

Vejledning

om virksomhedssikkerhed

Version 1.2.1

Indhold

1.	Virksomhedsgodkendelse	3
	Om vejledningen	3
	Behovet for godkendelse	3
	Godkendelsesproceduren	3
	Sikkerhedsansvaret i virksomheden	4
	Uddannelse.....	4
	Ejerskifte mv.	4
2.	Personelsikkerhed	5
	Personkredsen	5
	Beslutningsgrundlaget.....	5
	Godkendelsesproceduren	6
	Fratrædelseserklæringer	7
	Informationspligten.....	7
3.	Dokumentsikkerhed	7
	Klassifikation	7
	Registrering og reproduktion mv.	8
4.	Transport og forsendelse	8
	Medbringelse uden for virksomheden.....	8
	Forsendelse	8
	Transport af materiale.....	9
5.	IT-sikkerhed	9
	Internettet - herunder virksomhedens netværk.....	9
	Netværk og PC'er der højest skal behandle TIL TJENESTEBRUG.....	9
	Netværk og PC' der skal behandle FORTROLIGT og højere	10
	Lagermedier	10
	Udstyr til videokonferencer	10
	Password.....	10
	Mobiltelefoner og trådløse telefoner.....	10
6.	Fysisk sikkerhed	10
	Risikovurdering (risikoanalyse)	11
	Områdeinddeling/sikringsniveau	11
	Mekanisk sikring.....	11
	Elektronisk overvågning	11
	Bevogtning	11
	Adgangskontrol	11
	Kontorsikkerhed	11
7.	Internationale forhold	12
	Procedurer for besøg i udlandet	12
	Rejsevejledninger	13
	Dokumentation af Sikkerhedsgodkendelse.....	13

1. Virksomhedsgodkendelse

Om vejledningen

Denne vejledning giver basal information om regler og procedurer for danske virksomheder, der skal udføre sikkerhedsmæssigt klassificeret arbejde for forsvaret. De mere detaljerede sikkerhedsbestemmelser med gældende minimumskrav fremgår af FORSVARSKOMMANDOBESTEMMELSE 358-1 ([FKOBST 358-1](#)).

Rådgivning kan hentes ved Virksomhedssikkerhedssektionen (tlf. 33 32 55 66 – lokal 3422).

Vejledningen vil løbende blive justeret og udbygget bl.a. på grundlag af spørgsmål og forslag fra sikkerhedscheferne.

Behovet for godkendelse

Virksomheder, der udfører sikkerhedsmæssigt klassificeret arbejde for forsvaret, skal være sikkerhedsgodkendte af FE (Virksomhedssikkerhedssektionen).

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

Sikkerhedsgodkendelse 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 kundemyndigheden, sikkerhedsgodkendes blot det nødvendige antal medarbejdere. Disse medarbejdere knyttes herefter sikkerhedsmæssigt til den pågældende myndighed. Det klassificerede arbejde må ikke iværksættes, før konsulenterne er sikkerhedsgodkendte.

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 (se [ledsageskrivelsen](#)).

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 videregives.

Godkendelsesproceduren

Følgende kan indstille en virksomhed til sikkerhedsgodkendelse:

- Forsvarsministeriet
- Forsvarskommandoen (FKO)
- Hjemmeværnskommandoen (HJK)
- Forsvarets Materieltjeneste (FMT)
- Forsvarets Koncernfælles Informatiktjeneste (FKIT)
- Forsvarets Bygnings- og etablisementstjeneste (FBE)
- Organisationen Dansk Industri
- Sikkerhedsgodkendte virksomheder kan indstille om godkendelse af deres underleverandører (dette [indstillingsskema](#) benyttes).

Indstillende myndighed/virksomhed bør gøre tilbudsgivere opmærksom på, at der ved

eventuel kontrakt eller arbejde kan komme udgifter til sikkerhedsforanstaltninger, der er nødvendige for 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. Virksomheden skal ved mødet fremlægge et sammenskrevet resumé fra Erhvervs- og Selskabsstyrelsen, så ejerforhold og økonomiske forhold bliver oplyst. Virksomheden meddeles godkendelse, når de af FE stillede krav er opfyldte.

I forbindelse med mødet udleveres oplysningskemaer til brug for persongodkendelsen af ledelsen og de medarbejdere, der skal have adgang til klassificerede informationer.

Det er normalt et krav, at virksomhedslederen, bestyrelsesformanden, samtlige bestyrelsesmedlemmer, sikkerhedschefen (og evt. stedfortræder) sikkerhedsgodkendes af FE til virksomhedens klassifikationsgrad, dog som minimum til FORTROLIGT.

