. SIKRINGSPLANEN	5
	7. NØDFALDS-OG KATASTROFEPLANER	5
	8. KOORDINATION	5
	9. KONTROL- OG OVERVÅGNING	5
	9.1. Intern kontrol	6
	9.2. Risikolog	6
	9.3. Ekstern kontrol.....	7
	9.3.1 Generelle sikkerhedseftersyn	7
	9.3.2 Fritagelse for generelle sikkerhedseftersyn	8
	9.3.3 Eftersynsprogram.....	8
	9.3.4 Særlige sikkerhedseftersyn.....	8
	9.3.5 Tekniske sikkerhedseftersyn	8
	9.3.6 Forsvarets IT-systemer uden for koncernområdet.....	8
	9.3.7 COSMIC og ATOMAL sikkerhedseftersyn	9
	9.3.8 US ATOMAL SURVEY.....	9
	9.3.9 NATO sikkerhedsinspektion.....	9
	9.3.10 EU sikkerhedsinspektion	9
	9.4. Rapportering	9
	9.4.1 Generelle sikkerhedseftersyn	9
	10. ÅRSRAPPORT OVER SIKKERHEDSTILSTANDEN INDEN FOR FORSVARSMINISTERIETS OMRÅDE	9
	10.1. Forsvarsministeriet og dets styrelser, stabe og myndigheder	9
	10.2. Forsvarets Efterretningstjeneste.....	9
	10.3. Forsvarskommandoen	10

Bilag:

1. Vejledning til udarbejdelse af risikovurdering
2. Vejledning til udarbejdelse af sikkerhedsinstruks
3. Eksempel på forretningsorden for koordinationsudvalg vedrørende militær sikkerhed
4. Vejledning til indhold af rapport vedrørende generelt sikkerhedseftersyn

1. INDLEDNING

Risikostyring er en optimeringsproces, hvor sikkerhedsmiljøet kontinuerligt tilpasses myndighedens aktiver i forhold til truslerne således, at chefen netop kan acceptere risikoen. Risikostyringsprocessen skal ske i samspil med udvikling, drift og økonomi, så der opnås helhedsløsninger. Risikostyring er således ikke i sig selv et mål men et middel til at opnå mål inden for den militære sikkerhed.

Risikostyring er baseret på en systematik, hvori indgår kontinuerlig overvågning og kontrol af alle faktorer af betydning for den militære sikkerhed samt navnlig ændringer, der relaterer sig til trusler, aktiver og sikkerhedsmiljøet.

I Forsvarsministeriets koncern gennemføres risikostyring i sammenhæng med fastsatte minimumskrav til sikkerheden (basissikkerheden), som beskrevet i øvrige kapitler i denne bestemmelse. Væsentlige dokumenter til styring af den militære sikkerhed er risikovurderinger, sikkerhedsinstruktioner, sikkerhedskravsspecifikationer, sikringsplaner, kryptoplaner, nødfalds- og katastrofeplaner samt vagtinstruktioner. Kontrakter med bl.a. civile leverandører af sikkerhedsydelser samt lokale koordinerende retningslinjer myndighederne imellem indgår ligeledes i styringen af sikkerheden.

Risikovurderingen er dimensionerende for det sikkerhedsmiljø, der skal etableres, idet der i denne foretages en afvejning af konstaterede risici.

2. FORMÅL

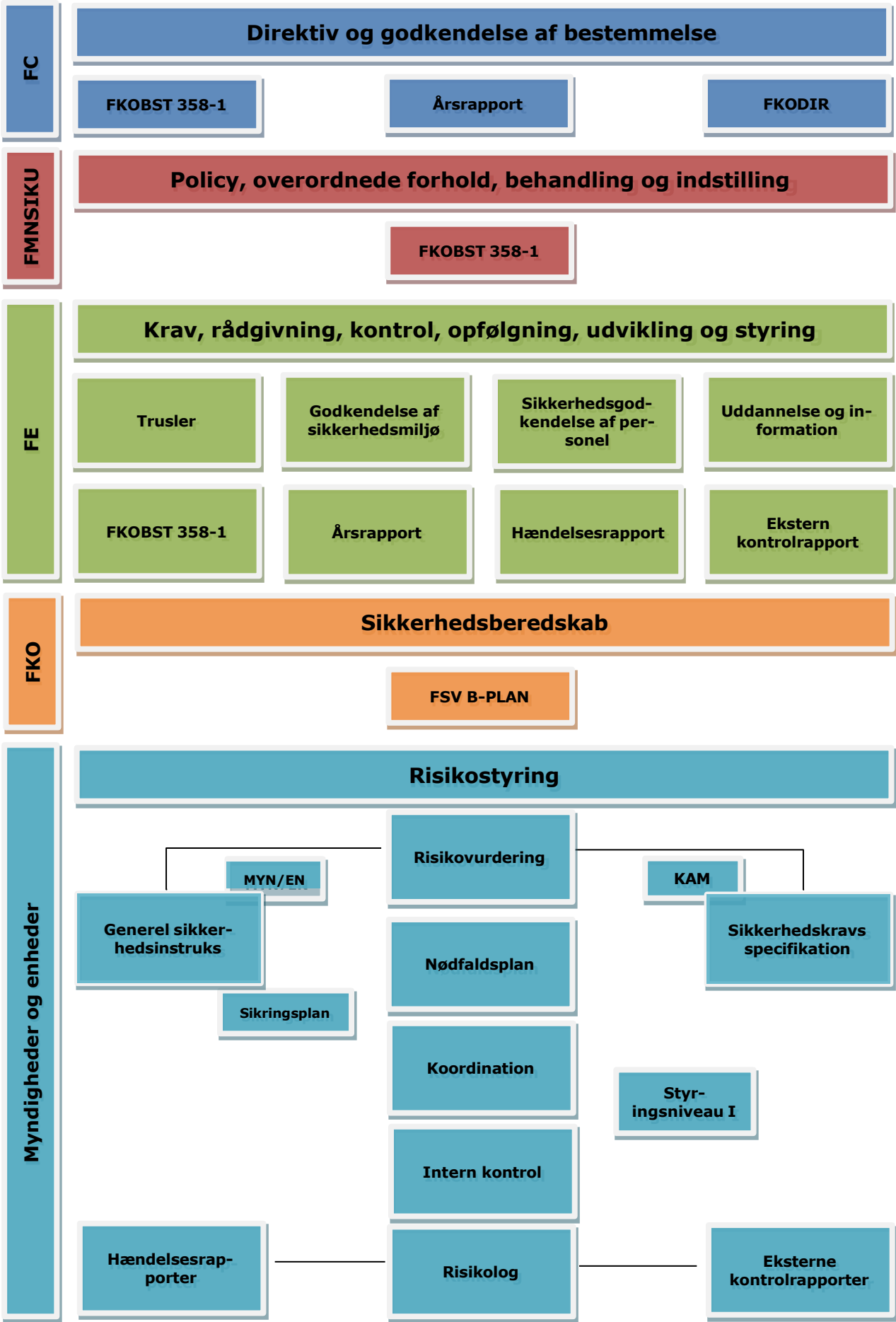
Formålet med dette kapitel er at beskrive, hvordan risikostyring gennemføres i praksis inden for militær sikkerhed, herunder med en detaljeret vejledning i gennemførelse af risikovurderinger, udarbejdelse af sikkerhedsinstruktioner samt gennemførelse af kontrol- og overvågningsaktiviteter.

Risikostyring på informationssikkerhedsområdet skal ske i henhold til bestemmelserne i FMNBST 358-1 om informationssikkerhedsledelse og FMNBST 358-2 om risikostyring inden for informationssikkerhed.

Der skal ske en koordination af risikostyringen på områderne militær sikkerhed og informationssikkerhed. Det bør særligt ske i forhold til vurdering og implementering af konkrete sikkerhedsforanstaltninger i sikkerhedsmiljøet med henblik på en tilstrækkelig og effektiv beskyttelse af myndighedernes aktiver.

3. OVERORDNET STYRING AF DEN MILITÆRE SIKKERHED

Det overordnede styringsprincip for den militære sikkerhed er risikostyring under overholdelse af minimumskrav. I figur 9-1 er vist, hvorledes den overordnede styring af den militære sikkerhedstjeneste finder sted.



Figur 9- 1

Af figur 9-1 fremgår det, at Forsvarschefen (FC) udgiver et direktiv for ledelse af den militære sikkerhedstjeneste. FC godkender desuden bestemmelser og udgiver årligt en rapport over den militære sikkerhedstilstand inden for koncernen.

Forsvarsministeriets Sikkerhedsudvalg (FMNSIKU) behandler FE's forslag til revision af FKOBST 358-1.

FE leder og kontrollerer den militære sikkerhedstjeneste, og gennemfører herunder udvikling af området med løbende ajourføring af FKOBST 358-1. Denne bestemmelse beskriver minimumskravene til den militære sikkerhedstjeneste. FE udarbejder trusselslister/vurderinger til brug for myndighedernes gennemførelse af risikovurderinger, og FKO iværksættelse af sikkerhedsberedskabsforanstaltninger, jf. FKO PLAN P 120-1. FE er koncernens sikkerhedsmyndighed, og godkender som sådan sikkerhedsmiljøer og koncernens personel. Desuden gennemfører FE sikkerhedsuddannelse og informationsvirksomhed.

På baggrund af FE's trusselsvurderinger iværksætter FKO sikkerhedsberedskabsforanstaltninger i henhold til FKOBST O.120-1. Sikkerhedsberedskabet er en overbygning på den basissikkerhed (minimumskrav), der er fastlagt i FKOBST 358-1.

Den militære sikkerhed styres på alle myndigheds- og ansvarsniveauer på baggrund af konkrete risikovurderinger. Disse danner basis for udarbejdelse af sikkerhedsinstrukser, sikringsplaner samt katastrofe- og eller nødfaldsplaner. Gennemførelse af såvel ekstern som intern kontrol samt rapportering af hændelser sker på alle niveauer og indgår som et væsentligt grundlag for styring samt FE's udvikling af den militære sikkerhedstjeneste.

4. RISIKOVURDERING

Risikovurderinger gennemføres systematisk, struktureret og på en standardiseret måde. Systematikken og strukturen skal synliggøre sammenhængene mellem årsager og virkninger. Den skal begrundes de valgte sikkerhedsløsninger således, at risici kan accepteres på et oplyst grundlag og fremadrettet styres og koordineres.

Risikovurderinger udarbejdes på alle niveauer i koncernen, idet de skaber forudsætningerne for etablering og drift af sikkerhedsmiljøer.

Risikovurderinger skal indgå som en integreret del af bygge- og anlægsprojekter og forskellige former for materielanskaffelsesprojekter, herunder informations- og kommunikationssystemer. Der tænkes i den forbindelse ikke på identifikation af risici i fm. projektets gennemførelse, men på afdækning af risici i forhold til den militære sikkerhed. Risikovurderinger kan ligeledes med fordel anvendes i fm. planlægning af operationer, hvori der i de fleste tilfælde foretages afvejning af forskellige former for risici, hvoraf nogle relaterer sig til den del af operationssikkerheden, der vedrører militær sikkerhed. Minimumskrav til sikkerhedsforanstaltninger skal efterleves uagtet risikovurderinger.

Vejledning til udarbejdelse af en risikovurdering fremgår af bilag 1. Denne vejledning er udarbejdet på baggrund af almindelig anerkendte principper for risikostyring. Om risikovurdering inden for informationssikkerhed se FMNBST 358-2.

5. SIKKERHEDSINSTRUKSER

5.1. Generel sikkerhedsinstruks

Det påhviler chefen (lederen, direktøren mfl.) at udgive en generel sikkerhedsinstruks dækkende eget myndighedsområde og omfattende alle relevante dele af sikkerhedstjenesten, dog med undtagelse af informationssikkerheden. Krav til instrukser på informationssikkerhedsområdet fremgår af kapitel 6. Retningslinjerne, som anført neden for, kan anvendes såvel nationalt som i fm. planlægning og gennemførelse af sikkerheden under internationale operationer.

Indholdet af sikkerhedsinstruksen er helt afhængig af myndighedens eller enhedens opgaveportefølje (kerneydelse) og resultatet af risikovurderingen. Kun relevante områder medtages, og der skal lægges vægt på at beskrive lokale sikkerhedsregler og -procedurer, herunder hvem der gør hvad inden for den militære sikkerhedstjenestes delområder. Hvor det er åbenlyst, at enheden ikke er i besiddelse af aktiver, der på nogen måde kræver sikkerhedsbeskyttelse, kan sikkerhedsinstruksen udarbejdes direkte uden forudgående risikovurdering. På de fleste etablissementer vil der være behov

for at koordinere indholdet af sikkerhedsinstrukserne for de myndigheder eller enheder, der er på tjenestestedet.

Sikkerhedsinstruksen skal være konkret, kortfattet og kendt af alt personel ved myndigheden eller enheden. Den skal således være let tilgængelig, fx på FIIN eller andet lokalt it-netværk. Sikkerhedsinstruksen udgør et væsentligt grundlag for tilrettelæggelse af den militære sikkerhedsuddannelse/instruktion.

Klassifikation af sikkerhedsinstruksen som helhed bør ikke være højere end TIL TJENESTEBRUG. Bilag med sikringsplan kan klassificeres højere.

Vejledning til udarbejdelse af en sikkerhedsinstruks fremgår af bilag 2.

6. SIKRINGSPLANEN

Sikringsplanen udarbejdes på baggrund af risikovurderingen. Den skal beskrive det fysiske sikkerhedsmiljøes opbygning og virkemåde. Sikringsplanen skal som minimum indeholde en områdekategorisering af arealer, bygninger og rum samt fastlæggelse af sikringsniveauer for aktiver, herunder mekanisk sikring og elektronisk overvågning. Desuden skal krav til bevogtning eller tidskrav for indsættelse af regional eller lokal indsatsstyrke fastlægges. Sidstnævnte er i mange tilfælde styrende for dimensionering af den mekaniske sikring, idet en længere indsatstid kan betyde, at genombrydningstiden for den mekaniske sikring må forøges.

Forhold vedr. adgangskontrol og adgangskontrolanlæg bør ligeledes indgå i sikringsplanen.

På de fleste etableringer vil der være behov for tæt koordination mellem de placerede enheder om udarbejdelse og vedligeholdelse af sikringsplaner, idet der i disse beskrives forhold af fælles betydning for sikkerhedsmiljøet, fx elektronisk overvågning, adgangskontrol og bevogtning.

Planen klassificeres efter indhold og fordeles snævert til relevant personel.

Vejledning for udarbejdelse af en sikringsplan fremgår af bilag 2 pkt. 7.

