FORSVARETS EFTERRETNINGSTJENESTE

Vejledning om virksomhedssikkerhed

Version 2.50

Juni 2024

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Telefon 33 32 55 66

Hjemmeside www.fe-ddis.dk
Mailadresse fe-ktp-godkendelser@mil.dk

Indhold

1. Virksomhedsgodkendelse 5
Om vejledningen 5
Behov for godkendelse 5
Godkendelsesproceduren 5
Fornyelse af virksomhedsgodkendelse 6
Sikkerhedsansvaret i virksomheden 6
Uddannelse 7
Ejerskifte mv. 7
2. Personelsikkerhed 7
Personkredsen 7
Beslutningsgrundlaget 7
Godkendelsesproceduren 8
Fortrolighedserklæring ved fratrædelse og stillingsskift 9
Informationspligten 9
3. Dokumentsikkerhed 10
Klassifikation 10
Registrering og reproduktion mv. 11
4. Transport og forsendelse 11
Medbringelse udenfor virksomheden 11
Forsendelse 11
Transport af materiale 11
5. IT-sikkerhed 12
Anvendelse af udstyr 12
Adgangsstyring 13
Netværksstyring 13
Informationssikkerhed i beredskabssituationer 13
Immaterielle rettigheder 13
6. Fysisk sikkerhed 13
Risikovurdering (risikoanalyse) 13
- Områdeinddeling/sikringsniveau 13
- Mekanisk sikring 14
- Elektronisk overvågning 14
- Bevogtning 14
- Adgangskontrol 14
- Kontorsikkerhed 14
7. Internationale forhold 14
Adgang til udenlandsk information 14
Procedurer for besøgstilladelser 15
Man skal sørge for at ansøge i god tid 15
Rejsevejledninger 16
Dokumentation af sikkerhedsgodkendelse 16

8. Meldepligt og rapportering..... 17

1. Virksomhedsgodkendelse

Om vejledningen

Denne vejledning giver generel information om regler og procedurer for danske virksomheder, der skal udføre sikkerhedsmæssigt klassificeret arbejde for Forsvaret og andre styrelser og myndigheder indenfor Forsvarsministeriets område.

De mere detaljerede sikkerhedsbestemmelser med gældende minimumskrav fremgår af "Bestemmelser for den militære sikkerhedstjeneste" (FKOBST 358-1).

Rådgivning kan hentes ved Sektionen for Person- og Industrisikkerhed i telefontiden mandag til torsdag 09:00-11:00 tlf. 79 59 80 60 eller pr. e-mail: fe-ktp-godkendelser@mil.dk.

Behov for godkendelse

Virksomheder, der udfører sikkerhedsmæssigt klassificeret arbejde for Forsvaret, skal være sikkerhedsgodkendt af FE. Sikkerhedsgodkendelserne behandles i FE af Sektionen for Person- og Industrisikkerhed.

Sikkerhedsgodkendelse vil normalt også være nødvendig for virksomheder, der skal udføre klassificeret arbejde for udenlandske virksomheder og myndigheder, herunder NATO eller EU.

Sikkerhedsgodkendelse af selve virksomheden er ikke nødvendig, hvis ikke der skal opbevares klassificerede informationer/materiale i virksomheden. Leverer virksomheden f.eks. udelukkende konsulentarbejde for Forsvaret, og de klassificerede informationer befinder sig hos kunden/myndigheden, sikkerhedsgodkendes blot det nødvendige antal medarbejdere. Disse medarbejdere knyttes herefter sikkerhedsmæssigt til den pågældende myndighed. Det klassificerede arbejde må ikke iværksættes, før konsulenterne er sikkerhedsgodkendt.

Der må ikke udleveres klassificerede informationer til en virksomhed, før der foreligger en sikkerhedsgodkendelse. Dette gælder dog ikke ved udbudsforretninger, hvor det er tilladt at udlevere materiale, der er klassificeret TIL TJENESTEBRUG. Ved udleveringen skal der i ledsageskrivelsen orienteres om de sikkerhedsmæssige aspekter (FKOBST 358-1 - se kapitel 8, bilag 1 til afsnit I).

Sikkerhedsgodkendte virksomheder har ansvar for, at deres underleverandører er sikkerhedsgodkendt til den nødvendige klassifikationsgrad, og at kunden har givet tilladelse til, at de pågældende klassificerede informationer må videregives.

Godkendelsesproceduren

Følgende kan indstille en virksomhed til sikkerhedsgodkendelse:

- Forsvarsministeriet (FMN)
- Forsvarskommandoen (FKO)
- Hjemmeværnskommandoen (HJK)
- Forsvarsministeriets Materiel- og Indkøbsstyrelse (FMI)
- Forsvarsministeriets Ejendomsstyrelse (FES)
- Organisationen Dansk Industri
- Sikkerhedsgodkendte virksomheder kan indstille om godkendelse af deres underleverandører (benyt dette indstillingsskema).

Indstillende myndighed/virksomhed bør gøre tilbudsgivere opmærksom på, at der ved eventuel kontrakt eller arbejde kan komme udgifter til sikkerhedsforanstaltninger, der er nødvendige for at kunne opnå og opretholde en sikkerhedsgodkendelse, såsom alarmanlæg, opbevaringsmidler og stand alone pc'er.