Når de nødvendige sikkerhedsforanstaltninger er foretaget, persongodkendelserne foreligger 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 for hvilket tidsrum.

Sikkerhedsansvaret i virksomheden

Ansvar for sikkerheden i virksomheden påhviler virksomhedens chef (indehaveren/øverste direktør). Han skal sørge for, at der udstedes en sikkerhedsinstruks med de lokale bestemmelser for sikkerhedsmiljøet. Han 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 ifm. vejledende sikkerhedseftersyn mv.
- Omgående rapportering til FE om alle sikkerhedsbetydende hændelser (spionage, sabotage, angreb mod klassificerede IT-systemer, kompromittering af klassificerede oplysninger mv.).

Uddannelse

Virksomhedssikkerhedssektionen afholder hvert år i maj måned et grundkursus for nye sikkerhedschefer. Grundkurset er obligatorisk.

Ejerskifte mv.

Planlægges der ejerskifte eller fusion, skal virksomheden snarest underrette Virksomhedssikkerhedssektionen om det kommende ejerforhold. Er ejerskiftet så langt fremskredet, at det allerede er registreret i Erhvervs- og Selskabsstyrelsen, medsendes et resumé.

Det er virksomhedens ansvar snarest muligt at underrette Virksomhedssikkerhedssektionen, den indstillende myndighed og 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 fra-

trædelseserklæringer til Virksomhedssikkerhedssektionen.

2. Personelsikkerhed

De detaljerede regler for personelsikkerhed findes i kapitel 2 i [FKOBST 358-1](#)

Personkredsen

I henhold til Statsministeriets cirkulære nr. 204 af 7. december 2001 (sikkerhedscirkulæret) skal personer, der får adgang til klassificerede informationer, være sikkerhedsgodkendte. For ansatte i virksomheder, der leverer varer eller tjenesteydelser til forsvaret, er det FE der foretager godkendelsen.

Det er normalt et krav, at virksomhedslederen, bestyrelsesformanden, samtlige bestyrelsesmedlemmer og sikkerhedschefen (og evt. stedfortræder) er sikkerhedsgodkendte til virksomhedens klassifikationsgrad, dog som minimum FORTROLIGT.

Desuden skal de medarbejdere i virksomheden, der skal have adgang til sikkerhedsmæssigt klassificerede oplysninger, være sikkerhedsgodkendte af FE.

Godkendelse til HEMMELIGT kan tidligst opnås, når pågældende har været ansat i virksomheden i mindst et år og har været sikkerhedsgodkendt til FORTROLIGT i mindst seks måneder. FE kan i særlige tilfælde dispensere fra denne regel.

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. Sager om sikkerhedsgodkendelse behandles efter Forvaltningslovens regler, herunder reglerne om partshøring, aktindsigt, begrundelse af afgørelser og klagevejledning.

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 inden for Forsvarsministeriets område og fra Politiets Efterretningstjeneste (PET). Ved godkendelser til de lavere klassifikationsgrader foretager PET normalt kun et registermæssigt check af, om personen er kendt i politiets registre, herunder mht. strafbare forhold, misbrugsproblemer og fremstillinger i retten. Ved godkendelser til de højeste klassifikationsgrader foretager PET en grundigere personundersøgelse, hvor der evt. indhentes oplysninger fra tidligere arbejdsgivere, uddannelsesinstitutioner, forretningsforbindelser og andre, der kender den undersøgte.

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. Sikkerhedschefen bør søge information om mulighederne for at opnå sikkerhedsgodkendelse, hvis det overvejes at indstille en udlænding, der har opholdt sig mindre end 7 år i Danmark.

I forbindelse med sikkerhedsgodkendelser får FE kun oplysninger fra Politiets Efterretningstjeneste, hvis den pågældende person har givet sit udtrykkelige samtykke hertil på oplysningsskemaet.

Bortset fra Kriminalregisterets oplysninger om domme og sigtelser forelægger PET alle oplysninger for "Wamberg-udvalget", der fører kontrol med PET's og FE's registre-

ringer. FE tilintetgør alle oplysninger om en person, når der ikke længere er behov for, at den

pågældende har en sikkerhedsgodkendelse. Oplysninger om sikkerhedsgodkendte personer tilintetgøres således, så snart FE får meddelelse om, at der ikke længere er behov for en sikkerhedsgodkendelse. Wamberg-udvalget fører kontrol med, at oplysninger tilintetgøres som beskrevet.