7. NØDFALDS- OG KATASTROFEPLANER

Disse planer udarbejdes for aktiver, der kan udsættes for trusler, hvortil der er knyttet en meget lav sandsynlighed, men en meget stor konsekvens hvis truslerne faktisk virker, og hvor det vil være forbundet med et uforholdsmæssigt stort ressourceforbrug, eller hvor det vil være teknisk eller på anden måde umuligt at etablere beskyttelsesforanstaltninger. På nationale etableringer kan det fx være evakueringsplaner for højt klassificerede dokumenter og/eller materielgenstande i tilfælde af fx brand, oversvømmelse og lign. For kryptomateriel (CCI) og kryptomaterialer gælder særlige regler jf. DAMSG 205, idet der for dette skal udarbejdes nødfaldsforanstaltninger, såvel nationalt som i internationale missionsområder. Nødfalds- og katastrofeplaner indgår normalt som bilag til sikkerhedsinstruksen. Planerne skal være let tilgængelige, og kendt af det personel, der skal bringe dem til udførelse.

8. KOORDINATION

På etableringer, hvor flere myndigheder og enheder er placeret, vil der normalt være behov for at koordinere den militære sikkerhed på stedet og evt. områder uden for etableringen, men med tilknytning til dette. Koordinationen skal medvirke til, at det samlede sikkerhedsmiljø er afstemt efter trusler og aktiver, og at der opnås synergieffekt med bedst mulig udnyttelse af ressourcerne. Chefen for den enkelte myndighed eller enhed er risikoejer, og skal således styre sikkerheden inden for eget område. Det er imidlertid væsentligt, at sikkerheden ved den enkelte myndighed ikke udmøntes i isolerede siloer, men understøtter den samlede sikkerhed på stedet. Som det fremgår af kapitel 1, vil der på mange af koncernens etableringer være udpeget en chef, der har ansvaret for, at denne koordination finder sted. For at opnå den ønskede effekt, skal koordinationen ske løbende og være struktureret. I bilag 3 er der vist et eksempel på en forretningsorden for det udvalg, benævnt "Koordinationsudvalg vedrørende militær sikkerhed" (KUVMILSIK), der varetager koordinationssopgaven. I bilaget er der desuden anført et antal områder, som skal koordineres, idet de normalt vil være af fælles betydning for de myndigheder og enheder, der er placeret på tjenestestedet. Principielt kan alle delområder af den militære sikkerhed behandles i udvalget.

9. KONTROL- OG OVERVÅGNING

Brud på den militære sikkerhedstjeneste kan få alvorlige konsekvenser, ikke blot internt i koncernen, men også for myndigheder eller enkeltpersoner i den øvrige del af samfundet. Det er derfor

væsentligt, at brud eller tilløb til brud konstateres så tidligt som muligt. Løbende kontrolvirksomhed på alle niveauer er således et vigtigt middel til at forebygge, at koncernens aktiver udsættes for uacceptable risici.

Kontrol af den militære sikkerhedstjeneste gennemføres dels som intern kontrol dels som ekstern kontrol.

Se kravene i FMNBST 358-1 om informationssikkerhedsledelse, hvad angår intern kontrol (egen- kontrol) og ekstern kontrol på informationssikkerhedsområdet.

Dele af kontrol- og overvågningsvirksomheden kan være automatiseret og foregå kontinuerligt.

De uregelmæssigheder eller svagheder, der ved kontrol afdækkes i sikkerhedsmiljøet, skal registreres, dokumenteres, rapporteres og korrigeres hurtigst muligt, evt. ved en fornyet (delvis) risikovurdering.

9.1. Intern kontrol

Intern kontrol knytter sig til chefansvaret på alle niveauer. Kontrollen skal gennemføres inden for relevante delområder af den militære sikkerhedstjeneste.

Kontrollen gennemføres normalt af myndighedens/enhedens sikkerhedsorganisation. Intern kontrol gennemføres på følgende måder:

- Som et samlet eftersyn mindst en gang om året af de væsentligste dele af den militære sikkerhed eller
- som en proces, hvor den militære sikkerhedstjenestes delområder kontrolleres enkeltvis i løbet af et år og
- som en kontrolforanstaltning efter sikkerhedsbrud eller formodning herom.

Ved tilrettelæggelse af den interne kontrol skal der lægges vægt på følgende områder:

- Sikkerhedsforståelse
- Opbevaring af våben, ammunition, eksplosivstoffer og andet vitalt materiel
- Opbevaring af kryptoudstyr og andet højt klassificeret IT-udstyr
- Opfølgning på udbedring af konstaterede fejl og mangler i sikkerhedsmiljøet
- Sikkerhedsgodkendelser og bemyndigelser for personalet
- Opdatering af risikovurdering, sikkerhedsinstrukser og sikringsplan
- Opbevaring, sanering og mønstring af højt klassificerede dokumenter og lagermedier
- Opbevaring og mønstring af sikkerhedsbetydende nøgler
- Omstilling af koder til opbevaringsmidler, ADK-anlæg mv.
- Overholdelse af indsattider for reaktionsstyrke.

Gennemført intern kontrol skal dokumenteres og kunne forevises ved generelle sikkerhedseftersyn. Dokumentation skal således opbevares ved myndigheden i mindst 5 år.

Skema til brug for intern kontrol findes i den elektroniske udgave af FKOBST 358-1 under bogmærke, "links til skrivbare skabeloner". Skemaet kan tilpasses efter behov.

9.2. Risikolog

Som et led i kontrol- og overvågningsvirksomheden skal der ved alle myndigheder og enheder, der er i besiddelse af aktiver, der fordrer sikkerhedsbeskyttelse, oprettes en risikolog. I risikologgen føres en oversigt over de fejl og mangler, der er konstateret ved intern- eller ekstern kontrol. Desuden anvendes risikologgen til registrering af sikkerhedsbrud og relevante hændelser. "Nærværende hændelser" bør også medtages, i det omfang disse kan eller skal anvendes i det forebyggende arbejde. Risikologgen er således et centralt dokument til styring af sikkerhedsmiljøets styrke gennem systematisk opfølgning på konstaterede fejl og mangler samt andre sikkerhedsbrud. Desuden kan risikologgen danne grundlag for statusrapportering til foresat myndighed, serviceleverandører og sikkerhedsmyndigheden (FE) vedr. militær sikkerhed. Eksempel på en risikolog fremgår af figuren herunder. Den viste risikolog findes som en skrivbar skabelon i den elektroniske udgave af FKOBST 358-1 under bogmærke "links til skrivbare skabeloner".

Intern kontrol

A	B	C	D	E	F
Lb.Nr.	Delområde	Beskrivelse af observation/risiko (når, hvad, hvor, hvorledes)	Beskrivelse af modforanstaltninger	Ansvar	Status og opfølgning
1	Personelsikkerhed	12 marts 2010. Har ved gennemgang af DeMars rapport ZPTC132 konstateret, at der i 29 forhold er uoverensstemmelse mellem funktionsbeskrivelses- og stillingshaverens sikkerhedsgodkendelsesklassifikation	23 marts 2010. Oplysningsskemaer modtaget fra alle 29. Disse er d.d. sendt til FE.	CH/A	22 maj 2010. Afventer stadig svar fra FE. FE rykket d.d. 01 juli 2010. Samtlige personer er meddelt godkendelser som ansøgt. CH/A orienteret. Sagen lukket
2					
3					
4					
5					
6					

Ekstern kontrol

A	B	C	D	E	F
Lb.Nr.	Delområde	Konstatering/risiko (når, hvad, hvor, hvorledes)	Beskrivelse af modforanstaltninger	Ansvar	Status og opfølgning
1	Fysisk sikkerhed	07 NOV 2010. Dør til våbenkammer i byg. 12 er ikke monteret med sikkerhedsgodkendt lås. Mangler nøk i bagkant. Risiko: HØJ	15 NOV 2010. Ny lås bestilt via LSE. Forventet levering 10. DEC. Ny dør og karm bestilt ved LSE. Forventet levering ikke oplyst. Samtlige våben flyttet til våbenkammer i byg. 18.	SIKOF	Ikke afsluttet
2					
3					
4					
5					
6					

Hændelser

A	B	C	D	E	F
Lb.Nr.	Delområde	Hændelse/risiko (når, hvad, hvor, hvorledes)	Beskrivelse af modforanstaltninger	Ansvar	Status og opfølgning
1	Informationssikkerhed	18 JUN 2010. Kaptajn Niels Nielsen melder at han, under tjenesterejse til Belgien, har mistet kryptokort til sin FAP (TTJ). Ingen risiko	18 JUN 2010. tabet meddelt til FKIT. Kryptokortet spærret.	KRYSOF	19 JUN 2010 Kaptajn Niels Nielsen orienteret om hændelsens udfald. Sagen afsluttet
2					
3					
4					
5					
6					
7					
8					

Figur 9- 2

9.3. Ekstern kontrol

Den del af kontrolvirksomheden, der gennemføres af foresatte eller andre myndigheder, betegnes "ekstern kontrol". Kontrollen gennemføres normalt i form af generelle sikkerhedseftersyn, hvor alle delområder af den militære sikkerhedstjeneste undtagen informationssikkerheden kontrolleres, dog tilpasset myndighedens opgaveportefølje. Kontrollen dokumenteres ved udfærdigelse af eftersynsrapporter.

9.3.1 Generelle sikkerhedseftersyn

Generelle sikkerhedseftersyn omfatter kontrol af den samlede militære sikkerhed ved en myndighed eller enhed. Eftersynet omfatter således organisatoriske forhold, uddannelse og en konkret vurdering af den samlede sikkerhedsmiljø styrke og svagheder. Endvidere vil der efter omstændighederne kunne udføres stikprøvekontrol hvad angår indholdet på pc'er udleveret af forsvaret i overensstemmelse med gældende lovgivning.

Generelle sikkerhedseftersyn gennemføres normalt en gang hvert tredje år.

FE gennemfører generelle sikkerhedseftersyn ved Forsvarsministeriets departement, styrelserne og som minimum de til styrelserne direkte underliggende myndigheder.

Følgende myndigheder gennemfører sikkerhedseftersyn ved egne underlagte myndigheder og enheder:

- Hjemmeværnskommandoen
- Forsvarskommandoen
- Forsvarskommandoen – Hærkommandoen
- Forsvarskommandoen – Søværnskommandoen

- Forsvarskommandoen – Flyverkommandoen
- Forsvarskommandoen – Arktisk Kommando
- Forsvarskommandoen – Specialoperationskommandoen
- Forsvarsministeriets Ejendomsstyrelse
- Forsvarsministeriets Materiel- og Indkøbsstyrelse
- Forsvarets Sanitetskommando
- Forsvarsministeriets Personalestyrelse
- Forsvarets Vedligeholdelsestjeneste
- Beredskabsstyrelsen
- Forsvarsakademiet.

I det omfang det findes formålstjenligt, kan der indgås aftaler om at efterse andre myndigheders underlagte enheder eller elementer. Disse aftaler skal i så fald fremgå af den til FE fremsendte oversigt over planlagte sikkerhedseftersyn

9.3.2 Fritagelse for generelle sikkerhedseftersyn

Myndigheder, der er pålagt at gennemføre generelle sikkerhedseftersyn, kan beslutte, at en enhed eller et element på eget myndighedsområde fritages helt eller delvis for generelle sikkerhedseftersyn, hvis der ved pågældende enhed/element, efter tilsynsmyndighedens vurdering, hverken opbevares materiale klassificeret FORTROLIGT eller højere, vitale og/eller sensitive aktiver (fx våben, ammunition, eksplosivstoffer og vanedannende medicin). En fritagelse herfor udelukker ikke, at der kan ske eftersyn af informationssikkerheden.

Enheder/elementer, der ønsker fritagelse for generelle sikkerhedseftersyn, skal årligt inden 31. oktober udfylde og fremsende et oplysningsskema til den eftersynsansvarlige myndighed. Oplysningsskemaet underskrives af chefen/lederen for pågældende enhed/element.

Oplysningsskema i forbindelse med fritagelse for generelle sikkerhedseftersyn findes i den elektroniske udgave af FKOBST 358-1 under bogmærke "links til skrivbare skabeloner".

Hvis der opstår ændringer i forhold til ovenstående, der kræver opbevaring af materialer (dokumenter, materiel m.v.) i sikrede områder, skal foresatte og den eftersynsansvarlige myndighed straks underrettes.

Ved den eftersynsansvarlige myndigheds fremsendelse af eftersynsprogrammet, jf. pkt. 9.3.2, for det efterfølgende år, skal det fremgå hvilke enheder/elementer, der er fritaget for generelle sikkerhedseftersyn.

9.3.3 Eftersynsprogram

Myndigheder, der gennemfører generelle sikkerhedseftersyn, skal inden 1. november sende en oversigt til FE over hvilke myndigheder/enheder, der planlægges eftersat de kommende tre år.

FE udsender inden 1. december et samlet eftersynsprogram for det kommende år.

9.3.4 Særlige sikkerhedseftersyn

Særlige sikkerhedseftersyn omfatter kontrol af specifikke dele af sikkerhedsmiljøet. De kan udføres efter behov af foresat myndighed. Særlige sikkerhedseftersyn gennemføres normalt kun inden for eget myndighedsområde. FE kan dog gennemføre særlige sikkerhedseftersyn på alle niveauer inden for koncernen.

9.3.5 Tekniske sikkerhedseftersyn

Tekniske sikkerhedseftersyn (TSE) omfatter teknisk kontrol af bygninger, lokaler og områder, hvori der skal installeres højt klassificeret udstyr eller gennemføres højt klassificerede briefinger o. lign. Tilsvarende eftersyn kan foretages på køretøjer, skibe og fly. TSE udføres af FE og rekvireres ved skrivelse klassificeret FTR (se kapitel 6, bilag 3).

9.3.6 Forsvarets IT-systemer uden for koncernområdet

Sikkerhedseftersyn af Forsvarets klassificerede IT-systemer, der er placeret ved myndigheder uden for koncernområdet, omfatter kontrol af at systemerne forvaltes i overensstemmelse med forsvarets militære sikkerhedsbestemmelser. Sikkerhedseftersynene, der udføres af FE mindst én gang hvert andet år, gennemføres som særlige sikkerhedseftersyn og omfatter såvel specifikke forhold vedrørende informationssikkerhed samt personel-, dokument- og fysisk sikkerhed.

9.3.7 COSMIC og ATOMAL sikkerhedseftersyn

COSMIC og ATOMAL sikkerhedseftersyn omfatter kontrol med disse materials tilstedeværelse, opbevaring og behandling. De udføres af FE ved myndigheder, der har COSMIC- og/eller ATOMAL registraturer og underregistraturer, efter en 24 måneders cyklus iht. gældende NATO-/nationale bestemmelser.

9.3.8 US ATOMAL SURVEY

Gennemføres lejlighedsvis af US Department of Energy og Department of Defense i Danmark, hvor ATOMAL registraturer og underregistraturer er oprettet.