Når FE har modtaget indstillingen, aftales der et møde i virksomheden, hvor FE fastlægger det konkrete behov for sikkerhedsforanstaltninger og persongodkendelser. Kravene afpasses bl.a. efter følsomheden af de informationer, som virksomheden skal have adgang til og evt. opbevare. Virksomheden meddeles godkendelse, når de af FE stillede krav er opfyldt.

I forbindelse med mødet orienteres der om de oplysningsskemaer eller den elektroniske indstilling, der skal benyttes i forbindelse med persongodkendelsen af ledelsen og de medarbejdere, der skal have adgang til klassificerede informationer.

Det er normalt et krav, at virksomhedens chef (indehaveren/øverste direktør), andre personer, der bestrider direktørstillinger i virksomheden, bestyrelsesformanden, samtlige bestyrelsesmedlemmer (gælder ikke TIL TJENESTEBRUG-godkendte virksomheder), sikkerhedschefen (og evt. stedfortræder) sikkerhedsgodkendes af FE til virksomhedens klassifikationsgrad, dog som minimum til FORTROLIGT.

Når de nødvendige sikkerhedsforanstaltninger er foretaget, persongodkendelserne foreligger, der er indsendt kopi af sikkerhedsinstruks, og virksomheden har underskrevet en sikkerhedsdeklaration, vil virksomheden og den indstillende myndighed få en skrivelse om godkendelsen. Det meddeles heri, hvilken klassifikationsgrad virksomheden godkendes til, og i hvilket tidsrum godkendelsen er gældende (2-4 år afhængigt af klassifikationsgrad).

Fornyelse af virksomhedsgodkendelse

Ved fortsat behov for virksomhedsgodkendelse, skal virksomhedens chef, sikkerhedschef eller stedfortrædende sikkerhedschef anmode FE om fornyelse af godkendelse, senest 3 måneder før godkendelsens udløb. Indstilling om fornyelse sker ved udfyldelse og fremsendelse af skema til fornyelse af virksomhedsgodkendelse.

Sikkerhedsansvaret i virksomheden

Ansvaret for sikkerheden i virksomheden påhviler virksomhedens chef (indehaveren/øverste direktør). Han/hun skal sørge for, at der udstedes en sikkerhedsinstruks med de lokale bestemmelser for sikkerhedsmiljøet i virksomheden. Han/hun er endvidere ansvarlig for, at der udpeges en sikkerhedschef (chefen kan evt. selv varetage denne opgave).

Sikkerhedschefen har ansvaret for udøvelsen af sikkerhedstjenesten i virksomheden, herunder bl.a.:

- Udarbejdelse og vedligeholdelse af sikkerhedsinstruksen
- Indstillinger/afmeldinger til FE vedrørende persongodkendelser
- Indstilling til FE om sikkerhedsgodkendelse af underleverandører
- Kontakten til FE i fm. vejledende sikkerhedseftersyn mv.

Der skal omgående rapporteres til FE om alle sikkerhedsbetydende hændelser (spionage, indbrud, tyveri, sabotage, angreb mod klassificerede it-systemer, kompromittering af klassificerede oplysninger mv.). Meldingen gives telefonisk eller pr. e-mail til FE.

En sikkerhedschef, der ikke har dansk statsborgerskab, må kun få adgang til information, der er klassificeret af danske myndigheder eller af myndigheder i den pågældendes hjemland. Er sikkerhedschefen statsborger i et NATO- og/eller EU-land, kan der desuden gives adgang til henholdsvis NATO- og EU-klassificerede informationer. Da sikkerhedschefen skal kunne håndtere den klassificerede information, som virksomheden modtager, bør virksomheden udpege en sikkerhedschef med dansk statsborgerskab, hvis virksomheden forventer at skulle behandle og opbevare udenlandsk klassificeret information.

Uddannelse

Sektionen for Person- og Industrisikkerhed afholder to gange om året Kursus for Sikkerhedschefer. Kurset er obligatorisk og foregår som hovedregel forår og efterår i København. FE sender mail til sikkerhedschefen med oplysninger om kurset ca. en måned forud for kursets afvikling.

Ejerskifte mv.

Planlægges der ejerskifte eller fusion, skal virksomheden snarest underrette Sektionen for Person- og Industrisikkerhed om det kommende ejerforhold. Det samme gælder, hvis virksomheden ændrer navn.

Det er virksomhedens ansvar snarest muligt at underrette Sektionen for Person- og Industrisikkerhed og den indstillende myndighed eller eventuel hovedleverandør i tilfælde af lukning af virksomheden eller konkurs, således at inddragelse af klassificeret materiale kan finde sted.

I tilfælde af lukning, konkurs eller afmelding af virksomheden afleveres samtlige fratrædelseserklæringer til Sektionen for Person- og Industrisikkerhed.

De detaljerede regler for personelsikkerhed findes i kapitel 2 i FKOBST 358-1.

2. Personelsikkerhed

Personkredsen

I henhold til Sikkerhedscirkulæret skal personer, der får adgang til klassificerede informationer, være sikkerhedsgodkendte. For ansatte i virksomheder, der leverer varer eller tjenesteydelser til myndigheder indenfor Forsvarsministeriets område, er det FE, der foretager godkendelsen.