Godkendelsesproceduren

Indstilling om persongodkendelse sker ved, at virksomhedens sikkerhedschef tilsender FE et udfyldt oplysningsskema. Der benyttes et af følgende skemaer:

- [Oplysningsskema I](#) benyttes ved indstillinger om godkendelse til TIL TJENESTEBRUG og FORTROLIGT (benyttes både ved 1. gangsgodkendelse og fornyelser)
- [Information form I](#) er en engelsksproget version.
- [Oplysningsskema II](#) benyttes ved indstillinger om 1. gangs godkendelse til HEMMELIGT (dette skema skal benyttes, selvom den pågældende ikke umiddelbart opfylder kravet om 1 års ansættelse i virksomheden og 6 måneders godkendelse til FORTROLIGT).
- [Information form II](#) er en engelsksproget version.
- [Oplysningsskema III](#) benyttes ved indstillinger om fornyelse af godkendelse til HEMMELIGT.
- [Information form III](#) er en engelsksproget version.

Oplysningsskemaerne indeholder en samtykkeerklæring, som FE skal have med original underskrift. Skemaerne kan derfor ikke tilsendes FE pr. E-mail, men skal sendes med posten (ikke rekommanderet) til adressen:

Forsvarets Efterretningstjeneste
Virksomhedssikkerhedssektionen
Kastellet 30
2100 København Ø

Det er meget vigtigt, at skemaerne bliver udfyldt omhyggeligt. Hvis der f.eks. i pkt. 10 i oplysningsskema II (1. gangsgodkendelse til HEMMELIGT) ikke er angivet adresser for tidligere beskæftigelse mv., så returnerer Virksomhedssikkerhedssektionen skemaet med forsinkelse til følge.

Ved udfyldelsen af Oplysningsskemaerne giver medarbejderen oplysninger, der kan anses for personfølsomme (oplysning om ægtefælle/registreret partner, om rejser til udlandet og om økonomiske forhold). Medarbejderen bør derfor gøres opmærksom på, at han kan lægge skemaets første sider i en lukket kuvert sammen med evt. bilagsmateriale om økonomiske forhold. Skemaets sidste side, der indeholder virksomhedens påtegning og underskrift, vedlægges af sikkerhedschefen ved fremsendelsen til FE.

FE meddeler sikkerhedsgodkendelser ved et brev til virksomhedens sikkerhedschef.

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

Sikkerhedsgodkendelser har følgende gyldighedsperioder:

TIL TJENESTEBRUG	(NATO RESTRICTED)	5 år
FORTROLIGT	(NATO CONFIDENTIAL)	5 år

Fratrædelseserklæringer

Når en sikkerhedsgodkendt medarbejder forlader virksomheden eller skifter til en anden funktion, der ikke kræver sikkerhedsgodkendelse, skal den pågældende underskrive en [fratrædelseserklæring](#).

Fratrædelseserklæringen skal opbevares i virksomheden i 5 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, flytninger til udlandet.
- Dødsfald, pensionering, afskedigelse og anden årsag til, at behovet for sikkerhedsgodkendelse bortfalder.
- Forhold i øvrigt, der kan være af betydning for den sikkerhedsmæssige vurdering af den pågældende.

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.

Klassifikation

Der anvendes følgende klassifikationsgrader:

NATIONAL (Dansk)	NATO	EU
YDERST HEMMELIGT (YHM)	COSMICTOP 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.

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

Registrering og reproduktion mv.

Det skal til enhver tid være registreret, hvor i virksomheden det klassificerede materiale befinder sig. Materiale klassificeret FTR 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.

Når virksomheden ikke længere har behov for det klassificerede materiale, skal det normalt returneres til den myndighed, som det er modtaget fra.

4. Transport og forsendelse

Det detaljerede regelsæt og blanketter mv. vedrørende medbringelse uden for tjenestestedet af klassificeret materiale findes i Kapitel 4 i [FKOBST 358-1](#).

Medbringelse uden for 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:

- Medbringelse skal være bemyndiget af virksomhedslederen eller sikkerhedschefen.
- En [fortegnelse](#) over det medbragte materiale skal opbevares i virksomheden.
- Personer, der har materialet i varetægt under rejsen, skal være sikkerhedsgodkendte 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 (certifikater udstedes af Virksomhedssikkerhedssektionen).
- Materiale klassificeret NATO SECRET eller NATO CONFIDENTIAL må ikke medbringes 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 forsendes med kurér, dog kan forsendelse inden for Danmark ske ved rekommanderet post.
- HEMMELIGT klassificeret post må kun forsendes med kurér.