9.3.9 NATO sikkerhedsinspektion

NATO Office of Security gennemfører sikkerhedsinspektion efter en 24 mdr. cyklus ved myndigheder, hvor COSMIC og ATOMAL registratur og underregistraturer er oprettet, samt ved myndigheder, hvor materiale (dokumenter) klassificeret NS modtages, behandles og opbevares.

9.3.10 EU sikkerhedsinspektion

Gennemføres af EU Security Office of the Council ved myndigheder i Danmark, herunder Forsvarsministeriet med tilhørende myndigheder og institutioner.

9.4. Rapportering

9.4.1 Generelle sikkerhedseftersyn

Efter gennemførelse af generelle sikkerhedseftersyn udfærdiger den kontrollerende myndighed en samlet rapport iht. bilag 4.

Rapporten skal give en aktuel status for sikkerheden, herunder konstaterede mangler og uregelmæssigheder ved sikkerhedsmiljøet. Der skal desuden gives anvisning på afhjælpning af disse. Rapporten tilsendes den/de kontrollerede myndighed(er), foresatte myndighed og FE inden 30 dage efter gennemførelse af eftersynet. Desuden sendes rapporten til de myndigheder der, ud over den eftersete myndighed, i rapporten er anført som ansvarlig for afhjælpning af mangler og uregelmæssigheder. På baggrund af rapporten udarbejder den kontrollerede myndighed og myndigheder, der i rapporten i øvrigt er anført som ansvarlig for afhjælpning af mangler og uregelmæssigheder, en kort redegørelse med plan for afhjælpning af disse.

Redegørelsen sendes til den kontrollerende myndighed og FE senest 45 dage efter modtagelse af eftersynsrapporten. Myndigheder der, ud over den kontrollerede myndighed, i rapporten er anført som ansvarlig for afhjælpning af mangler og uregelmæssigheder, sender sin redegørelse til den eftersete myndighed inden 45 dage.

Kontrolskema til brug for gennemførelse af generelle sikkerhedseftersyn findes i den elektroniske udgave af FKOBST 358-1 under bogmærke "link til skrivbare skabeloner" (Rapport vedrørende generelt sikkerhedseftersyn / intern kontrol). Kontrolskemaet kan tilpasses efter behov, og udgør samtidig grundlaget for eftersynsrapporten.

10. ÅRSRAPPORT OVER SIKKERHEDSTILSTANDEN INDEN FOR FORSVARSMINISTERIETS OMRÅDE

10.1. Forsvarsministeriet og dets styrelser, stabe og myndigheder

Forsvarsministeriet og dets styrelser, stabe og myndigheder udarbejder årligt en "Årsoversigt over Sikkerhedstilstanden" inden for eget myndighedsområde omfattende forhold, der har haft indflydelse på den militære sikkerhedstjeneste.

Årsoversigten udarbejdes bl.a. på grundlag af gennemførte sikkerhedseftersyn, eftersynsrapporter, intern kontrol samt konstaterede sikkerhedsbrud jf. risikologgen.

FE udsender indkaldelse af årsoversigter senest i oktober måned samme år som årsoversigten dækker. Indhold og opstilling af årsoversigten fremgår af den skabelon, der henvises til i FE's skrivelse.

Årsoversigten sendes senest 31. januar til FE for året forud.

10.2. Forsvarets Efterretningstjeneste

FE udarbejder "Årsrapport over sikkerhedstilstanden inden for Forsvarsministeriets område" på grundlag af egne gennemførte sikkerhedseftersyn og årsoversigter fra koncernens styrelser og myndigheder. Rapporten sendes inden udgangen af april til forsvarschefen, der efterfølgende udsender til koncernens styrelser og myndigheder.

10.3. Forsvarskommandoen

FKO udsender på vegne af FC "Årsrapport over sikkerhedstilstanden inden for Forsvarsministeriets område".

Bilag 1 til kapitel 9. Vejledning til udarbejdelse af risikovurdering.

Underbilag:

1. Definitioner, terminologi og forkortelser

1. INTRODUKTION TIL RISIKOVURDERING

Risikovurderinger gennemføres systematisk, struktureret og på en standardiseret måde.

Denne vejledning beskriver denne systematik. Ordforklaring fremgår af underbilag 1. Til vejledningen er knyttet et antal skemaer, der alle findes i en skrivbar version i den elektroniske version af FKOBST 358-1 under bogmærke "link til skrivbare skabeloner".

Risikovurderinger gennemføres normalt af SIKOF og/eller ISO. Det er imidlertid vigtigt, at personel med et godt overblik over og indsigt i myndighedens eller enhedens opgaver, ydelser og aktiver deltager i processen som specialister inden for relevante områder. Afhængig af risikovurderingens rammer og omfang, bør der tillige inddrages repræsentanter fra de funktionelle tjenester og andre serviceleverandører inden for det relevante område.

Risikovurderinger kan principielt gennemføres i to trin. I første trin gennemføres en sikkerhedsmæssig overvejelse uden ressourcekrævende kvalitative eller statistiske analyser. Der foretages en overordnet vurdering af risikobilledet ved en kombination af vurdering og enkel analyse. I andet trin gennemføres en detaljeret analyse af de områder, der i trin 1 har afdækket kritiske områder. Altså aktiver, hvortil der er identificeret en uacceptabel høj eller meget usikker risiko. Dette kan navnlig være tilfældet ved udarbejdelse af risikovurderinger for nye etableringer, nye informationssystemer og kritiske operationer eller processer samt i tilfælde, hvor ikke hidtil anvendte beskyttelsesforanstaltninger forventes implementeret.

Ved at anvende det regneark (Excel) og udarbejde de bilag, der er beskrevet i risikovurderingens faser, vil der kunne opnås sammenhæng og overblik. Dette er en forudsætning for, at risikostyring, herunder løbende optimering af sikkerhedsmiljøet, kan finde sted under anvendelse af færrest mulige ressourcer.

2. BESKRIVELSE AF FASERNE I RISIKOVURDERINGEN

Udarbejdelse eller ajourføring af en risikovurdering sker som gennemløb af en cyklus, der består af 9 faser som vist i figur 9-1-1.

Overordnet set gennemføres faserne med henblik på besvarelse af følgende tre hovedspørgsmål:

- Hvilke aktiver skal beskyttes?
- Hvad skal aktiverne beskyttes imod?
- Hvor godt og hvordan skal aktiverne beskyttes?

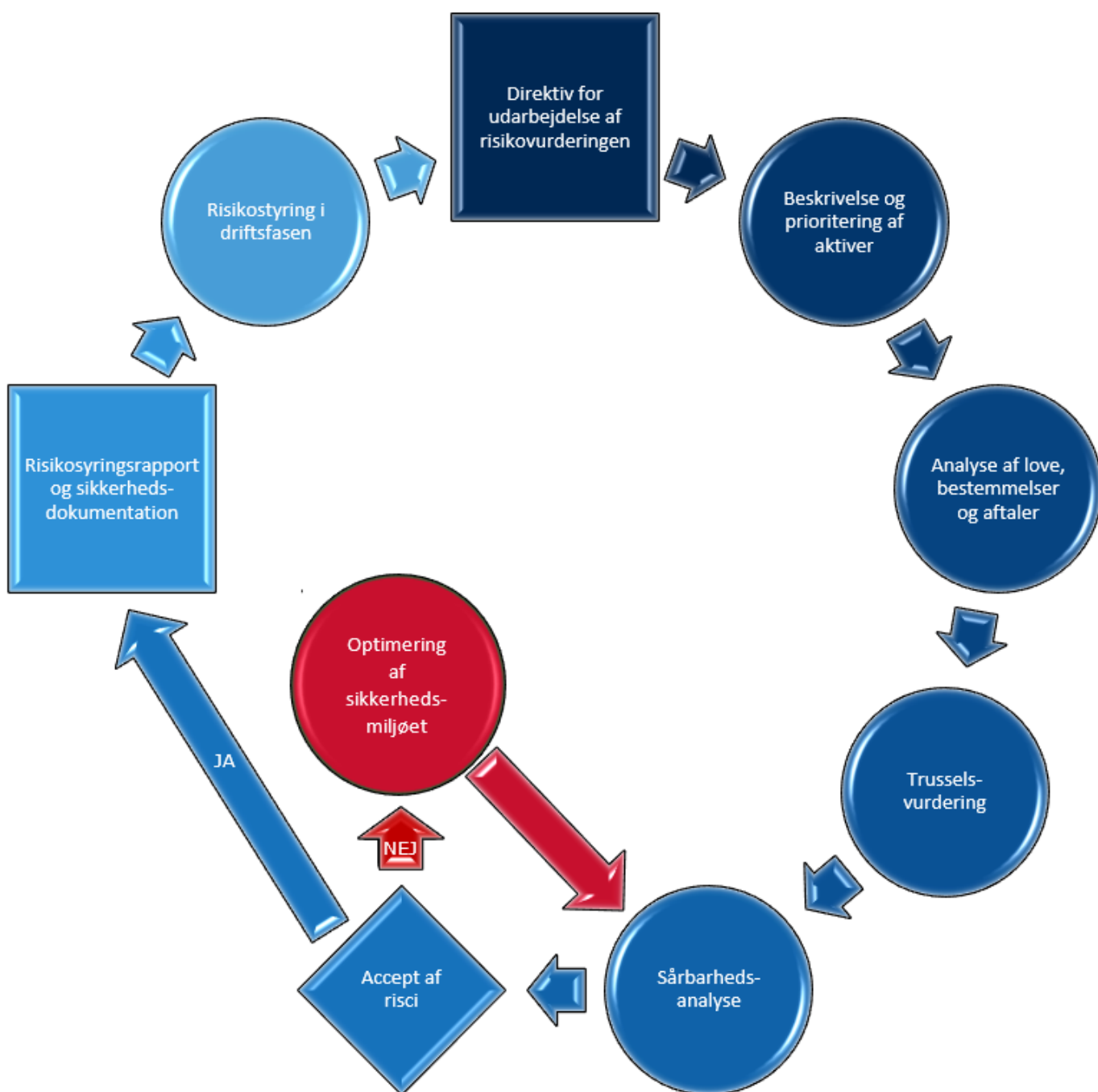


Fig. 9-1-1

Som nævnt ovenfor, anvendes et regneark for at skabe struktur, sammenhæng og overblik over aktiverne, truslerne og sikkerhedsmiljøet. Regnearket har et antal faneblade til brug i de forskellige faser i risikovurderingen. Det findes som en skrivbar skabelon i den elektroniske udgave af FKOBST 358-1 under bogmærke "links til skrivbare skabeloner".

I det følgende beskrives faserne mere detaljeret.

3. FASE 1, DIREKTIV FOR UDARBEJDELSE AF RISIKOVURDERING.

I denne fase fastlægges rammerne for risikovurderingen. Det kan dreje sig om geografisk udstrækning, koordination med sideordnede enheder, projektbeskrivelser, økonomiske forhold mv. Der skal også tages stilling til, hvilke myndigheder, herunder funktionelle tjenester og serviceleverandører, der

skal involveres i risikovurderingen. Der skal i den forbindelse lægges vægt på at afklare, hvilke roller deltagerne har i forhold til den proces, der skal finde sted.

Chefen bør så vidt muligt, i samråd med SIKOF eller ISO, gøre sig overvejelser om, hvilken risiko han er villig til at løbe eller forventer at ville acceptere.

Et eksempel herpå kan være, at chefen vil acceptere et risikoniveau for trusler vedr. tyveri af materiel på middel, men at han/hun, i en nærmere angivet periode før en enhed skal indsættes, ønsker risikoniveauet sænket til lav ved f.eks. at forstærke sikkerhedsmiljøet.

Resultatet af fase 1 er et direktiv (plan) for udarbejdelse af risikovurderingen.

4. FASE 2, BESKRIVELSER AF AKTIVER.

I denne fase kortlægges og beskrives alle de aktiver, der ligger inden for direktivets (ansvarsområdets) rammer. Beskrivelsen af et aktiv skal bl.a. indeholde oplysninger om, hvorvidt aktivet er vitalt for opgaveløsningen eller kerneydelsen, og om det er sensitivt. For begge områder vælges mellem ja eller nej (rød/grøn) i de enkelte celler i kolonnerne C og D. Se figur 9-1-2.

Liste over aktiver					
Aktiv nr.	Aktiv	Sensitivt	Vitalt	Reference	Bemærkninger
1	Shortbreak (nødgenerator for offentlig strøm)	Nej	Ja		Eftersyn v. civil leverandør en gang årligt jf. SLA zz.
2	TCE 621 X-postterminal (krypto)	Ja	Nej	DAMSL 250	HEM
3	STU II B/EASY FAX (krypto)	Ja	Ja	DAMSL 185	HEM
4	TTJ Hardware FIIN LAN (administrativt)	Nej	Ja	DAMSL 231 og zz ISI del 2	FKIT ASM
5	Personel, teknisk	Nej	Ja	Jf. godkendt SNO.	Alle skal være godkendt til HEM jf. funktionsbeskrivelser.
6	Håndvåben (30 stk)	Ja	Nej		Myndighedsbeholdning
7	Vagt- og beredskabstøj	Nej	Ja		30 min. teknisk beredskab
8	UPS til opretnet net, FIN og X-post	Nej	Ja		
9	Operative planer (rå)	Ja	Nej		Ingen af betydning for den daglige drift.
10	Brændstoflager til nødgenerator	Nej	Ja		Dieselolie fra civil leverandør
11					
12					
13					
14					
15					
16					
17					
18					

Fig. 9-1-1

I beskrivelsen af, hvor vitale aktiver er, skal der tages stilling til forhold som "single point of failure" og lavineeffekter.

"Single point of failure" kendetegner det forhold, at et svigt i tilgængeligheden for eller ødelæggelse af et aktiv, kan bringe hele enhedens opgaveløsning til standsning. Et eksempel herpå kunne være et strømsvigt for en computerbaseret operationscentral, der øjeblikkeligt bringer alle arbejdsprocesser til standsning.

Lavineeffekter forekommer, når svigt i tilgængeligheden ved eller ødelæggelse af et aktiv påvirker tilgængeligheden/anvendeligheden ved andre aktiver, der igen påvirker tilgængeligheden/anvendeligheden ved endnu andre aktiver og så fremdeles. Et eksempel herpå kan være, at køleanlægget for et computersystem svigter, hvilket bevirker, at dele af computersystemet begynder at svigte, der igen medfører, at det adgangskontrolsystem, det styrer, svigter.

Beskrivelsen af hvor sensitiv et aktiv er, indeholder oplysning om fortrolighedsforhold, og tager i de fleste tilfælde udgangspunkt i den militære klassifikation. Men også uretmæssig anvendelse og tyvetækkelighed indgår i vurderingen. I den forbindelse skal håndvåben, ammunition og eksplosivstoffer kategoriseres som havende en høj sensitivitet, idet disse materielgenstande ved misbrug kan bringe andres liv i fare og skade forsvarrets omdømme.