Beslutningsgrundlaget

Ifølge Sikkerhedscirkulæret skal afgørelser om sikkerhedsgodkendelse træffes på grundlag af en konkret vurdering. FE skal især lægge vægt på, om den pågældende person har en sådan adfærd og karakter, at der ikke kan være tvivl om pågældendes pålidelighed med hensyn til håndtering af klassificerede informationer. Oplysninger om en ægtefælles eller samlevers adfærd og karakter kan også tillægges betydning.

Afgørelser om sikkerhedsgodkendelse træffes på grundlag af oplysninger, som den pågældende person selv giver ved udfyldelsen af et oplysningsskema, og de oplysninger, FE rekvirerer fra myndigheder indenfor Forsvarsministeriets område og fra Politiets Efterretningstjeneste (PET). Ved godkendelse til de lavere klassifikationsgrader foretager PET normalt kun en kontrol af, om personen er kendt i politiets registre, herunder strafbare forhold, misbrugsproblemer og fremstillinger i retten. Ved godkendelse til de højeste klassifikationsgrader foretager PET en grundigere personundersøgelse, hvor der evt. indhentes oplysninger fra tidligere arbejdsgivere, uddannelsesinstitutioner og andre, der kender den pågældende.

Det er ikke muligt at sikkerhedsgodkende en person, hvis den pågældende kun har opholdt sig en kortere årrække i Danmark, og det samtidig ikke er muligt at skaffe pålidelige informationer fra tidligere opholdslande. Det er således normalt en forudsætning for sikkerhedsgodkendelse, at den pågældende person indenfor de seneste syv år har været bosat i Danmark eller i lande, der er medlem af NATO og/eller EU.

Det er alene statsborgere fra NATO-lande, der kan sikkerhedsgodkendes til behandling af NATO-klassificerede informationer. Har den pågældende opholdt sig mindre end fem år i Danmark, indstiller FE til hjemlandet om sikkerhedsgodkendelse.

I forbindelse med sikkerhedsgodkendelse får FE kun oplysninger fra PET, hvis den pågældende person - og dennes eventuelle ægtefælle/samlever - har givet sit udtrykkelige samtykke hertil ved underskrift på oplysningsskemaet/ved afgivet samtykke på det elektroniske indstillingsskema. PET's og FE's behandling af personoplysninger kontrolleres af Tilsynet med Efterretningstjenesterne.

Godkendelsesproceduren

Indstilling om persongodkendelse sker ved, at virksomhedens sikkerhedschef sender en mail med følgende oplysninger til fe-ktp-godkendelser@mil.dk:

- Fulde navn på indstillede
- CPR-nummer
- Stillingsbetegnelse
- Ønsket klassifikationsgrad
- Tjenestefunktion og/eller arbejde (projekt) den indstillede skal bestride

Alternativt sendes et af nedenstående udfyldte oplysningsskemaer til FE:

- Oplysningsskema 1 benyttes ved indstillinger om godkendelse til TIL TJENESTEBRUG og FORTROLIGT (benyttes både ved førstegangsgodkendelse og fornyelser)
- Information form 1 er en engelsksproget version
- Oplysningsskema 2 benyttes ved indstillinger om førstegangsgodkendelse til HEMMELIGT
- Information form 2 er en engelsksproget version
- Oplysningsskema 3 benyttes ved indstillinger om fornyelse af godkendelse til HEMMELIGT
- Information form 3 er en engelsksproget version.

Vær opmærksom på, at oplysningsskemaerne og mails vedr. indstilling indeholder personoplysninger. FE henstiller til, at mails indeholdende personoplysninger krypteres med TLS version 1.2 eller højere. Såfremt jeres mailservice ikke overholder dette krav, kan I ikke indsende indstillinger til vores mail. Det er jeres ansvar som virksomhed, at jeres mailservice understøtter denne kryptering.

Henstillingen følger Datatilsynets vejledning vedrørende transmission af personoplysninger via mail.

Bemærk, at FE ikke kan modtage end-to-end-krypterede mails, eller mails der kræver kodeord eller tilføjelsesprogrammer.

Oplysningsskemaer og indstillinger kan også sendes med posten (ikke rekommanderet) til adressen:

Forsvarets Efterretningstjeneste
Sektionen for Person- og Industrisikkerhed
Kastellet 30
2100 København Ø

Det er vigtigt, at skemaerne bliver udfyldt omhyggeligt. Hvis der f.eks. i pkt. 10 i oplysningsskema 2 (førstegangsgodkendelse til HEMMELIGT) ikke er angivet fuld postadresse, telefonnummer og kontaktperson for tidligere beskæftigelse mv., så returnerer Sektionen for Person- og Industrisikkerhed skemaet til virksomhedens sikkerhedschef med forsinkelse til følge. Personer i virksomheden, der beskæftiger sig med oplysningsskemaer, skal

være sikkerhedsgodkendt til minimum TIL TJENESTEBRUG. Virksomheden må ikke opbevare kopier af udfyldte skemaer, efter skemaerne er indsendt til FE.