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 over materialet, der skal transporteres.
- 4) Personer, der gennemfører transporten, skal 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, således:
 - Under transport til/fra udlandet skal Courier Certificate bilag 8-I-2 og/eller bilag 8-I-3 samt Certificate of Security Clearance (bilag 8-I-4) medbringes. Begge certifikater udstedes af Virksomhedssikkerhedssektionen ved FE. Efter transportens gennemførelse returneres bilag 8-I-2 og/eller bilag 8-I-3 i udfyldt stand til Virksomhedssikkerhedssektionen
 - Under transport inden for landets grænser skal Certificate of Security Clearance (bilag 8-I-4 og/eller bilag 8-I-5) medbringes. Certifikatet udstedes af Virksomhedssikkerhedssektionen ved FE.

5. IT-sikkerhed

De detaljerede regler for IT-sikkerhed (benævnes informationssikkerhed i det danske forsvar) findes i kapitel 6 i [FKOBST 358-1](#).

Informationssikkerhed har til formål at sikre fortrolighed, integritet og tilgængelighed for informationer på IT- og kommunikationssystemer.

Internettet - herunder virksomhedens netværk.

Der eksisterer principielt ingen sikkerhed på Internettet. Det er for tiden ikke muligt at etablere tekniske løsninger, der med tilstrækkelig sikkerhed forhindrer uønsket indtrængning i tilkoblede systemer. Der må derfor ikke til internettet tilsluttes elektroniske systemer, herunder PC'er eller PDA'er, der behandler klassificerede eller sensitive informationer.

Der må ikke sendes klassificerede informationer på internettet. Kommercielle kryptosystemer giver ikke tilstrækkelig sikkerhed.

Netværk og PC'er der højst skal behandle TIL TJENESTEBRUG

Enkeltstående PC'er og netværk, der benyttes til behandling af informationer, der er klassificeret TIL TJENESTEBRUG, skal etableres således:

Netværket skal være separeret fra resten af virksomhedens netværk.

Der skal være etableret fysik sikkerhed således at der ikke må kunne ske uerkendt adgang til området, låsen skal være af type SKAFOR rød, der skal være åbningskontakt på døren og IR overvågning af lokalet med en reaktionstid, der skal være aftalt med politi eller vagtselskab.

Rådgivning vedr. etablering af disse installationer kan fås ved Forsvarets Koncernfælles IT-tjeneste.

Installationen skal godkendes af FE før ibrugtagning

Netværk og PC' der skal behandle FORTROLIGT og højere

De tekniske sikkerhedskrav til IT-systemer, der behandler informationer klassificeret FORTROLIGT og opefter, er komplicerede og hviler i vidt omfang på klassificerede NATO-bestemmelser. De sikkerhedsgodkendte virksomheder henvises derfor til at rette forespørgsel til FE, hvis de ønsker at etablere sådanne.

Lagermedier

Lagermedier (harddiske og disketter mv.) skal være afmærkede med den brugende medarbejders navn og klassifikationen. Lagermedier må ikke genanvendes i lavere klassificerede netværk.

Lagermedier, der har været benyttet til behandling af alle typer af klassificerede informationer, må ikke forlade virksomhedens kontrol (dvs. gives væk, sælges eller på anden måde anvendes uden for virksomheden).

Fsva. medier, der har været anvendt til TIL TJENESTEBRUG, skal disse destrueres ved virksomhedens foranstaltning.

Fsva. medier, der har været anvendt til FORTROLIGT og højere, skal disse destrueres ved FE mellemkomst.

Bærbare PC'er skal fysisk beskyttes, opbevares og transporteres i forhold til klassifikationsgraden for de informationer, der behandles på PC'en.

Udstyr til videokonferencer

Videokonferenceudstyr må kun benyttes til formidling af klassificeret information, hvis FE har godkendt det samlede system. Opmærksomheden henledes på, at det er relativt enkelt at placere akustisk aflytningsudstyr. FE er derfor behjælpelig med at foretage tekniske sikkerhedseftersyn af videokonferencelokalet og evt. tilstødende lokaler.

Password

Adgang til klassificeret information på netværk og PC'er skal være beskyttet med password. Passwords er personlige og må ikke videregives til andre. Passwords skal vælges således, at de ikke let kan gættes (ikke navne og begreber knyttet til familien og fødselsdage mv.).

Ved opsætning af operativsystemet skal det sikres, at password udløber efter maksimalt 180 dage, består af mindst 9 tegn, heraf skal anvendes tegn fra minimum 3 ud af 4 karaktersæt (store/små bogstaver, tal og specialtegn).