Til kortlægning af aktiverne anvendes regnearkets røde faneblad. figur 9-1-2.

4.1. Ordning og prioritering af aktiver.

Med henblik på at skabe overblik over aktiverne bør disse ordnes eller grupperes. Fx kan der foretages en opdeling i materiel, dokumenter, personel, infrastruktur, it-systemer osv. Dette kan være nødvendigt, når antallet af aktiver er meget stort. Aktiverne kan også prioriteres ud fra, hvor væsentlige de er i forhold til opgaveløsningen eller, hvor sensitive de er. Hvor der er tale om et begrænset antal aktiver, kan ordning og prioritering af disse ske umiddelbart.

Resultatet af fase 2 er en [prioriteret liste](#) over aktiver, bilagt evt. dokumentation over vitale forhold, identificerede "Single point of failure" og lavineeffekter. Listen skal accepteres af såvel chefen som øvrige deltagere i processen, idet den danner fundament for de øvrige faser i processen. Der er nu taget stilling til, "**hvilke aktiver skal beskyttes**".

5. FASE 3, ANALYSE AF LOVE OG BESTEMMELSERS BETYDNING FOR SIKKERHEDSMILJØET.

Med baggrund i den prioriterede liste over aktiver, undersøges det for hvert aktiv, om der i medfør af internationale eller nationale love, bestemmelser eller aftaler, herunder SLA og andre kontrakter mv., foreligger forpligtelser til at indrette sikkerhedsmiljøet efter bestemte forskrifter eller standarder. Det kan f.eks. være forpligtelsen til at efterleve NATO eller EU bestemmelser for systemer, der indeholder klassificeret NATO eller EU information, kontraktlige forpligtelser til at beskytte sensitivt materiel, arbejdsmiljøbestemmelser, fredningsforhold mv. Men det kan også være foresatte myndigheds særlige bestemmelser om foranstaltninger m.h.p. at beskytte myndighedens renommé.

Resultatet af fase 3 er en liste for hvert aktiv over referencer til forskrifter og standarder, som virksomheden er forpligtet til at følge. Listen kan vedlægges som et bilag til risikovurderingen. Alternativt anføres referencerne i listen over aktiverne.

6. FASE 4, TRUSSELSVURDERING.

Denne fase omfatter en identifikation af de trusler, der kan rettes mod aktiverne. I kapitel 1 pkt. 6.1 beskrives de generelle trusler, som trusselsvurderingen skal baseres på. Den enkelte trussel skal beskrives med en sandsynlighed for, at den virker og konsekvensen heraf, dvs. den maksimale skadelige virkning, når der ikke tages hensyn til beskyttelse af aktivet. Disse to parametre, dvs. sandsynligheden og konsekvensen, bruges til at fastlægge trusselniveauet. Truslerne beskrives og vurderes af FE bl.a. med angivelse af en generel sandsynlighed for, at de vil forekomme. Beskrivelser af trusler til brug såvel nationalt som internationalt tilvejebringes ad kommandovejen. De nationale trusler beskrives og vurderes normalt en gang om året og tilsendes concernens NIV II myndigheder af FE. Såvel sandsynlighed som konsekvens anføres med værdierne høj, middel og lav (rød, gul og grøn). Er der for en trussel anført sandsynligheden "ingen", medtages den ikke i det videre arbejde.

Truslernes sandsynlighed og konsekvensen, hvis de indvirker, indføres for hvert aktiv i regnearkets blå faneblad som vist i figur 9-1-3 under anvendelse af "drop down boxen" i den enkelte celle.

Trusselsvurdering																
2	Aktiv nr.	Aktiv	Sensitivt	Vitalt	Spionage		Sabotage		Under-gravende virksomhed		Terrorisme		Civile uroligheder		Kriminalitet	
3					San	Kon	San	Kon	San	Kon	San	Kon	San	Kon	San	Kon
4	1	Shortbreak (nødgenerator for offentlig strøm)	Nej	Ja							Middel	Middel			Høj	Middel
5	2	TCE 621 X-postterminal (krypto)	Ja	Nej	Middel	Høj					Middel	Middel			Høj	Høj
6	3	STU II B/EASY FAX (krypto)	Ja	Ja	Middel	Høj					Middel	Middel			Høj	Høj
7	4	TTJ Hardware FIIN LAN (administrativt)	Nej	Ja	Middel	Middel					Middel	Lav			Høj	Lav
8	5	Personel, teknisk	Nej	Ja	Middel	Middel			Lav	Middel	Middel	Høj			Høj	Middel
9	6	Håndvåben (30 stk)	Ja	Nej	Middel	Lav					Middel	Lav			Høj	Høj
10	7	Vagt- og beredskabskøretøjer	Nej	Ja	Middel	Lav					Middel	Middel			Høj	Middel
11	8	UPS til operativt net, FIIN og X-post	Nej	Ja	Middel	Lav					Middel	Høj			Høj	Høj
12	9	Operative planer (få)	Ja	Nej	Middel	Middel					Middel	Lav			Høj	Middel
13	10	Brændstoftager til nødgenerator	Nej	Ja							Middel	Middel			Høj	Middel
14	0	0	0	0												
15	0	0	0	0												
16	0	0	0	0												
17	0	0	0	0												
Liste over aktiver (fase2) Trusselsvurdering (fase4-1) Trusselsniveau (fase4-2) Sårbarhedsanalyse (fase5) Risikoniveau (fase5) Vejledninger																
Tegning Autofigurer																
NUM																

Fig. 9-1-2

Med henblik på at bestemme og synliggøre trusselniveauet for hvert enkelt aktiv, indføres disse i skemaerne som vist i figur 9-1-4 i regnearkets lilla faneblad.

	A	B	C	D	E	F	G	H	I	J	K	L
1	1. Trusselsniveau spionage											
2												
3												
4	Lav											
5												
6	Middel											
7												
8	Høj											
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												

Fig. 9-1-3

Der udfyldes ét skema for hver trussel, idet aktiverne anføres med deres nummer og indføres i det felt, der svarer til den i trusselslisten (blå faneblad) fastlagte sandsynlighed og konsekvens. Farverne rød, gul og grøn er et udtryk for trusselsniveauet for hvert enkelt aktiv, idet rød svarer til et højt trusselsniveau, gul svarer til middel og grøn til lav. Ved denne visualisering gives et umiddelbart billede af mulige kritiske risici.

Resultatet af fase 4 er en trusselsliste (vurdering) og et trusselsbillede for hver trussel, der viser, **"hvad aktiverne skal beskyttes imod"**.

7. FASE 5 SÅRBARHEDSSANALYSE

I denne fase gennemføres en vurdering (analyse) af, hvor sårbar myndigheden eller enheden er. Der kan her være tale om to situationer. En, hvor der allerede eksisterer et sikkerhedsmiljø, og en hvor sikkerhedsmiljøet endnu ikke er etableret eller udviklet. Sidstnævnte kan fx være tilfældet ved projektering af nye etableringer og bygninger, udvikling af informationssystemer, våbensystemer mv. I sidstnævnte situation kan sårbarhedsanalysen være meget omfattende, navnlig hvis der forventes implementeret beskyttelsesforanstaltninger, der ikke før har været anvendt, fx ny teknologi inden for it-sikkerhedsområdet eller den fysiske sikkerhed.

Grundlaget for gennemførelse af sårbarhedsanalysen er i begge tilfælde aktiverne, trusselsniveauerne og de minimumskrav til beskyttelse, der er fastsat i respektive kapitler i denne bestemmelse, fx kapitel 3 f.s.v.a. materiel.

7.1. Eksisterende sikkerhedsmiljø (version 0)

I denne situation foretages der en vurdering (analyse) af det eksisterende sikkerhedsmiljøets styrke og svagheder. Det forudsættes, at de identificerede trusler vil indvirke, og nu tages alle eksisterende beskyttelsesforanstaltninger med i betragtningerne.

Dette gøres indledningsvis ved en systematisk gennemgang af eksisterende sikkerhedsinstrukser, sikringsplaner, uddannelsesplaner og risikologgen. Derved skabes der et overblik over sikkerhedsmiljøets omfang og virkemåde. Det væsentlige er imidlertid hvordan og hvor godt sikkerhedsmiljøet fungerer i praksis. Derfor bør der foretages forskellige former for afprøvninger, fx om en reaktionsstyrke kan være til stede inden for den fastlagte tid eller om en Firewall i et informationssystem lever op til de stillede krav. Af risikologgen kan det umiddelbart konstateres, i hvilket omfang tidligere konstaterede fejl og mangler (sårbarheder) er afhjulpnet og hvilke sikkerhedsbrud, der er konstateret. Fx kan mange sikkerhedsbrud og fejl kombineret med manglende opfølgning indikere, at sikkerhedsmiljøet kan være svagt.

Det er væsentligt, at der ikke kun fokuseres på det fysiske sikkerhedsmiljø, men også personellens sikkerhedsforståelse. Der er således ofte en sammenhæng mellem mangelfuld sikkerhedsuddannelse/instruktion og antallet af sikkerhedsbrud.

Resultaterne af vurderingen/analysen af sikkerhedsmiljøets styrke i forhold til hvert aktiv og de trusler, der er identificeret, indtastes som vist i figur 9-1-5 i regnearkets grønne faneblad. Sikkerhedsmiljøets styrke udtrykkes ved anvendelse af værdierne stærk, middel eller svag.

Sårbarhedsanalyse										
Aktiv Nr.	Aktiv	Sensitivt	Vitalt	Spionage	Sabotage	Under-gravende virksomhed	Terrorisme	Civile uroligheder	Kriminalitet	
1	Shortbreak (nødgenerator for offentlig strøm)	Nej	Ja				Middel		Middel	
2	TCE 621 X-postterminal (krypto)	Ja	Nej	Stærkt			Middel		Stærkt	
3	STU II B/EASY FAX (krypto)	Ja	Ja	Stærkt			Middel		Stærkt	
4	TTJ Hardware FIIN LAN (administrativt)	Nej	Ja	Stærkt			Svagt		Stærkt	
5	Personel, teknisk	Nej	Ja	Middel		Middel	Middel		Stærkt	
6	Håndvåben (30 stk)	Ja	Nej	Svagt			Stærkt		Middel	
7	Vagt- og beredskabskøretøjer	Nej	Ja				Svagt		Svagt	
8	UPS til operativt net, FIN og X-post	Nej	Ja	Stærkt			Stærkt		Stærkt	
9	Operative planer (få)	Ja	Nej	Stærkt			Stærkt		Stærkt	
10	Brændstoftager til nødgenerator	Nej	Ja				Svagt		Svagt	
0	0	0	0							
0	0	0	0							
0	0	0	0							
0	0	0	0							

Fig. 9-1-4

Fastlæggelse af risikoniveauet sker ved at indføre hvert enkelt aktiv i skemaerne i regnearkets orange faneblad, som vist i figur 9-1-6. Der anvendes ét skema for hver trussel, der er identificeret. Trusselsniveauet, som den ene værdi (høj, middel eller lav), hentes fra regnearkets lilla faneblad i fase 4. Værdien for sikkerhedsmiljøets styrke fremgår af det grønne faneblad (svag, middel eller stærk).

3. Risikoniveau undergravende virksomhed											
Trusselsniveau	Sikkerhedsmiljø, styrke										
	Stærk			Middel			Svag				
Lavt											
Middel											
Højt											
Lavt											
Middel											
Højt											

Fig. 9-1- 5

Farverne rød, gul og grøn er et udtryk for risikoniveauet for hvert enkelt aktiv, idet aktiver i det røde felt er udsat for et højt risikoniveau (kritisk), aktiver i gule felter middel og aktiver i grønne er udsat for et lavt risikoniveau. Ved denne visualisering gives et umiddelbart billede af aktuelle kritiske risici, der kræver optimering af sikkerhedsmiljøet.

Resultatet af fase 5 er en liste over sikkerhedsmiljøets styrke i ft. truslerne og minimumskravene samt et risikobillede for hver enkelt trussel.

7.2. Intet sikkerhedsmiljø

I de tilfælde, hvor der ikke eksisterer et sikkerhedsmiljø, eller hvor et sådan endnu ikke er udviklet, tages der udgangspunkt i hvert enkelt aktiv og de fastsatte minimumskrav til sikkerheden. Der tages i den forbindelse hensyn til den i fase 3 gennemførte analyse af love og bestemmelsers betydning for sikkerhedsmiljøet.

Det generelle sikkerhedsmiljø beskrives i et udkast til en sikkerhedsinstruks jf. bilag 2 til kapitel 9. For informationssystemer beskrives sikkerhedsmiljøet i en sikkerhedskravsspecifikation, installationsdokumentation og i informationssikkerhedsinstrukser, del 1 og 2 jf. afsnit III til kapitel 6. Disse dokumenter kan indgå som bilag til projektbeskrivelser, business cases, programoplæg o. lign.

I fm. udvikling af et nyt sikkerhedsmiljø vil det ofte være nødvendigt at indhente ekspertbistand, herunder ressourcemæssige vurderinger ved de funktionelle tjenester, civile virksomheder og sikkerhedsmyndigheden. Der kan ligeledes være behov for at foretage simuleringer, og andre former for afprøvninger, herunder analyser af fx statistiske data, der kan underbygge og dokumentere styrken i de anbefalede sikkerhedssystemer. I de tilfælde, hvor et sikkerhedsmiljø ikke kan etableres inden for rammerne af minimumskravene, skal risikovurderingen og beskrivelserne af det ønskede sikkerhedsmiljø, jf. ovenfor, forelægges sikkerhedsmyndigheden (FE) til godkendelse. Sikkerhedsmiljøet for informationssystemer klassificeret FTR og HEM skal i alle tilfælde godkendes af FE.

Til sårbarhedsanalyse og fastlæggelse af risikoniveau anvendes regnearkets grønne og orange faneblad, som beskrevet oven for.

Resultatet af fase 5 er en oversigt over aktiverne med angivelse af det eksisterende eller det projekterede sikkerhedsmiljøs styrke samt udkast til sikkerhedsinstruks med sikringsplan eller en sikkerhedskravsspecifikation med informationssikkerhedsinstrukser (jf. kapitel 9 pkt. 5). Desuden et risikobillede for hver trussel.

Den endelige sårbarhedsanalyse bør som minimum klassificeres FORTROLIG.

8. FASE 6, ACCEPT AF RISIKO.

I denne fase skal sårbarhedsanalysen forelægges chefen til godkendelse. Hvis der er overensstemmelse mellem det af chefen fastsatte niveau for accept af risiko (evt. fastlagt i fase 1) og resultatet af sårbarhedsanalysen (risikobilledet), godkendes sikkerhedsmiljøet, og der kan fortsættes til fase 7. I modsat fald må der foretages forbedringer af sikkerhedsmiljøet. Denne proces fortsættes indtil chefen netop kan acceptere risikoen, idet han/hun dog ikke kan acceptere forhold, der ikke opfylder minimumskravene i FKOBST 358-1.