FE meddeler sikkerhedsgodkendelse ved et brev til virksomhedens sikkerhedschef, som derpå er ansvarlig for at oplyse medarbejderen i virksomheden om sikkerhedsgodkendelsen.

Afslag på sikkerhedsgodkendelse vil blive begrundet over for den pågældende person, men normalt ikke over for virksomheden, da afgørelsen i almindelighed vil bygge på følsomme personoplysninger. Afslag kan påklages af den pågældende medarbejder til Forsvarsministeriet.

Sikkerhedsgodkendelser af personer har normalt en gyldighedstid på fem år. Personer med bopæl i udlandet dog kun to år.

Særligt vedr. indstilling af udlændinge

Hvis en person har boet eller haft et længerevarende ophold i udlandet indenfor de seneste syv år, skal den eller de seneste bopælsadresser i udlandet påføres skemaet eller vedlægges som bilag.

Vær desuden opmærksom på, at der ved indstilling af udlændinge til klassifikationsgraden HEMMELIGT, skal vedlægges oplysninger om økonomiske forhold i bilag, svarende til de oplysninger der normalt vil fremgå af en dansk årsopgørelse. Herunder opdaterede oplysninger om;

- Indtægt
- Indestående/værdi af aktier
- Ejendomsværdi
- Gæld (offentlig/privat)

Oplysningerne vedlægges som kopier af originale dokumenter, hvori de relevante oplysninger er markeret. Oplysningerne skal suppleres med en oversættelse af de relevante oplysninger til dansk eller engelsk.

Fortrolighedserklæring ved fratrædelse og stillingsskift

Når en sikkerhedsgodkendt medarbejder forlader virksomheden eller skifter til en anden funktion, der ikke kræver sikkerhedsgodkendelse, skal den pågældende underskrive en fortrolighedserklæring.

Fortrolighedserklæringen skal opbevares i virksomheden i fem år, efter at den pågældende medarbejder er ophørt med at være beskæftiget med klassificeret materiale. Erklæringen tjener to formål:

1) at sikre, at medarbejderen er blevet indskærpet, at klassificerede informationer ikke må videregives efter fratrædelsen/funktionsskiftet, og
2) at medarbejderen, ved sin underskrift, har erklæret ikke at være i besiddelse af klassificeret materiale.

Informationspligten

Sikkerhedschefen skal løbende underrette FE om følgende forhold vedrørende de sikkerhedsgodkendte personer:

- Navneændringer og flytninger til udlandet
- Dødsfald, pensionering, afskedigelse og anden årsag til, at behovet for sikkerhedsgodkendelse bortfalder
- Ved indgåelse af ægteskab eller fast samlivsforhold (sker ved at fremsende et nyt oplysningsskema/sende en mail vedr. genindstilling)
- Forhold i øvrigt, der kan være af betydning for den sikkerhedsmæssige vurdering af den pågældende.

Opfylder virksomheden ikke sin informationspligt, kan det medføre, at FE må genoverveje virksomhedens sikkerhedsgodkendelse.

3. Dokumentsikkerhed

Det detaljerede regelsæt om dokumentsikkerhed fremgår af kapitel 4 i FKOBST 358-1.

Dokumentsikkerhed har til formål at beskytte klassificerede informationer mod spionage, kompromittering og tab.
Beskyttelsen sker ved klassifikation og en hertil svarende behandling, opbevaring, mønstring, forsendelse og destruktion af informationerne.
Materiale, der er klassificeret eller påført særlig mærkning, må ikke videregives til uvedkommende eller offentliggøres. Dette må kun ske med den udstedende myndigheds tilladelse.

Overtrædelser vil efter de nærmere omstændigheder være strafbare efter straffelovens § 152 a og forvaltningslovens § 27, stk. 4.

Klassifikation

Der anvendes følgende klassifikationsgrader:

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

Informationer klassificeres efter en vurdering af, hvilken skadevirkning det vil få, hvis informationen kommer i de forkerte hænder.

Informationer kan desuden være påført forskellige mærkninger, der indikerer et særligt tilhørsforhold eller beskyttelseskrav, herunder f.eks. følgende:

- ”NATO” eller ”EU” betyder, at materialet er den pågældende internationale organisations ejendom. Materialet må ikke overgives til myndigheder udenfor organisationen uden særlig tilladelse
- ”ATOMAL” betyder, at materialet er NATO’s ejendom og indeholder oplysninger om atomare forhold. Det skal beskyttes på særlig måde og må kun behandles af særligt bemyndigede
- ”UNCLASSIFIED” betyder, at materialet ikke er sikkerhedsmæssigt klassificeret, men er beregnet til internt brug og ikke må offentliggøres uden udstederens eller FE’s tilladelse
- ”PERSONOPLYSNING, FORTROLIG” betyder, at materialet indeholder personfølsomme oplysninger.

Det er kun den udstedende myndighed, der kan ændre klassifikationen og mærkningen på informationsbærende materiale.

Registrering og reproduktion mv.

Det skal til enhver tid være registreret, hvor i virksomheden det klassificerede materiale befinder sig. Materiale klassificeret FORTROLIGT eller højere må kun udleveres til medarbejderne mod personlig kvittering. Virksomheden skal mindst en gang årligt sikre sig (mønstre), at materiale klassificeret HEMMELIGT er til stede.