Mobiltelefoner og trådløse telefoner

Mobiltelefoner må ikke benyttes til at udveksle information, der er klassificeret. Mobiltelefoner og trådløse telefoner må ikke medbringes i mødelokaler, hvor der udveksles informationer, der er klassificerede FORTROLIGT eller højere.

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 Virksomhedssikkerhedssektionen fastsætte, hvilke yderligere sikringsforanstaltninger, der skal etableres.

Påtænker virksomheden at foretage bygnings- og lokalemæssige ændringer, der er af

sikkerhedsmæssig betydning, skal der straks rettes henvendelse til Virksomhedssikkerhedssektionen. 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 spionage (inkl. industrispionage), sabotage, hærværk og tyveri. Egentlig bevogtning udføres af vagtmandskab, portner, receptionist e. lign. 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 blindes med gardiner/persienner, således at indblik udefra hindres.

Opstilling af elektronisk kontorudstyr (fx edb-udstyr, telefon og telefax) skal overholde gældende bestemmelser i kapitel 6 i [FKOBST 358-1](#). Virksomheden skal endvidere fastsætte regler for brug (og medbringelse) af bærbart edb-udstyr og mobiltelefoner i lokalet.

Virksomheden skal sørge for, at der er opbevaringsmidler (penge- og sikringskabe) med en sikkerhedsklassifikation, der tillader opbevaring af det klassificerede materiale. Virksomheden skal tilvejebringe udstyr (fx makulatorer), der opfylder kravene til tilintetgørelse af informationsbærende materiale (fx papir, view-foils, disketter, 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](#)

Procedurer for besøg i udlandet

Hvis der under besøg i udlandet skal drøftes klassificerede forhold, skal både besøgsmodtageren og den besøgende være sikkerhedsgodkendte til den pågældende klassifikationsgrad. Dette sikres gennem en internationalt aftalt procedure, hvor den besøgende via sit hjemlands sikkerhedsmyndighed ansøger besøgslandet om en besøgstilladelse.

Selvom man ikke påtænker at drøfte klassificerede forhold, skal der altid søges om tilladelse forud for besøg på militære etableringer og sikkerhedsgodkendte virksomheder i udlandet.

Har man ikke fået tilladelsen før sin ankomst til landet, vil man normalt blive nægtet adgang til besøgsstedet.

Virksomhedssikkerhedssektionen ved FE udfærdiger de nødvendige dokumenter i forbindelse med besøg. Der kan være tale om et antal besøg inden for en defineret periode.

Den danske virksomheds sikkerhedschef skal i god tid før besøget i udlandet tilsende FE en udfyldt [besøgsanmodning](#). 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.

Skemaet kan sendes enten med posten, eller ved [e-mail](#).

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

- a. Besøgets forventede klassifikationsgrad (Virksomhedssikkerhedssektionen undersøger, om firmaet er sikkerhedsgodkendt til den krævede klassifikation).
- b. Besøgsmodtager
 - Virksomhedens navn
 - Virksomhedens adresse
 - Virksomhedens telefon nr.
 - Virksomhedens kontaktpersoner
- c. Besøgende
 - Fulde navn
 - Fødselsdato
 - Fødested
 - Nationalitet
 - Sikkerhedsgodkendelse

- Pasnummer og eventuel ID-kort nr.

d. Egen virksomhed

- Årsag til besøg
- Kopi af en eventuel invitation.
- Besøgsperiode (fra/til).

Den ansøgende virksomhed eller person vil fra Virksomhedssikkerhedssektionen 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.

Efter hjemkomsten bør sikkerhedschefen evt. indhente oplysninger om, hvorvidt medarbejderen har været udsat for hændelser af sikkerhedsmæssig karakter eller af usædvanlig art. Disse oplysninger viderebringes til Virksomhedssikkerhedssektionen ved FE.

Klik her for orientering om reglerne for [transport og forsendelse](#) af klassificeret materiale.

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. Dokumentationen kan tilvejebringes ved, at FE udsteder et "NATO Facility Security Clearance Certificate". Dokumentation kan også ske ved, at FE besvarer en FIS (Facility Security Clearance Information Sheet) fra sikkerhedsmyndighed i det pågældende land.

Der er indgået aftaler med en række lande om gensidig anerkendelse af sikkerhedsaftaler, herunder med de fleste NATO og EU-lande (Virksomhedssikkerhedssektionen kan oplyse, om der er indgået aftale med et givet land). Ved klassificeret arbejde for myndigheder eller virksomheder i disse lande vil sikkerhedsgodkendelsen af den danske virksomhed normalt skulle dokumenteres ved, at FE besvarer en FIS.

-----ooOoo-----