Resultatet af denne fase er chefens accept af alle risici og dermed det eksisterende eller planlagte sikkerhedsmiljøs opbygning og virkemåde. Der er således taget stilling til, **”*hvor godt aktiverne skal beskyttes og hvordan*”**.

9. FASE 7, OPTIMERING AF SIKKERHEDSMILJØ.

I det omfang, at der i fase 5 viser sig kritiske risici, eller at chefen i fase 6 ikke kan acceptere risikoniveauet, skal sikkerhedsmiljøet udbygges og optimeres. Der kan være andre grunde til, at sikkerhedsmiljøet skal eller bør justeres, fx:

- At planlagte beskyttelsesforanstaltninger ikke har den ønskede virkning
- At funktionelle tjenester eller andre serviceleverandører ikke kan levere den ønskede sikkerhed
- At sikkerhedsmyndigheden ikke kan godkende dele af sikkerhedsmiljøet
- Økonomiske eller andre ressourcemæssige forhold.

Afhængig af sikkerhedsmiljøets kompleksitet, kan der være behov for en egentlig analyse med opstilling af forskellige muligheder for ændring af sikkerhedsmiljøet med en opgørelse af fordele og ulemper. Analysen skal skabe grundlag for et begrundet valg af alternative beskyttelsesforanstaltninger, der til sammen optimerer sikkerhedsmiljøet således, at de eksisterende risici herved bringes på et niveau, som chefen netop kan acceptere. I denne optimering indgår tillige hensyn til relevante funktionelle tjenester og andre serviceleverandørers virke.

Resultatet af fase 7 er en konkret anbefaling om etablering af nye beskyttelsesforanstaltninger og evt. nedlæggelse af visse forældede eller på anden måde mangelfulde foranstaltninger

10. FASE 8, DOKUMENTATION

I denne fase samles det udarbejdede materiale til en samlet rapport. Følgende bør indgå:

- Chefens direktiv
- Et regneark med oversigt over aktiver med dokumentation for, hvor vitale og sensitive aktiverne

er

- Bilag med angivelse af forhold af betydning for dimensionering af sikkerhedsmiljøet
- En trusselsliste med trusselsbilleder og evt. bilag, der nærmere beskriver specifikke trusler
- Et regneark med en sårbarhedsanalyse og risikobilleder
- Evt. delanalyser af et eksisterende eller et projekteret sikkerhedsmiljøes styrke
- Evt. direktiv fra CH til optimering af sikkerhedsmiljø
- Sikkerhedsinstrukser, specifikationer, erklæringer mv.
- Evt. godkendelser fra sikkerhedsmyndigheden (FE)
- Evt. kontrakter eller andre former for aftaler af betydning for implementering og drift af dele af sikkerhedsmiljøet, fx indsatsstyrke, elektronisk overvågning, vedligeholdelse af software til beskyttelse af informationssystemer o. lign.
- Evt. implementeringsplaner for etablering af sikkerhedsmiljø eller optimering af dette
- CH accept af risiko.

På baggrund af risikovurderingen færdiggøres den endelige sikkerhedskravsspecifikation (IT) og sikkerhedsinstruks. I det omfang der har været arbejdet med flere versioner, sammenskrives disse til en endelig version.

Risikovurderingen giver ligeledes anledning til at vurdere behov for uddannelse/instruktion af myndighedens eller enhedens personel, idet den rette sikkerhedsforståelse er en forudsætning for, at sikkerhedsmiljøet fungerer i praksis.

Til slut skal der i denne fase tages stilling til, hvilke parametre af betydning for sikkerhedsmiljøet, der løbende skal overvåges, herunder hyppighed og hvem der gør det. Det vil normalt være forhold vedr.:

- opgaver/kerneydelsen
- aktiver, fx anskaffelse og udfasning
- trusler
- ændringer i bestemmelser og lovgivning
- sikkerhedsbrud
- fejl og mangler
- økonomi
- driftstatusrapporter for informationssystemer
- overholdelse af indgåede samarbejdsaftaler og kontrakter.

Der bør tages stilling til, i hvilke tilfælde ændringer i ovennævnte parametre giver anledning til fornyet risikovurdering eller på anden måde justeringer i de elementer, der indgår i denne.

Resultatet af fase 8 er en samlet sikkerhedsdokumentation, som minimum bestående af en risikovurdering og sikkerhedsinstruks med sikringsplan, og eller sikkerhedskravsspecifikation med informationssikkerhedsinstrukser. Disse dokumenter skal alle være godkendt af chefen. I en række tilfælde skal sikkerhedsdokumentationen ligeledes være godkendt af relevante funktionelle tjenester, andre serviceleverandører samt FE.

10.1. Fase 9 Styringsaktiviteter.

Denne fase er ikke en del af risikovurderingen, men medtages for at slutte den i pkt. 2 beskrevne cyklus, idet afvigelser kan give anledning til, at en ny cyklus må gennemløbes helt eller delvis. Implementering, vedligeholdelse og optimering af et sikkerhedsmiljø kræver løbende overvågning og kontrol af de parametre, der er nævnt i fase 8. Kontrolvirksomheden er beskrevet i kapitel 9, pkt. 9.

Helt essentielt i styringen af sikkerheden er risikologgen. I denne logges de afvigelser i form af sikkerhedsbrud eller tilløb til sådanne, konstaterede fejl og mangler, herunder manglende overholdelse af fx SLA, der er af betydning for sikkerhedsmiljøet. Risikologgen danner også grundlag for afgivelse af rapporter til foresat myndighed, serviceleverandører og sikkerhedsmyndigheden.

Sikkerhedsbrud rapporteres som beskrevet i kapitel 10.

Underbilag 1 til bilag 1 til kapitel 9. Definitioner, terminologi og forkortelser

ABM	Forkortelse for Ansvarlig Brugermyndighed (anvendes i forhold til IKT-systemer).
ASM	Forkortelse for Ansvarlig Systemmyndighed (anvendes i forhold til IKT-systemer).
Baseline	Ordet "baseline" dækker her over et samlet øjebliksbillede af et dynamisk dokument. Betegnelsen indgår ofte i forbindelse med konfigurationsstyring eller versionsstyring. Et eksempel kan være at den sikkerhedsansvarlige har udarbejdet en sikkerhedsdokumentation version 1 for et system. Kort tid herefter gennemføres 4 mindre konfigurationsændringer af systemet, der medfører konsekvensrettelser til sikkerhedsdokumentationen. Disse gennemføres i form af rettelsesmeddelelser nr. 1-4. Den samlede dokumentation udgøres nu af version 1 + rettelsesmeddelelserne 1-4. Når sikkerhedsdokumentationen baselines sker ved udsendelse af en version 2, hvor alle tidligere rettelsesmeddelelser er indarbejdet.
Beskyttelse/ beskyttelsesforanstaltning	Beskyttelse betegner den egenskab, der tilføres et aktiv eller forhold der tilvejebringes, således at det bedre kan modstå trusler.
Aktiver	Omfatter alle myndighedens aktiver lige fra materielle ting som personel, materiel, våben, bygninger, it-systemer, dokumenter, økonomiske midler mv. til immaterielle ting som data, information, viden, renommé, mv.
KAM	Forkortelse for Kapacitets Ansvarlig Myndighed (anvendes i forhold til IKT-systemer).
Kritiske risici	Betegnelsen kritiske risici dækker over de risici, der ikke kan accepteres. Især spiller kritiske risici en central rolle i en overordnet risikovurdering, der sigter mod at træffe beslutning om på hvilke områder, der skal udarbejdes en detaljeret risikovurdering.
Kvalitativ	Kvalitativ er en egenskab ved et udsagn, der sigter til at udsagnets indhold ikke er målbart, det er en kvalitet ved den eller det udsagn handler om. En ekspertvurdering baseret på sprogligt formulerede kriterier er en kvalitativ vurdering.
Kvantitativ	Kvantitativ er en egenskab ved et udsagn, der sigter til at udsagnets indhold er målbart. Resultatet af statistiske målinger, hvor måleresultaterne fremkommer i en form, hvor de fx matematisk kan sammenregnes er en kvantitativ måling.
Lavineeffekt	Betegner sammenhængen mellem flere på hinanden følgende virkninger af en trussel i form af en kædereaktion. Således kan en meget lille risiko, der knytter sig til en trussel medføre en serie af små virkninger, der samlet bliver alvorlig for myndigheden.

**Risiko
(definition)**

Muligheden for, at der indtræffer en hændelse (en konkret udmøntning af en trussel), der påvirker fastlagte mål og strategier i uønsket retning, med det implementerede sikkerhedsmiljø inddraget i vurderingen. En risiko udtrykkes således ved produktet af trusslens sandsynlighed og konsekvens samt sikkerhedsmiljøets styrke, hvilket svarer til produktet af trusselsniveauet og sikkerhedsmiljøets styrke.

Risikobillede

Er en oversigt over samtlige risici, der er afdækket af risikovurderingen med angivelse af risikoniveau. Det kan fx præsenteres i en oversigtsmatrix.

**Risikoniveau
(definition)**

Risikoniveauet betegner produktet af en trussels sandsynlighed, konsekvens og sikkerhedsmiljøets styrke. Det svarer til produktet af trusselsniveauet og sikkerhedsmiljøets styrke. Ved anvendelse af kvalitative metoder følger produktudregningen denne tabel:

Trussels-niveau	X	Sikkerhedsmiljøets styrke	=	Risiko-niveau
Lav	X	Stærk	=	Lav
Lav	X	Middel	=	Lav
Lav	X	Svag	=	Lav
Middel	X	Stærk	=	Lav
Middel	X	Middel	=	Middel
Middel	X	Svag	=	Middel
Høj	X	Stærk	=	Lav
Høj	X	Middel	=	Middel
Høj	X	Svag	=	Høj

**Risikostyring
(definition)**

Den ledelsesmæssige styring af myndighedens indsats i fm. håndtering af afdækkede risici.

**Risikovurdering
(definition)**
Sikkerhedsmiljø

En systematisk afvejning af myndighedens risikobillede.

Betegner det samlede sæt af beskyttelsesforanstaltninger i forhold til de aktiver som myndigheden råder over. Der er ikke tale om en ren summering af beskyttelsesforanstaltningerne, idet sikkerhedsmiljøet søges tilrettelagt, således at beskyttelsesforanstaltningerne bringes i samvirke og at synergi-effekter udnyttes.

Sikkerhedsmyndigheden

I forhold til informationer af fælles betydning for NATO, EU og WEU, varetages denne rolle af FE. Til rollen er tillagt bemyndigelse til godkendelse af sikkerhedsløsninger (godkendelse af risikoniveau).

Single Point of Failure

Den engelske betegnelse for det forhold, at et svigt i tilgængeligheden for et aktiv kan bringe hele myndighedens eller enhedens "produktion" til øjeblikkelig standsning (kerneydelsen kan ikke leveres).

SLA	Står for Service Level Agreement og betegner det formelle dokument, der udtrykker den enighed, der er forhandlet mellem en kunde og en leverandør vedr. leverance af service-ydelser. Resultatet skal udtrykkes i målelige termer.
Sårbarhed (definition)	Et aktivs mangel på beskyttelse, der udsat for en trussel kan medføre uønskede hændelser.
Sårbarhedsanalyse (definition)	Er en analyse af sikkerhedsmiljøets styrke over for de trusler, der potentielt kan indvirke på et aktiv med henblik på at af-dække de virkninger, de enkelte dele af truslernes sandsyn-ligheder og konsekvenser, har på aktivet (indgår i enhver risi-kovurdering).
Trussel (definition)	Betegner en skadevoldende eller sikkerhedstruende hæn-delse, der potentielt kan medføre (betydelig) skade for en myndighed. En trussel beskrives ved dens sandsynlighed for forekomst (lav/middel/høj) samt ved hvor høj grad af skade (lav/mid-del/høj), den kan volde virksomheden uden sikkerhedsmiljø inddraget.
Trusselsbillede	Er en oversigt over samtlige trusler, med angivelse af trus-selsniveau. Det kan fx præsenteres i en oversigtsmatrix.
Trusselsliste	En liste over trusler, som minimum beskrevet ved deres sand-synlighed. En trussel betragtes som potentiel, så længe dens sandsynlig-hed og konsekvens ikke er fastlagt.

Bilag 2 til kapitel 9. Vejledning til udarbejdelse af sikkerhedsinstruks

Denne vejledning findes som en skrivbar skabelon i den elektroniske version af FKOBST 358-1 under bogmærke "links til skrivbare skabeloner". Til hvert pkt. er der knyttet en meget kort vejledning, der alene skal opfattes som en ledetråd. Vejledningen kaldes frem ved at trykke på F1 tasten. For yderligere vejledning henvises til respektive kapitler.

En sikkerhedsinstruks udarbejdes på baggrund af en risikovurdering. Sikkerhedsinstruksen skal være konkret, kortfattet og kendt af alt personel ved myndigheden eller enheden. Den skal ligeledes være let tilgængelig, fx på det lokale netværk. Sikkerhedsinstruksen udgør et væsentligt grundlag for tilrettelæggelse af den militære sikkerhedsuddannelse/instruktion.

Indholdet af sikkerhedsinstruksen er helt afhængig af myndighedens eller enhedens opgaveportefølje og infrastrukturen i området. Kun relevante områder medtages og der skal lægges vægt på at beskrive de lokale sikkerhedsregler og -procedurer, herunder hvem der gør hvad inden for den militære sikkerhedstjenestes delområder.

Klassifikation af sikkerhedsinstruksen som helhed bør ikke være højere end TIL TJENESTEBRUG. Bilag med bl.a. sikringsplan kan klassificeres højere.

SIKKERHEDSINSTRUKS

1. GENERELLE FORHOLD

- 1.1. Sikkerhedsorganisation og detailansvar
- 1.2. Overordnet koordination og samvirke med andre enheder på etablissementet/området
- 1.3. Uddannelsesprogram for militær sikkerhed (evt. som særligt bilag)
- 1.4. Klassifikationsgrader og mærkninger samt offentliggørelse af tjenstlige sager
- 1.5. Nødsfalds-/katastrofeforanstaltninger (evt. som særligt bilag).

2. PERSONELSIKKERHED

- 2.1. Procedurer for sikkerhedsgodkendelse
- 2.2. Bemyndigelse til indsiget i HEM/YHM-klassificeret materiale
- 2.3. Tavshedspligt
- 2.4. Oplysningspligt og ændringer til personoplysninger
- 2.5. Særlige forhold vedr. tjenstlige rejser til udlandet
- 2.6. Udstedelse af sikkerhedscertifikater
- 2.7. Bopæl i udlandet
- 2.8. Forbindelse med udlændinge
- 2.9. Tjenstlige aktiviteter med lande uden for NATO og EU
- 2.10. Dødsfald.