Virksomheden må ikke kopiere materiale klassificeret FORTROLIGT eller højere.
Materiale klassificeret til TIL TJENESTEBRUG må gerne fotokopieres. Vær dog opmærksom på, at den udstedende myndighed kan begrænse adgangen til reproduktion med følgende påskrift:
"Uddrag/oversættelse/afskrift/fotokopi/optryk må ikke foretages uden udsteders tilladelse"

Når virksomheden ikke længere har behov for det klassificerede materiale, f.eks. fordi kontrakten er afsluttet, skal materialet normalt returneres til den myndighed, som det er modtaget fra. Materialet må kun makuleres, hvis myndigheden eller FE har givet sin tilladelse hertil.

4. Transport og forsendelse

Det detaljerede regelsæt og blanketter mv. vedrørende medbringelse af klassificeret materiale udenfor virksomheden findes i kapitel 4 i FKOBST 358-1.

Medbringelse udenfor virksomheden

Materiale klassificeret TIL TJENESTEBRUG kan medbringes på rejser og til privat bopæl uden særlige restriktioner.
Materiale klassificeret FORTROLIGT eller HEMMELIGT må medbringes på rejser på følgende betingelser:

- Medbringelsen skal være bemyndiget af virksomhedslederen eller virksomhedens sikkerhedschef
- En fortegnelse over det medbragte materiale skal opbevares i virksomheden
- Personer, der har materialet i deres varetægt under rejsen, skal være sikkerhedsgodkendt til samme klassifikationsgrad, som det medbragte
- Materialet skal være emballeret i overensstemmelse med reglerne herfor og skal transporteres i enten en godkendt og aflåst transportkasse, tilsvarende stålindsats i mappe eller en plomberbar taske
- Materialet må ikke fremtages på offentlige steder
- Ved rejser til udlandet skal der medbringes kurércertifikat (udstedes af Sektionen for Person- og Industrisikkerhed)
- Materiale, klassificeret NATO SECRET eller NATO CONFIDENTIAL, må ikke medbringes på rejse gennem ikke-NATO-lande.

Forsendelse

For forsendelse af klassificeret materiale til ind- og udland gælder følgende:
- TIL TJENESTEBRUG må sendes med almindelig post
- FORTROLIGT skal sendes med kurér, dog kan forsendelse indenfor Danmark ske ved rekommanderet post
- HEMMELIGT klassificeret post må kun forsendes med kurér. Det gælder både i Danmark og til udlandet.

Transport af materiale

Materiale, der er klassificeret TIL TJENESTEBRUG, kan uden særlige sikkerhedsforanstaltninger transporteres i ind- og udland af personer, der er sikkerhedsgodkendt til denne klassifikationsgrad eller højere.
For transport af materiale, der er klassificeret FORTROLIGT eller HEMMELIGT, gælder følgende regler:

1) Gældende bestemmelser for pakning og emballering skal overholdes (se kapitel 4 i FKOBST 358-1)

2) Den for projektet/leverancen ansvarlige myndighed skal have givet tilladelse til transporten
3) Der skal foreligge en fortegnelse i virksomheden over materialet, der skal transporteres
4) Personer, der gennemfører transporten, skal som minimum være sikkerhedsgodkendt til samme klassifikationsgrad som transportens indhold
5) Alt materiale uanset rumfang skal transporteres i godkendt transportmiddel
6) Under transporten skal der medbringes certifikater mv., således:
   - Under transport til/fra udlandet skal der medbringes kurércertifikat (Courier Certificate) samt Personnel Security Clearance Confirmation. Efter transportens gennemførelse returneres kurércertifikatet i udfyldt stand til Sektionen for Person- og Industrisikkerhed
   - Under transport indenfor landets grænser skal der medbringes en fortegnelse over det medbragte materiale.

5. IT-sikkerhed

De detaljerede regler for informationssikkerhed på it- og kommunikationsområdet i det danske forsvar og i sikkerhedsgodkendte virksomheder findes i kapitel 6 i FKOBST 358-1.

Kravene til virksomheders styring af informationssikkerheden afhænger af de produkter og ydelser, som virksomhederne leverer. En række krav vil blive stillet og kontrolleret, såfremt virksomheden skal behandle klassificerede informationer elektronisk på sine egne systemer.

Myndigheder og styrelser i Forsvaret har implementeret et ledelsessystem til styring af informationssikkerheden efter den internationale standard ISO/IEC 27001-2013.

Virksomheder, der udfører arbejde for forsvaret, skal tilsvarende have implementeret et ledelsessystem til styring af informationssikkerheden efter ISO/IEC 27001-2013 eller en anden relevant standard.

Styring af informationssikkerheden har til formål at sikre fortrolighed, integritet og tilgængelighed for informationer, der lagres, behandles eller transmitteres ved hjælp af informations- og kommunikationsteknologi.

Informationssikkerheden skal styres på baggrund af en vurdering af relevante trusler med henblik på evaluering af risikoen for tab af fortrolighed, integritet og tilgængelighed. Risikovurderinger skal ajourføres regelmæssigt under arbejdets udførelse, således at ændringer i trusselsbilledet håndteres løbende.

De konkrete krav til virksomheders styring af informationssikkerheden bør fremgå af de indgåede kontrakter samt af en eventuel sikkerhedsgodkendelse.

Anvendelse af udstyr

Kravene til virksomhedens medarbejdere vedrørende anvendelse af udstyr til behandling af klassificerede informationer skal fremgå af sikkerhedsinstruksen. I forbindelse med behandling af informationer, klassificeret til FORTROLIGT eller højere, skal medarbejderne have læst, forstået og underskrevet en erklæring om overholdelse af regelsættet.

Aktiver, der anvendes ved udførelse af arbejde for Forsvaret, skal identificeres og registreres. Fortegnelse over aktiver skal ajourføres. Sikkerhedsinstruksen skal indeholde retningslinjer for håndtering af aktiverne i overensstemmelse med klassifikationsgraden af de informationer, der behandles via aktivet.
Udstyr skal mærkes med dets anvendelse og klassifikation for bl.a. at undgå fejlbrug. For harddiske, der indeholder informationer klassificeret TIL TJENESTEBRUG, gælder, at de ikke må genbruges til behandling af ikke-klassificerede informationer.

Lagermedier med informationer klassificeret til FORTROLIGT eller højere skal efter endt brug afleveres til Forsvaret til destruktion.

Videokonferenceudstyr kan benyttes til formidling af klassificeret information, hvis FE har godkendt det samlede system.

Adgangsstyring

Kun medarbejdere med et arbejdsbetinget behov, og som er sikkerhedsgodkendt, kan tildeles adgang til behandling af klassificerede informationer. Der skal gennemføres periodisk kontrol af medarbejdernes adgange og rettigheder til systemer med klassificerede informationer.

Der skal være etableret "pauseskærm", der aktiveres efter maks. 15 minutter.
Administration af adgangskoder til klassificerede informationer skal følge reglerne i retningslinjerne i kapitel 6, A.9.4.3. i FKOBST 358-1.

Netværksstyring

Informationstjenester, brugere og informationssystemer på netværk skal opdeles med henblik på at understøtte sikkerheden i de kritiske systemer. Systemer, hvor der behandles klassificerede informationer, må ikke forbindes til andre systemer uden godkendelse fra FE.

Informationssikkerhed i beredskabssituationer

Virksomheden skal definere krav til informationssikkerhed i kritiske situationer, og kravene skal indarbejdes i virksomhedens beredskabsplaner, genetableringsprocesser m.m.

Immaterielle rettigheder

Virksomheden skal sikre, at alle relevante krav i forbindelse med immaterielle rettigheder ved anvendelse af beskyttede softwareprodukter efterleves.

6. Fysisk sikkerhed

De detaljerede regler for fysisk sikkerhed findes i kapitel 7 i FKOBST 358-1.

Fysisk sikring har til formål at beskytte mod uvedkommendes indtrængen i bygninger mv. og adgang til klassificerede informationer.
Fysisk sikring etableres med låse, gitre, pengeskabe, forstærkede døre, alarmer, vagter mv.
I forbindelse med den første godkendelse vil Sektionen for Person- og Industrisikkerhed fastsætte, hvilke yderligere sikringsforanstaltninger der eventuelt skal etableres.
Påtænker virksomheden at foretage bygnings- og lokalemæssige ændringer, der er af sikkerhedsmæssig betydning, skal der straks rettes henvendelse til Sektionen for Person- og Industrisikkerhed. Erfaringen viser, at udgifterne til ændrede sikringsforanstaltninger ofte bliver væsentligt mindre, hvis overvejelser herom indgår allerede ved projekteringen.

Risikovurdering (risikoanalyse)

Omfanget af sikringsforanstaltninger fastsættes på baggrund af de aktuelle risikofaktorer og indarbejdes i en sikringsplan, der kan omfatte følgende:

- **Områdeinddeling/sikringsniveau**

Til opbevaring af materialer, klassificeret FORTROLIGT og højere, skal der etableres sikrede områder, hvor de samlede sikringsmæssige foranstaltninger skal modsvare mængden og graden af det klassificerede materiale.

Kravene til de sikringsmæssige foranstaltninger udtrykkes oftest i sikringsniveauer, der er fastsat af Forsikring og Pension. Opbevaring af øvrigt vitalt materiale vil ofte følge disse krav.

- **Mekanisk sikring**

Mekanisk sikring er sikring af grænseflader – mur, væg, gulv, loft/tag, vindue og dør, der er placeret i grænsefladen – med låse, beslag, gitre o. lign., der vanskeliggør oplukning eller gennembrydning. Sikringen kan udføres som skal-, celle- eller objektsikring. Mekanisk sikring omfatter også etablering af hegn (perimetersikring), evt. præventiv belysning og opbevaringsmidler (sikrings- og pengeskabe).

- **Elektronisk overvågning**

Elektronisk overvågning omfatter automatiske indbrudsalarmanlæg (AIA), adgangskontrolanlæg (ADK), videoovervågningsanlæg og overfaldstryk. Ved alle former for elektronisk overvågning skal alarmoverførsel ske til en døgnbemandet vagtbygning eller godkendt kontrolcentral.