3. MATERIELSIKKERHED

- 3.1. Generelle forhold vedr. klassifikation og mærkning
- 3.2. Opbevaring af klassificeret og vitalt/sensitivt materiel jf. sikringsplanen
- 3.3. Procedurer for håndtering af FTR- og HEM-klassificeret materiel
- 3.4. Procedurer for håndtering af håndvåben, ammunition og eksplosivstoffer
- 3.5. Procedurer for håndtering af våben, systemer og andet materiel med særlig sikkerhedsrisiko
- 3.6. Andet vitalt/sensitivt materiel
- 3.7. Opbevaring af udlånt våben og ammunition
- 3.8. Opbevaring af militære og civile skytteforeningers våben

- 3.9. Emballering og forsendelse/transport af FTR/HEM-klassificeret materiel
- 3.10. Beskyttelse i f.m. transport af våben, ammunition og eksplosivstoffer
- 3.11. Særlige forhold under øvelser/deployering/indsættelse (operative forhold)
- 3.12. Kompromittering, bortkomst eller beskadigelse
- 3.13. Mønstring i sikkerhedsmæssig henseende.

4. DOKUMENTSIKKERHED

- 4.1. Klassificering og særlig mærkning af dokumenter og andet informationsbærende materiale
- 4.2. Udfærdigelse, fremstilling, registrering og reproduktion
- 4.3. Pakning, kvittering, forsendelse og transport (ekstern)
- 4.4. Procedurer for intern transport/forsendelse
- 4.5. Modtagelse, registrering og intern sagsvandring
- 4.6. Medbringelse af klassificeret materiale uden for tjenestestedet
- 4.7. Opbevaring af klassificeret informationsbærende materiale (jf. sikringsplanen)
- 4.8. Rettelser, sanering og tilintetgørelse (HEM/YHM)
- 4.9. Mønstring (HEM/YHM).

5. OPERATIONSSIKKERHED

- 5.1. Generelle principper og ansvar for planlægningen
- 5.2. Operative delforanstaltninger
- 5.3. Logistiske delforanstaltninger
- 5.4. Tekniske delforanstaltninger
- 5.5. Administrative delforanstaltninger
- 5.6. Særlige forhold under øvelsesvirksomhed, herunder ved deltagelse af udenlandske enheder
- 5.7. Kontrolforanstaltninger for operationssikkerhed.

6. INFORMATIONSSIKKERHED

Skabelon for udarbejdelse af sikkerhedsdokumentation for nationale systemer, herunder risikovurdering og informationssikkerhedsinstrukser (ISI) fremgår af kapitel 6. Informationssikkerhedsinstruks del II kan evt. indgå som selvstændigt bilag til sikkerhedsinstruksen.

7. FYSISK SIKKERHED

- 7.1. Lokal ansvarsfordeling
- 7.2. Samarbejde og koordination med øvrige myndigheder/enheder
- 7.3. Kontorsikkerhed
- 7.4. **Sikringsplan** (normalt som bilag)
 - 7.4.1. Fastlæggelse og beskrivelse af områdeinddeling for etablering, bygninger og rum
 - 7.4.2. Fastlæggelse og beskrivelse af sikringsniveauer i bygninger og rum
 - 7.4.3. Mekanisk sikring:
 - 7.4.3.1. Grænseflader
 - 7.4.3.2. Perimeterhegn
 - 7.4.3.3. Opbevaringsmidler
 - 7.4.3.4. Låse
 - 7.4.3.5. Nøgler
 - 7.4.3.6. Koder
 - 7.4.4. Elektronisk overvågning:
 - 7.4.4.1. AIA-anlæg
 - 7.4.4.2. Videoovervågningsanlæg
 - 7.4.4.3. Overfaldsalarmer
 - 7.4.4.4. ADK-anlæg
 - 7.4.5. Adgangskontrol:
 - 7.4.5.1. Opholdskontrol
 - 7.4.6. Bevogtning:
 - 7.4.6.1. Faktiske krav til indsætstid
 - 7.4.6.2. Prioritering af indsættelse

7.4.6.3. Koordination ved indsættelse

7.4.6.4. Vagtinstruks.

Sikringsplanen bør være et særskilt og klassificeret bilag til sikkerhedsinstruksen, da den kan indeholde sensitive informationer om sikkerhedsmiljøets virkemåde og mulige svagheder. Af samme årsag bør indsigt i dette dokument begrænses til det absolut nødvendige.

8. INDUSTRISIKKERHED

- Kontakt til Sektionen for Sikkerhedsgodkendelser ved FE
- Ansvar i fm. civile virksomheders arbejde og færden på/ved MYN/ENH
- Indstillingsprocedure for sikkerhedsgodkendelse af civile virksomheder
- Indstillingsprocedure for sikkerhedsgodkendelse af civile personer, der skal udføre arbejde i sikrede og kontrollerede områder.

9. RISIKOSTYRING

- Intern kontrol
- Ekstern kontrol
- Risikolog.

10. RAPPORTERING

- Brud på den militære sikkerhed
- Mistænkelige observationer
- Rapporteringsformer
- Rapporteringsformularer.

Bilag 3 til kapitel 9. Eksempel på forretningsorden for koordinationsudvalg vedrørende militær sikkerhed**1. OPRETTELSE, FORMÅL MV.**

Koordinationsudvalg vedrørende militær sikkerhed (KUVMILSIK) er nedsat i henhold til FKOBST 358-1, Bestemmelser for den Militære Sikkerhedstjeneste.

Formålet med udvalget er, at koordinere den militære sikkerhedstjeneste på etableringer, hvor flere myndigheder og enheder er samplacerede.

2. SAMMENSÆTNING.

I KUVMILSIK indgår repræsentanter for de myndigheder, der er garnisoneret på etableringen. Normalt disses sikkerhedsofficerer (SIKOF) og eller Informationssikkerhedsofficerer (ISO).

Formandskabet varetages af den chef, der af styrelsen eller myndigheden er udpeget som ansvarlig for at koordinere den militære sikkerhedstjeneste på stedet.

Formanden udpeger en suppleant til at varetage ledelsen af udvalgets arbejde og møder i dennes fravær.

Myndighederne udpeger suppleanter efter behov, fx. assisterende SIKOF.

Sekretærfunktionen varetages af den myndighed, som formanden er chef for.

KUVMILSIK kan efter behov supplere sig med repræsentanter fra andre myndigheder eller særlige sagkyndige.

3. KOMPETENCE.

KUVMILSIK skal koordinere den samlede militære sikkerhedstjeneste inden for etableringen og evt. eksterne områder tilknyttet dette.

I tilfælde af uoverensstemmelser vedr. den militære sikkerhedstjeneste er det formandens ansvar, at problemstillingen løftes til nærmeste højere niveau ved de involverede myndigheder eller enheder.

KUVMILSIK kan efter behov nedsætte og styre arbejdsgrupper med specialopgaver af såvel permanent som midlertidig art. Dette kan fx være samordning af større sikringsprojekter, der berører flere myndigheder på stedet.

4. DAGSORDEN.

De ordinære møder har følgende faste punkter på dagsordenen:

1. Godkendelse af dagsorden.
2. Godkendelse af referat fra forrige møde.
3. Behandling af emner rejst af myndighederne (se bilag).
4. Gennemgang af erindringsliste.
5. Gennemgang af national trusselvurdering (møde i 3. kvartal).
6. Orientering fra medlemmerne.
7. Orientering fra formanden.
8. Eventuelt.
9. Dato for næste møde.

5. MØDER OG MØDELEDELSE.

KUVMILSIK afholder ét møde i hvert kvartal. På mødet i 4.kvartal fastlægges mødedatoer for det efterfølgende år. Ekstraordinære møder kan afholdes efter formandens bestemmelse eller på foranledning af myndighederne. I det omfang, der ikke er emner til behandling på et møde, kan formanden aflyse det.

Møderne ledes af formanden eller i dennes forfald en af ham udpeget, normalt SIKOF ved myndigheden.

Der er mødepligt i KUVMILSIK.

6. INDKALDELSE, REFERAT OG ERINDRINGSLISTE

Mødeindkaldelser med emner til dagsorden udsendes af sekretariatet senest to uger før et møde. Emner, der ønskes behandlet og optaget på dagsordenen, skal være sekretariatet i hænde senest tre uger før et møde.

Sekretariatet udarbejder et beslutningsreferat, evt. bilagt særlige udtalelser eller standpunkter fra mødedeltagerne.

Mødereferatet udsendes senest to uger efter et mødes afholdelse. Evt. bemærkninger til referatet fremsættes på næste ordinære møde og optages i referatet fra dette møde.

Sekretariatet fører erindringsliste jf. dagsordenens pkt. 4.

7. ØKONOMI

Udgifter forbundet med udvalgets virksomhed afholdelse af deltagerne selv.

Denne forretningsorden er vedtaget på KUVMILSIK møde: dato.

Oversigt over områder, der skal koordineres på etablissementerne

Under iagttagelse af chefansvaret, kan alle dele af den militære sikkerhedstjeneste behandles efter behov i KUVMILSIK. Nedenfor er anført en række forhold vedrørende den militære sikkerhedstjeneste, som skal koordineres på etablissementerne. Da udvalgets kompetence alene er af koordinerende art, skal der lægges vægt på sikkerhedsmæssige forhold af fælles betydning for etablisementet. Dette gælder navnlig forhold vedr. bevogtningstjeneste samt adgangs- og opholdskontrol.

1. UDARBEJDELSE OG AJOURFØRING AF RISIKOVURDERINGER

- Registrering af sensitive og vitale aktiver
- Fælles opfattelse af love og bestemmelsers betydning for sikkerhedsmiljøet
- Fælles opfattelse af trusler
- Vurdering af sårbarheder i sikkerhedsmiljøet
- Risikovurderinger i fm. særlige arrangementer, bl.a. VIP besøg
- Sikkerhedsmæssige snitflader til eksterne myndigheder, funktionelle tjenester og evt.
- Civile serviceleverandører.

2. UDARBEJDELSE OG AJOURFØRING AF SIKKERHEDSINSTRUKSER

- Sikkerhedsgodkendelser af civile leverandører/håndværkere
- Evt. fællessekretariats håndtering af klassificerede (FTR og højere) dokumenter
- Nødfalds- og katastrofeplaner
- Sikkerhedsmæssige forhold i fm. større øvelser på etablisementet.

2.1. Udarbejdelse og ajourføring af sikringsplaner

- Standard for mekanisk sikring. FES er systemansvarlig MYN
- Standard for elektronisk overvågning. FES er systemansvarlig MYN
- Standard for adgangskontrol til bygninger og anlæg, herunder anvendelse af ADK-anlæg. FES er systemansvarlig MYN for ADK-anlæg
- Anvendelse af lokal indsatsstyrke (LIS) i bevogtningen
- Indsættelse af regional indsatsstyrke (RIS) i bevogtningen
- Prioritering af indsættelsen af LIS/RIS ved flere samtidige alarmer
- Afgivelser til bevogtning (LIS)
- Vagtinstrukser
- Fælles anvendelse af sikrede lokaliteter, fx i fm våben og ammunitionsoplæg o. lign.
- Færdsel og ophold på fælles arealer inden for etablisementet
- Civile leverandørers adgang til arealer, anlæg og bygninger

- Transporter af vitalt og eller sensitivt materiel
- Informationssikkerhed på brugerniveau, ISO virksomhed
- Sikkerhed i forhold til fælles IT-installationer (IT-hardware).

3. KONTROL

- Forberedelse i fm. gennemførelse af generelle sikkerhedseftersyn
- Opfølgning efter generelle sikkerhedseftersyn (risikolog)
- Resultater af og erfaringer med intern kontrol (risikolog)
- Status vedr. gennemførelse af sikringsprojekter, herunder økonomiske forhold
- Gennemgang af FC årlige rapport over sikkerhedstilstanden, fx på mødet i 2. kvartal.

4. SIKKERHEDSMÆSSIGE HÆNDELSER

Udveksling af erfaringer vedr. konstaterede sikkerhedsmæssige hændelser (risikolog).
Mistænkelige observationer, opmærksomhedsuddannelse.

5. UDDANNELSE

Muligheder for fælles uddannelsesprogrammer og erfaringsudveksling vedr. disse.

6. SIKKERHEDSBEREDSKAB

Sikkerhedsberedskab indgår ikke som en del af den militære sikkerhedstjeneste, men er en overbygning til denne. Imidlertid bliver SIKOF i de fleste tilfælde involveret, når sikkerhedsberedskabsforanstaltninger skal iværksættes. Det fleste steder kan KUVMILSIK således med fordel varetage denne koordination også.

7. ANDET

Pressepolicy ved sikkerhedsmæssige hændelser.

Bilag 4 til kapitel 9. Vejledning til indhold af rapport vedrørende generelt sikkerhedseftersyn**1. INDLEDNING**

Rapport vedrørende generelt sikkerhedseftersyn findes i den elektroniske version af FKOBST 358-1 under bogmærke skrivbare skabeloner. Skabelonen kan tilpasses ved at slette eller tilføje felter og tekst, så den passer til det aktuelle behov ved den myndighed, der skal efterses.

I alle tilfælde, hvor det konstateres, at kravene jf. FKOBST 358-1 ikke er opfyldt, eller hvor der konstateres andre uregelmæssigheder, skal dette anføres. I disse tilfælde, skal der gives klare anvisninger på, hvorledes kravene kan opfyldes, procedurer omlægges mv. Den eller de myndigheder, der er ansvarlig for at dette sker, skal anføres.

2. VURDERING**2.1. Sikkerhedstilstanden ved myndigheden/Institutionen bedømmes således:**

I rapportens pkt. 9.3. markeres pågældende delområde og bedømmelsen vælges i rulleteksten.

2.2. Der anlægges følgende bedømmelseskriterier:

- **MEGET TILFREDSSTILLELSE:**
Myndigheden/enheden har opfyldt alle væsentlige krav og standarder, og der er ikke behov for forbedringer på de undersøgte områder.
- **TILFREDSSTILLELSE:**
Myndigheden/enheden har opfyldt alle væsentlige krav og standarder, og der er ikke behov for større forbedringer på de undersøgte områder.
- **IKKE HELT TILFREDSSTILLELSE:**
Myndigheden/enheden har ikke opfyldt et eller flere af de væsentlige krav og standarder. Der skal foretages forbedringer.
- **IKKE TILFREDSSTILLELSE:**
Myndigheden/enheden har ikke opfyldt hovedparten af de væsentlige krav og standarder, eller et enkelt meget væsentligt krav. Der skal snarest foretages forbedringer.

Hvis dele af sikkerhedstjenesten ikke er eftersat, anføres efter forholdene:

- Ikke eftersat eller Ikke aktuelt.