- **Bevogtning**

Bevogtning har til formål at hindre (industri)spionage, terroranslag, sabotage, hærværk og tyveri. Egentlig bevogtning udføres af vagtmandskab, portner, receptionist eller lignende. Bevogtningsmæssigt tilsyn kan udføres af et godkendt vagtselskab ved patruljering, fastboende personer m.fl. Ved bevogtningen overvåges færdsel til og fra området, uvedkommendes indtrængen i og ophold på området forhindres og politi tilkaldes evt.

- **Adgangskontrol**

Adgangskontrol omfatter kontrol ved ind- og udpassage samt opholdskontrol. Dette gennemføres enten ved indsats af medarbejdere (portner/receptionist) eller ved anvendelse af ADK for fast adgangsberettigede.

- **Kontorsikkerhed**

Kontorsikkerhed omfatter de tiltag, der skal træffes i den enkelte virksomhed for at imødegå kompromittering af klassificeret materiale, mens det behandles og opbevares på kontorer, mødelokaler, arkiver mv.
Mødelokaler, hvor klassificerede informationer behandles, skal opfylde de fastsatte minimumskrav til sikringsforanstaltninger vedrørende bl.a. aflåsning, opbevaring af klassificeret materiale, evt. bevogtning og adgangskontrol. Der skal etableres mulighed for at vinduer mv. kan blændes med gardiner/persienner, således at indblik udefra hindres.
Virksomheden skal sørge for, at der er opbevaringsmidler (penge- og sikringsskabe) med en sikkerhedsklassifikation, der tillader opbevaring af det klassificerede materiale. Virksomheden skal tilvejebringe udstyr (f.eks. makulatorer), der opfylder kravene til tilintetgørelse af informationsbærende materiale (f.eks. papir, view-foils, usb-sticks, CD-ROM mv.) afhængig af klassifikationsgraden.

7. Internationale forhold

De detaljerede regler for internationale forhold findes i kapitel 8 (afsnit III) i FKOBST 358-1.

Adgang til udenlandsk information

I henhold til bilaterale sikkerhedsaftaler, som Danmark har indgået med andre lande, er det som udgangspunkt alene danske statsborgere og statsborgere fra det pågældende land, der må gives adgang til det pågældende lands klassificerede information. Hvis der opstår behov for at give en medarbejder, der er statsborger i et 3. land, adgang til informationen, skal man via FE indhente forudgående tilladelse fra den udenlandske udsteder.

Procedurer for besøgstilladelser

Hvis der under besøg i udlandet eller ved udlændinges besøg ved danske sikkerhedsgodkendte virksomheder skal drøftes forhold, der er klassificeret FORTROLIGT/CONFIDENTIAL eller højere, skal både besøgsmodtageren og den besøgende være sikkerhedsgodkendt til den pågældende klassifikationsgrad. Dette sikres gennem en internationalt aftalt procedure, hvor den besøgende virksomhed via sit hjemlands sikkerhedsmyndighed ansøger besøgslandet om en besøgstilladelse.

En række lande, herunder Danmark, stiller også krav om besøgstilladelse ved besøg, hvor der skal drøftes forhold, der er klassificeret til den laveste klassifikationsgrad TIL TJENESTEBRUG/RESTRICTED[1] , eller hvis besøgsstedet er et militært tjenestested[2]. Hvis man er i tvivl om, hvorvidt der skal ansøges om besøgstilladelse i disse tilfælde, må man forhøre sig herom hos besøgsmodtageren.

Man skal sørge for at ansøge i god tid

De fleste landes sikkerhedsmyndigheder forlanger at få ansøgningen fra FE mindst 20 arbejdsdage før besøget, og for enkelte landes vedkommende (bl.a. USA) er kravet helt op til 30 arbejdsdage. Hertil skal lægges ekspeditionstiden hos FE. Sektionen for Person- og Industrisikkerhed videreformidler de nødvendige dokumenter til relevant sikkerhedsmyndighed i forbindelse med besøg. Der kan være tale om et enkelt besøg eller et antal besøg indenfor en defineret periode. Ansøgninger vedrørende besøg i udlandet skal således normalt afleveres til FE senest 35 arbejdsdage før besøget.

Besøg vedr. ikke-klassificerede møder/projekter kræver ikke besøgstilladelse, med mindre der er tale om et militært tjenestested.
Har man ikke fået besøgstilladelsen før sin ankomst til det udenlandske besøgssted, vil man normalt blive nægtet adgang. Tilsvarende er det en betingelse for, at en dansk, sikkerhedsgodkendt virksomhed må modtage et klassificeret besøg fra udlandet, at FE har givet en besøgstilladelse.

Udenlandske virksomheder, der skal aflægge besøg ved danske sikkerhedsgodkendte virksomheder, bør vejledes om, at de skal anvende denne blanket, som i udfyldt stand skal sendes til den relevante sikkerhedsmyndighed i hjemlandet (derfra videresendes blanketten med nødvendige attestationer til FE).

Den danske virksomheds sikkerhedschef skal i god tid før besøget i udlandet sende en udfyldt besøgsanmodning til FE. Hertil anvendes blanketter, således:

- Ved besøg i **USA** anvendes denne blanket. 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 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.
- Ved besøg i **alle andre lande** anvendes denne blanket

Den udfyldte blanket kan sendes enten med posten eller pr. e-mail til Sektionen for Person- og Industrisikkerhed.

Som kontrol kan det nævnes, at den udfyldte besøgsanmodning som minimum skal indeholde:

a. Besøgets forventede klassifikationsgrad (Sektionen for Person- og Industrisikkerhed undersøger, om firmaet er sikkerhedsgodkendt til den krævede klassifikation).

[1] Gælder for besøg i Danmark, Albanien, Bulgarien, Canada, Tjekkiet, Estland, Grækenland, Italien, Litauen, Luxembourg, Norge, Slovenien, Tyrkiet og USA.
[2] Gælder Danmark, Canada, Grækenland, Nederlandene, Tyrkiet m.fl.

b. Besøgsmodtager
- Virksomhedens navn
- Virksomhedens adresse
- Virksomhedens telefonnummer
- Virksomhedens kontaktpersoner.

c. Besøgende
- Fulde navn
- Fødselsdato
- Fødested
- Nationalitet
- Sikkerhedsgodkendelsens niveau
- Pasnummer

d. Egen virksomhed
- Årsag til besøg
- Kopi af en eventuel invitation
- Besøgsperiode (fra/til)
- Underskrift sikkerhedschef/chef

Den danske virksomhed vil fra Sektionen for Person- og Industrisikkerhed eller myndighederne i besøgslandet modtage en bekræftelse på, at besøget er godkendt.

Rejsevejledninger

Virksomheden skal sørge for, at den rejsende får en orientering om de risici, der kan være forbundet med at rejse i det pågældende land. Oplysninger om rejselandet og rejsevejledninger kan hentes på Udenrigsministeriets hjemmeside. Virksomheden kan desuden rette henvendelse til Sektionen for Person- og Industrisikkerhed for vejledning.

Efter hjemkomsten bør sikkerhedschefen evt. indhente oplysninger om, hvorvidt medarbejderen har været udsat for hændelser af sikkerhedsmæssig karakter eller af usædvanlig art. Disse oplysninger videreformidles til Sektionen for Person- og Industrisikkerhed.

Dokumentation af sikkerhedsgodkendelse

Hvis en virksomhed ønsker at give tilbud på eller skal udføre klassificeret arbejde, der indgår i et NATO-projekt, skal den kunne dokumentere sin sikkerhedsgodkendelse. Dokumentation kan ske ved, at FE besvarer en forespørgsel fra sikkerhedsmyndigheden i det pågældende land – dvs. et Facility Security Clearance Information Sheet (FSCIS).
Dokumentation af den enkelte medarbejders deltagelse i et enkelt møde kan tilvejebringes ved, at virksomheden sender en Request for Visit (RfV) til FE. Se mere om RfV under det tidligere punkt ” **Man skal sørge for at ansøge i god tid** ” i nærværende afsnit.

I det tilfælde at RfV skal suppleres med et certifikat, eller hvor der kun er behov for et certifikat, skal Request for Personnel Security Clearance Confirmation (PSCC) fremsendes til FE. Skabelon til PSCC findes under kapitlet "Link til skrivbare skabeloner på FIIN og internet" i FKOBST 358-1.

8. Meldepligt og rapportering

Virksomhedens sikkerhedschef skal omgående **melde** til Sektionen for Person- og Industrisikkerhed, telefonisk eller pr. e-mail, hvis der på virksomheden er:

- Mistanke om eller konstatering af spionage, sabotage, subversion, terrorvirksomhed samt lignende skadevoldende virksomhed
- Hændelser, der skønnes af sikkerhedsmæssig betydning, herunder indbrudsforsøg, indbrud, tyveri, tab/bortkomst af materiel eller materielgenstande, komponenter m.v.
- Kompromittering af klassificerede oplysninger (dvs. at oplysninger er kommet til uvedkommendes kendskab, eller der er en risiko for, at dette er sket)
- Mistænkelig adfærd
- Brud på eller mistanke om brud på den etablerede fortroligheds-, integritets- og tilgængelighedssikkerhed i informationssystemer.

Virksomhedens sikkerhedschef skal søge oplyst hos Sektionen for Person- og Industrisikkerhed, om der er særlige hensyn at tage, eller om yderligere foranstaltninger skal iværksættes, f.eks. øjeblikkelig kontakt til politiet.

En skriftlig rapport skal umiddelbart efter enhver mistanke eller konstatering af sikkerhedsbrud fremsendes til Sektionen for Person- og Industrisikkerhed. Rapporten skal indeholde flest mulige af nedennævnte punkter:

- 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, samt hvilke undersøgelser der i øvrigt er foretaget – herunder om politiet 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.

Som beskrevet i pkt. 1, skal den indstillende myndighed og evt. hovedleverandør underrettes snarest muligt i tilfælde af lukning af virksomheden eller konkurs, således at der kan foretages inddragelse af klassificeret materiale. Endvidere skal FE underrettes, hvis der planlægges ejerskifte/fusion eller virksomheden ændrer navn.