Kapitel 10**HÆNDESESHÅNTERING OG -RAPPORTERING****Indhold**

Kapitel 10.....	1
HÆNDESESHÅNTERING OG -RAPPORTERING	1
1. INDLEDNING	1
2. FORMÅL.....	1
3. ANSVAR.....	2
4. DEFINITIONER	2
4.1. Hændelse.....	2
4.2. Kompromittering.....	2
4.3. Sikkerhedsbrud.....	2
4.4. Sårbarhed	2
5. KONCERNFÆLLES RAMME FOR HÆNDESESHÅNTERING	2
5.1. Planlæg og forbered	2
5.2. Opdag og reager	3
5.3. Lessons Identified / Lessons Learned	3
6. SIKKERHEDSOMRÅDER OG RAPPORTERINGSKRAV.....	3
6.1. Hændelser inden for personelsikkerhed.....	4
6.2. Hændelser inden for materielsikkerhed	4
6.2.1 Våben, ammunition og eksplosivstoffer.	4
6.3. Hændelser inden for dokumentssikkerhed.....	6
6.4. Hændelser inden for operationssikkerhed	6
6.5. Hændelser inden for kryptosikkerhed.....	6
6.6. Hændelser inden for cyber- og informationssikkerhed	7
6.7. Hændelser inden for persondatasikkerhed (GDPR).....	7
6.8. Hændelser inden for fysisk sikkerhed.....	7
6.9. Hændelser inden for industrisikkerhed	7
6.10. Øvrige forhold.....	8
7. AFSLUTNING AF SAGER VEDRØRENDE BORTKOMST OG KOMPROMITTERING AF KLASSIFICEREDE INFORMATIONSBÆRENDE MATERIALER	8

1. INDLEDNING

Der skal ved konstatering af sikkerhedsmæssige hændelser rapporteres hurtigst muligt, med det formål at understøtte håndtering og eventuel efterforskning af hændelser.

Rettidig rapportering af brud eller mistanke om brud på den militære sikkerhed er endvidere forudsætningen for, at FE og FMN kan yde den nødvendige rådgivning med henblik på at minimere eventuelle skadelige virkninger af en hændelse. Rapporteringen skal desuden medvirke til at skabe og vedligeholde et normalbillede af den militære sikkerhed, herunder operationssikkerhed. Normalbilledet er tillige med til at danne grundlag for udarbejdelse af trussels- og risikovurderinger, forslag til justering af de militære sikkerhedsbestemmelser og sikkerhedsforanstaltninger samt analyser til brug for hele koncernen.

2. FORMÅL

Formålet med kapitlet er at fastlægge principper og rammer, der sikrer effektiv håndtering af hændelser, samt rettidig rapportering af og opfølgning på hændelser i koncernen, herunder i forhold til involvering af FE og FMN. Principperne og rammerne i kapitlet gælder både hændeshåndtering internt og på tværs af myndighederne i koncernen.

3. ANSVAR

Enhver myndighedschef er ansvarlig for at iværksætte afbødende foranstaltninger og rapportering ved erkendelse af eller mistanke om hændelser inden for militær sikkerhed, samt for at indsamle og rapportere erfaringer og resultater efter undersøgelser af sådanne forhold.

FE og FMN kan inden for hver af myndighedernes ansvarsområder på eget initiativ eller efter anmodning yde rådgivning om eller anviser supplerende sikkerhedsmæssige, afbødende foranstaltninger. FE eller afhængigt af hændelsestypen FMN vil desuden vurdere, i hvilket omfang der skal foretages yderligere undersøgelser og rapportering.

4. DEFINITIONER

Dette afsnit gennemgår de væsentligste definitioner for hændelseshåndtering og -rapportering.

4.1. Hændelse

En eller flere uventede og/eller uønskede omstændigheder, der muligvis kan påvirke eller kompromittere den militære sikkerhed. Denne betegnelse anvendes overordnet, men også indledningsvist, indtil omstændighederne om en hændelse er nærmere analyseret.

4.2. Kompromittering

En kompromittering er en aktørs bevidste forsøg på - og succes med - at opnå et brud på den militære sikkerhed. Inden for informationssikkerhed beskrives dette som et brud på fortroligheden, integriteten og/eller tilgængeligheden.

4.3. Sikkerhedsbrud

Et sikkerhedsbrud er et internt og typisk utilsigtet brud på de regler og bestemmelser, der gælder for de respektive sikkerhedsområder, jf. pkt. 6. Som ved en kompromittering, beskrives dette også som et brud på fortroligheden, integriteten og/eller tilgængeligheden inden for informationssikkerhed.

4.4. Sårbarhed

En sårbarhed er en svaghed, der kan udnyttes af en aktør til at forsøge at kompromittere sikkerheden. Sårbarheder kan fx findes i it-systemer eller fysiske sikkerhedsforanstaltninger.

5. KONCERNFÆLLES RAMME FOR HÆNDELSHÅNDTERING

De respektive sikkerhedsområder har forskellig karakter, og når en hændelse opstår, vil der være forskellige interessenter og ansvarshavende, som skal inddrages. Nogle hændelser indvirker desuden på flere sikkerhedsområder på én gang.

Det er myndighedschefens ansvar at sikre, at der for alle relevante sikkerhedsområder er udarbejdet og dokumenteret én eller flere interne processer for hændelseshåndtering, og at der er udpeget ansvarlige chefer eller medarbejdere for at vedligeholde processerne.

For koncernfælles systemer og andre aktiver, der anvendes på tværs af flere myndigheder, gælder desuden, at den it-ansvarlige eller kapacitetsansvarlige myndighed skal udarbejde processer for hændelseshåndtering, der giver både leverandør og forretning mulighed for at reagere hurtigt og koordineret, når en hændelse opdages.

Håndtering af hændelser opdeles i denne bestemmelse i 3 faser:

- Planlæg og forbered
- Opdag og reagér
- Lessons Identified and Lessons Learned (LI/LL)

5.1. Planlæg og forbered

Det er myndighedens ansvar at sikre, at der inden for alle sikkerhedsområder udarbejdes, kommunikeres og afprøves processer for, hvordan både chefer og medarbejdere skal forholde sig ved hændelser. Myndighedens processer skal udarbejdes inden for rammen af denne bestemmelse samt øvrigt, gældende forvaltningsgrundlag.

Det er vigtigt, at den lokale sikkerhedsorganisation er i stand til at reagere efter kendte processer og planer ved hændelser inden for alle sikkerhedsområder. Det er myndighedens ansvar at sikre, at

medarbejderne er bekendte med den lokale sikkerhedsorganisation og med processerne for hændelseshåndtering og -rapportering.

5.2. Opdag og reager

Det er myndighedens ansvar at reagere, når en hændelse opstår, ved at involvere den lokale sikkerhedsorganisation hurtigst muligt. Den lokale sikkerhedsorganisation skal i samarbejde med involverede parter analysere alle hændelser med henblik på at forstå hændelsens umiddelbare omfang og herigennem iværksætte relevante tiltag. Hvis det ikke er muligt at vurdere omfanget og/eller håndtere en hændelse lokalt, skal den lokale sikkerhedsorganisation eskalere hændelsen internt i egen organisation og inddrage relevante interessenter i henhold til myndighedens egne processer. Vedrører hændelsen koncernfælles systemer eller andre aktiver, der anvendes på tværs af flere myndigheder, skal relevante myndigheder involveres hurtigst muligt.

Den lokale sikkerhedsorganisation skal registrere og sikre tilstrækkelig dokumentation af alle hændelser til senere brug for LI/LL, jf. afsnit 5.3., samt til periodisk rapportering af hændelserne. Det påhviler alle involverede myndigheder at registrere observationer og efterfølgende bidrage til LI/LL.

Ved en hændelse, hvor flere myndigheder er involveret, vil det som udgangspunkt være den it-ansvarlige eller kapacitetsansvarlige myndighed, der er ansvarlig for at lede håndteringen af hændelsen under inddragelse af alle relevante interessenter i koncernen. Ansvar for håndtering af en hændelse kan overføres mellem myndigheder, hvis der indgås en eksplicit aftale herom.

5.3. Lessons Identified / Lessons Learned

Lessons Identified / Lessons Learned (LI/LL) er en systematisk tilgang til erfaringsindhentning, der bygger på at omsætte observationer til varige ændringer gennem først en analyse og dernæst implementering.

Ved enhver hændelse skal det vurderes, om der skal gennemføres LI/LL med henblik på at undgå en lignende hændelse i fremtiden og på at forbedre interne og tværorganisatoriske processer for hændelseshåndtering og -rapportering. Der skal som minimum gennemføres LI/LL ved alle kritiske hændelser, herunder hændelser der kan få eller har haft store konsekvenser for myndigheden eller koncernen samt hændelser, hvor tidligere indsatser ikke har haft den ønskede effekt.

Udbedrende aktiviteter kan omfatte:

- Ny risikovurdering af et aktiv
- Forbedring af sikkerhedsmiljøet, hvor hændelsen indtraf
- Forbedring af myndighedens proces for hændelseshåndtering

Det er myndighedens ansvar at sikre, at værdifuld læring fra overståede hændelser opsamles og anvendes, herunder ved inddragelse af involverede parter.

6. SIKKERHEDSOMRÅDER OG RAPPORTERINGSKRAV

Dette afsnit beskriver hændelsestyper inden for de forskellige sikkerhedsområder i koncernen. Desuden fremgår der inden for hvert sikkerhedsområde krav til rapportering.

Rapporteringsbegrebet omfatter både den orientering om hændelser, som skal ske, men også kommunikation i forbindelse med selve håndteringen af hændelser.

Alle hændelser og kritiske sårbarheder, der vurderes at kunne føre til hændelser, skal rapporteres skriftligt ved brug af de officielle rapporteringsskabeloner. For hvert enkelt sikkerhedsområde fremgår neden for en oversigt over faste adressater for rapportering.

Ved hændelser af særlig hastende karakter kan og bør lettest tilgængelige kommunikationsform anvendes indledningsvist, herunder fx telefonopkald eller VTC. Herefter skal der ske en skriftlig rapportering, som kan suppleres af yderligere rapportering afhængigt af hændelsens karakter og udvikling.

Alle typer af hændelser, der kan påvirke Forsvarets operative virke, skal hurtigst muligt kommunikeres til FKO-JOC.

Alle hændelser, der vurderes at have offentlighedens interesse, herunder vurderes at blive gjort til genstand for omtale i medierne, skal hurtigst muligt eskaleres til styrelseschefen samt til FMN.

[Link til rapporteringsskabeloner findes her](#)

6.1. Hændelser inden for personelsikkerhed

Hændelser inden for personelsikkerhed defineres som erkendelse af eller mistanke om hændelser, der kan have eller har haft skadelig, nedsættende eller begrænsende indflydelse på beskyttelsen af medarbejderne i Forsvarsministeriets koncern mod terrorisme, spionage, sabotage, undergravende virksomhed, kompromittering mv.

Det er en hændelse, når der opstår sikkerhedsmæssige betænkeligheder vedrørende en sikkerhedsgodkendt person, herunder ved problemer af økonomisk art, problemer med alkohol, medicin eller narkotika, eller fordi den pågældende færdes i ekstremistiske og/eller kriminelle miljøer.

Det er endvidere en hændelse, når der er mistanke om eller kendskab til, at en ansat sikkerhedsgodkendt person har været i konflikt med straffeloven, militær straffelov, våbenloven eller lov om euforiserende stoffer. Overtrædelser af færdselsloven skal rapporteres, hvis det vedrører spirituskørsel eller har medført fængselsstraf eller inddragelse af førerretten.

Faste adressater ved rapportering:

- Foresatte myndighed, FE

6.2. Hændelser inden for materielsikkerhed

Hændelser inden for materielsikkerhed defineres som erkendelse af eller mistanke om hændelser, der kan have eller har haft indflydelse på beskyttelse af Forsvarets materiel, forsyninger mv. mod spionage, sabotage eller hærværk, tyveri og bortkomst samt cyberangreb.

Der er tale om en hændelse ved bortkomst, herunder tyveri, tilvejebringelse, kompromittering eller formodning herom af materiel klassificeret FORTROLIGT eller højere samt materiel af vital og/eller sensitiv betydning (se kap. 3).

Rapporteringen afhænger af, om der ved hændelsen er sket et brud på de fysiske sikkerhedsforanstaltninger, om hændelsen udgør en sikkerhedsmæssig risiko eller om hændelsen ikke udgør en sikkerhedsmæssig risiko.

Enhedschefen – eksempelvis chefen for en underafdeling eller tilsvarende – er ansvarlig for, at der føres tilsyn med beholdningsmæssige afvigelser af våben, ammunition og eksplosivstoffer samt vitalt eller sensitivt materiel.

Chefen er ligeledes ansvarlig for, at der i forbindelse med hændelser rapporteres til Politiet, Forsvarets Auditørkorps, Forsvarets Efterretningstjeneste og Forsvarsministeriets Materiel- og Indkøbsstyrelse i henhold til punkt 6.2.

Såfremt der ved en hændelse ikke er sket et brud på de fysiske sikkerhedsforanstaltninger, og hændelsen ikke udgør en sikkerhedsmæssig risiko ud fra et risiko- og væsentlighedsprincip kan enhedschefen afgøre hændelsen uden rapportering til Forsvarets Efterretningstjeneste og Forsvarsministeriets Materiel- og Indkøbsstyrelse. Dog skal der altid ske særskilt anmeldelse til Forsvarets Auditørkorps, såfremt der er en formodning om, at en kriminel handling er begået.

Såfremt hændelsen ikke medfører rapportering til Forsvarets Efterretningstjeneste og Forsvarsministeriets Materiel- og Indkøbsstyrelse skal der føres journal ved myndigheden over disse afgørelser, og journalen skal arkiveres efter gældende regler herfor. Journalen skal forelægges myndighedschefen (chefer for eskadre, regiment eller wing) til underskrivelse som minimum halvårligt.

Journalen gemmes til fremvisning ved sikkerhedseftersyn.

6.2.1 Våben, ammunition og eksplosivstoffer.

Ved bortkomst af våben, ammunition og eksplosivstoffer skal myndighedschefen til hver en tid vurdere, hvorvidt der er tale om en hændelse, der har udgjort en sikkerhedsmæssig risiko ud fra et risiko- og væsentlighedsprincip. Der rapporteres jf. vurdering beskrevet i pkt. 6.2.1.1. – 6.2.1.4.

Tilvejebringelse af våben, ammunition og eksplosivstoffer rapporteres jf. pkt. 6.2.1.5.

6.2.1.1 Hændelse med et brud på de fysiske sikkerhedsforanstaltninger.

Er der ved hændelsen sket et brud på de fysiske sikkerhedsforanstaltninger, der hvor våben, ammunition og eksplosivstoffer er opbevaret, eller der i forbindelse med bortkomsten er mistanke om en kriminel handling, skal bortkomsten af våben, ammunition og eksplosivstoffer, uanset mængde, indberettes til den lokale politikreds via politiets hjemmeside. Den indberettende myndighed modtager ved indberetningen en kvittering og journalnummer. Indberetning skal ligeledes gennemføres i Forsvarsministeriets Materiel- og Indkøbsstyrelses database "Registrering af bortkomne/tilvejebragte genstande" med angivelse af det journalnummer politiet har givet sagen.

Såfremt der er formodning om, at en kriminel handling er begået, f.eks. pligtforsømmelse, tyveri mv. skal indberetningen tillige sendes til Forsvarets Efterretningstjeneste og til Forsvarets Auditørkorps.

Politiets hjemmeside: <https://politi.dk/anmeld-kriminalitet> (Internet)

Forsvarsministeriets Materiel- og Indkøbsstyrelses database: [Registrering af bortkomne/tilvejebragte genstande](#) (FIIN)

Forsvarets Efterretningstjeneste: "[Rapport om brud på den militære sikkerhedstjeneste](#)" sendes til FE-MYN@fiin.dk

Forsvarets Auditørkorps: fauk-myn@fiin.dk

6.2.1.2 Hændelse der udgør en sikkerhedsmæssig risiko.

Omhandler hændelsen bortkomst af beskedne mængder ammunition og eksplosivstoffer, der udgør en sikkerhedsmæssig risiko ud fra et risiko- og væsentlighedsprincip, skal hændelsen indberettes til den lokale politikreds via politiets hjemmeside, indrapporteres i Forsvarsministeriets Materiel- og Indkøbsstyrelses database "Registrering af bortkomne/tilvejebragte genstande" og til Forsvarets Efterretningstjeneste.

Såfremt der er formodning om, at en kriminel handling er begået, f.eks. pligtforsømmelse, tyveri mv., skal der altid ske særskilt anmeldelse herom til Forsvarets Auditørkorps.

Politiets hjemmeside: <https://politi.dk/anmeld-kriminalitet> (Internet)

Forsvarsministeriets Materiel- og Indkøbsstyrelses database: [Registrering af bortkomne/tilvejebragte genstande](#) (FIIN)

Forsvarets Efterretningstjeneste: "[Rapport om brud på den militære sikkerhedstjeneste](#)" sendes til FE-MYN@fiin.dk

Forsvarets Auditørkorps: fauk-myn@fiin.dk

6.2.1.3 Hændelse uden brud på fysiske sikkerhedsforanstaltninger og ingen sikkerhedsmæssig risiko.

Hvis der ved hændelsen ikke er sket et brud på de fysiske sikkerhedsforanstaltninger, og hændelsen ikke vurderes at udgøre en sikkerhedsmæssig risiko, kan myndighedschefen afgøre hændelsen uden rapportering til Forsvarets Efterretningstjeneste og Forsvarsministeriets Materiel- og Indkøbsstyrelse. Såfremt der er formodning om, at en kriminel handling er begået, f.eks. pligtforsømmelse, skal der altid ske særskilt anmeldelse herom til Forsvarets Auditørkorps.

Forsvarets Auditørkorps: fauk-myn@fiin.dk

6.2.1.4 Årlig rapportering.

Styrelser, stabe og myndigheder skal i deres årsoversigter over sikkerhedstilstanden angive, om hændelser inden for materielsikkerhed er sket ved brud på de fysiske sikkerhedsforanstaltninger, om hændelsen udgør en sikkerhedsmæssig risiko eller om hændelsen ikke udgør en sikkerhedsmæssig risiko.

Forsvarets Efterretningstjeneste kan på eget initiativ eller efter anmodning yde rådgivning om i hvilket omfang, der skal foretages eventuelle supplerende sikkerhedsmæssige afbødende foranstaltninger. Forsvarets Efterretningstjeneste vil desuden vurdere i hvilket omfang, der skal foretages yderligere undersøgelser og rapportering.

6.2.1.5 Tilvejebringelse.

Ved tilvejebringelse af våben, ammunition og eksplosivstoffer skal hændelsesstedet indberette tilvejebringelsen til Forsvarsministeriets Materiel- og Indkøbsstyrelse. Indberetning skal gennemføres i Forsvarsministeriets Materiel- og Indkøbsstyrelses database "Registrering af bortkomne/tilvejebragte genstande" og til Forsvarets Efterretningstjeneste, jævnfør gældende rapporteringsprocedure.

Efter modtagelse af indberetning underretter Forsvarsministeriets Materiel- og Indkøbsstyrelse politiet med henblik på registrering i Koster registret.

Ved tilvejebringelse af våben, ammunition og eksplosivstoffer skal hændelsesstedet sikre sig, at rapportformular fremsendes som efterretning til Forsvarsministeriets Auditørkorps.

Forsvarsministeriets Materiel- og Indkøbsstyrelses database: [Registrering af bortkomne/tilvejebragte genstande](#) (FIIN)

Forsvarets Efterretningstjeneste: ["Rapport om brud på den militære sikkerhedstjeneste"](#) sendes til FE-MYN@fiin.dk

Forsvarets Auditørkorps: fauk-myn@fiin.dk

6.3. Hændelser inden for dokumentsikkerhed

Hændelser inden for dokumentsikkerhed defineres som erkendelse af eller mistanke om hændelser, der kan have eller har haft indflydelse på fortrolighed, integritet eller tilgængelighed af koncernens klassificerede informationsbærende materialer (fx dokumenter, eksterne harddiske, USB lagermedier, CD og DVD'er og andre databærende medier). Hændelser vedrørende informationsbærende medier kan ofte involvere andre sikkerhedsområder og skal i givet fald håndteres og rapporteres i henhold til krav på disse områder.

Hændelser vedrørende dokumentsikkerhed skal rapporteres internt i egen myndighed og til FE.

Faste adressater ved rapportering:

- Danske dokumenter: Udstedende myndighed (USM)
- Udenlandske dokumenter: FE

6.4. Hændelser inden for operationssikkerhed

Hændelser inden for operationssikkerhed defineres som erkendelse af eller mistanke om hændelser, der kan have eller har haft indflydelse på beskyttelse af Forsvarets operationer, såvel nationale som internationale, øvelser og anden hertil knyttet aktivitet mod spionage, terrorisme, undergravende virksomhed, sabotage mv.

Der er tale om en hændelse ved kendskab til eller mistanke om forsøg på indhentning af oplysninger om og/eller hindring eller forsinkelse af planlægning, forberedelse og udførelse af militære operationer og indsættelse samt dertil knyttede aktiviteter i koncernen. Det er desuden en hændelse, hvis det konstateres, at ikke alment tilgængelige militære anlæg, enheder, våben, medarbejdere, materiel, sikkerhedsforanstaltninger mv. fotograferes eller på anden måde afbildes, omtales eller vises i offentligt tilgængelige fora.

Hændelser, der kan påvirke operationssikkerheden, skal eskaleres hurtigst muligt til FKO-JOC.

Faste adressater ved rapportering:

- Foresatte myndighed, FE, FKO-JOC

6.5. Hændelser inden for kryptosikkerhed

Hændelser inden for kryptosikkerhed defineres som uautoriserede personers indsigt eller mulighed for indsigt i krypteringsinformation eller -teknologi. I DAMSG 205, kapitel 9, er der listet, hvilken type hændelser der som minimum kan udgøre et brud på kryptosikkerheden.

Brud på kryptosikkerheden skal rapporteres i henhold til kap. 9 i DAMSG 205, herunder altid til CFCS. Den indledende rapportering skal ske omgående. Det er vigtigere at rapportere hurtigt, end at rapporten overholder formalia, og end at foretage undersøgelse af hændelsen. Et brud på

kryptosikkerheden kan medføre et brud på informationssikkerheden, der jf. § 45 i Justitsministeriets sikkerhedscirkulære, også skal rapporteres. Rapporteringen skal som minimum klassificeres FORTROLIGT. Forsendelse skal ske i overensstemmelse med bestemmelserne om håndtering af klassificeret information i Justitsministeriets sikkerhedscirkulære.

Faste adressater ved rapportering:

- Foresatte myndighed, FE (CFCS), kontrollerende myndighed (jf. kryptoplanen)

6.6. Hændelser inden for cyber- og informationssikkerhed

Hændelser inden for cyber- og informationssikkerhed defineres som erkendelse af eller mistanke om hændelser, der har haft eller kan få indflydelse på fortrolighed, integritet eller tilgængelighed af informationer behandlet i koncernens IKT-, OT- og IOT-systemer, disse systemers funktionalitet, eller i systemer ved eksterne leverandører, der behandler koncernens data eller data om koncernen.

Hændelser inden for cyber- og informationssikkerhed skal den lokale sikkerhedsorganisation hurtigst muligt eskalere til FMI Security Operations Center (SOC), når it-ansvaret ligger ved FMI.

For de systemer, hvor myndigheden selv er it-ansvarlig, skal den lokale sikkerhedsorganisation eskalere hændelsen internt efter egne processer samt inddrage FMI SOC. FMI SOC kan herved få overblik over hændelser i koncernen og vil i nødvendigt omfang kunne støtte myndighedens håndtering af hændelsen.

Den it-ansvarlige myndighed sikrer relevant rapportering til FMN samt til andre relevante interessenter, herunder it-serviceudvalg. Den it-ansvarlige myndighed skal ligeledes sikre rapportering til CFCS ved større hændelser samt hændelser på klassificerede systemer.

Faste adressater ved rapportering:

- Foresatte myndighed, FMI SOC

6.7. Hændelser inden for persondatasikkerhed (GDPR)

Hændelser inden for persondatasikkerhed defineres som erkendelse af eller mistanke om hændelser, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Foruden at de i pkt. 6.6. angivne rapporteringskrav skal følges, skal hændelser relateret til persondatasikkerhed hurtigst muligt eskaleres til den dataansvarliges DPO. FMNBST 280-2 foreskriver yderligere retningslinjer for håndtering af og rapportering om hændelser inden for persondatasikkerheden.

Faste adressater ved rapportering:

- Ved anmeldelse til Datatilsynet: Foresatte myndighed, FMN Team GDPR

6.8. Hændelser inden for fysisk sikkerhed

Hændelser inden for fysisk sikkerhed defineres som ulovlig indtrængen eller forsøg herpå på etableringer og andre af koncernens områder. Det gælder også ved indbrud, indbrudsforsøg og tyveri fra militære kvarterer, Forsvarets lejemøbler og Forsvarets køretøjer mv.

Ved hændelser relateret til den fysiske sikkerhed skal der foruden intern rapportering gives en indledende melding til FKO-JOC.

Faste adressater ved rapportering:

- Foresatte myndighed, FE, FKO-JOC, FES og bevogtningsansvarlig myndighed

6.9. Hændelser inden for industrisikkerhed

Hændelser inden for industrisikkerhed defineres som hændelser, der har eller har haft indflydelse på beskyttelsen af sikkerhedsgodkendte virksomheder og sikkerhedsgodkendte ansatte mod spionage, sabotage, terrorisme og cyberangreb samt hærværk, tyveri mv.

Faste adressater ved rapportering:

- Foresatte myndighed, FE, kontrakt- og projektansvarlig myndighed

6.10. Øvrige forhold

Ved mistænkelige sikkerhedsmæssige hændelser, som ikke falder under de foregående sikkerhedsområder, skal den lokale sikkerhedsorganisation registrere alle henvendelser, observationer m.v. og i nødvendigt omfang rapportere dette internt.

Sager, som vurderes at være relateret til mulig spionage-, terror-, sabotage- eller undergravende virksomhed samt organiseret kriminalitet, rapporteres til FE hurtigst muligt på FIIN (FE-KTP-ASH) eller IKL (FE-KTP-ASH@MIL.DK).

Sager vedrørende underslæb, bedrageri eller tyveri mv. begået mod koncernens myndigheder/enheder skal rapporteres til FAUK.

7. AFSLUTNING AF SAGER VEDRØRENDE BORTKOMST OG KOMPROMITTERING AF KLASIFICEREDE INFORMATIONSBÆRENDE MATERIALER

Hændelser vedrørende informationer med relation til eller ophav ved særlige, eksterne myndigheder skal som hovedregel afsluttes af FE jævnfør nedenstående.

- Danske informationer. USM afslutter sagen ved rapportering til involverede parter.
- NATO-informationer. FE afslutter sagen ved rapportering til NATO i henhold til C-M(2002)49.
- EU-informationer. FE afslutter sagen ved rapportering til EU i henhold til "Sikkerheds forskrifter for Rådet for den Europæiske Union".
- WEU-informationer. FE afslutter sagen ved rapportering til WEU i henhold til "WEU Sikkerhedsforskrifter (RS 100)".
- FN-informationer. FE afslutter sagen.
- OSCE informationer. FE afslutter sagen.

LINK TIL SKRIVBARE SKABELONER M.M. PÅ FIIN OG INTERNET

Nr.	Skabelon/sprog	Platform	
		FIIN	Internet
01	Courier Certificate, NATO 		
02	Fratrædelseserklæring 	 	
03	Indstilling om sikkerhedsgodkendelse 	 	
04	Klassificerede sager medtaget fra tjenestestedet 		
05	Kvittering/receipt  		
06	Oplysningsskema 1 	 	
07	Oplysningsskema 1 	 	
	Instructions for completion of Information Form 1 		
08	Oplysningsskema 2 	 	
09	Oplysningsskema 2 	 	
	Instructions for completion of Information Form 2 		
10	Oplysningsskema 3 	 	
11	Oplysningsskema 3 	 	
	Instructions for completion of Information Form 3 		
12	Oplysningsskema i forbindelse med fritagelse for generelle sikkerhedseftersyn 		
13	Rapport om brud på den militære sikkerhed 		
14	Rapport om brud på informationssikkerheden 		
15	Rapport om brud på kryptosikkerheden 		
16	Rapport vedrørende generelt sikkerhedseftersyn/intern kontrol 		
17	Rapportering – Bort- eller tilvejekomst af våben, ammunition, eksplosivstoffer samt vitalt og/eller sensitivt materiel 		
	Vejledninger til do 		
18	Rapporteringsskema for ikke klassificerede systemer 		

Nr.	Skabelon/sprog	Platform	
		FIIN	Internet
19	Rapporteringsskema for årlig rapportering af sikkerhedsrelevante installationer 		
20	Risikolog, skabelon 		
21	Risikovurdering, skabelon 		
22	Sikkerhedsinstruks, skema 		
23	Tavshedspligt, præcisering af gældende regler vedrørende 		
24	Tilintetgørelsesbevis for klassificerede materialer 		
25	FKO It Eftersynsskema		
26	Request for Personnel Security Clearance Confirmation, Nato		
27	Personnel Security Clearance Confirmation, Nato		
28	Fritagelse for generelle sikkerhedseftersyn, oplysningsskema	 	