Ej sekretess

Datum	Diarienummer	Ärendetyp
2019-12-20	19FMV6705-1:1	Beslut
	Dokumentnummer	Sida
	ange	1(57)
Giltig t.o.m.	Upphäver	
Tills vidare	15FMV11468-2:1	

Beslutande

Anders Sjöborg,
Chef Jurstab

Föredragande

Johan Bendz,
Jurstab Säk

Tjänsteföreskrift avseende säkerhetsskydd och sekretess (2020)

< 7 bilagor, 1 underbilaga>

Innehåll

1 Inledning

1.1 Syfte och omfattning

Syftet med denna tjänsteföreskrift (TjF) är att identifiera och omhänderta de krav i lagar, förordningar och föreskrifter som gäller för sekretess och FMV:s säkerhetskänsliga verksamhet. Utöver dessa redovisar TjF av FMV formulerade bestämmelser inom området.

Kapitel 4-19 i denna TjF, tillsammans med bilagorna 2-7, innehåller bestämmelser för FMV rörande säkerhetskänslig verksamhet, säkerhetsskydd, sekretess, hantering av säkerhetsskyddsklassificerade eller sekretessreglerade uppgifter, samt hantering av säkerhetskänslig materiel.

Denna TjF kompletteras med vägledningar som beskriver hur bestämmelserna kan uppfyllas inom utvalda områden. Vägledningarna riktar sig till all FMV personal, medan TjF i huvudsak riktar sig till beslutsfattare och aktörer inom säkerhetsskyddsfunktionen.

I inledningen av vissa kapitel redovisas en s.k. verksamhetslogik, vars syfte är att redovisa förekommande övergripande principer.

1.2 Kravkällor

Förkortningar enligt detta avsnitt och avsnitt 2.2 tillämpas i denna TjF.

1.2.1 Externa kravkällor

Bestämmelser om säkerhetsskydd och sekretess, vilka beaktas i denna TjF, finns främst i:

- säkerhetsskyddslagen (2018:585), SSL
- offentlighets- och sekretesslagen (2009:400), OSL
- säkerhetsskyddsförordningen (2018:658), SSF
- offentlighets- och sekretessförordningen (2009:641), OSF
- förordning (2010:649) om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet
- Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2019:2), FFS-SäkS
- Försvarsmaktens föreskrifter om signalskyddstjänst inom totalförsvaret (FFS 2019:9), FFS-SigS

Andra bestämmelser som relaterar till säkerhetsskydd och sekretess finns i:

- skyddslagen (2010:305), SKL
- lag (2000:130) om försvarsunderrättelseverksamhet, LFU
- lag (1971:1078) om försvarsuppfinningar, FUL
- skyddsförordningen (2010:523), SKF
- förordning (2000:131) om försvarsunderrättelseverksamhet, FFU
- Riksarkivets myndighetsspecifika föreskrifter om gallring och annan arkivhantering (RA-MS 2018:42), RAMS
- Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2), PMFS

1.3 Interna kravkällor

Som grund för denna tjänsteföreskrift ligger även:

- Arbetsordning Försvarets materielverk 2019 (18FMV7202-3:1), ArbO FMV
- FM-FMV Samordningsöverenskommelse 2019 (18FMV8760-1:1), SAMO
- FMV Beslut avseende informationshantering vid FMV (skr 21835:62745/2005, 2005-09-07)
- FMV Beslut avseende informationshantering vid FMV (skr VO Kom Tjänst 21835:82752/05, 2005-11-29)
- Signalskyddsinstruktion Försvarets materielverk (19FMV6857-1:1), SSI

1.4 Beroenden

Vid arbete med säkerhetsskydd och sekretess är det även nödvändigt att ta hänsyn till andra regleringar än de som är direkt styrande för denna TjF eller som denna TjF refererar till. Exempel på sådana regleringar är:

- FMV TjF för Användning av FMV:s IT-system (15FMV11909-1:1)
- Ackrediteringsmetod FMV IT-system (18FMV3427-3:1)
- FMV TjF avseende utlämning av allmän handling (15FMV12043-1:1)
- FMV TjF för hantering av personuppgifter (18FMV4221-1:1)

Det finns även beroenden till internationella avtal i form av bi-/multilaterala säkerhetsskyddsöverenskommelser. Se kapitel 16.

Förutom SAMO (FM-FMV) finns motsvarande med FRA och FOI. Dessa innehåller regleringar som har betydelse för säkerhetsskyddet.

Andra hänsyn kan även behöva tas inom specifika verksamheter, exempelvis FMV Patent med de regleringar som framgår av FUL.

I det praktiska arbetet med säkerhetsskyddsplanering finns även beroenden till exempelvis hotbildsanalyser (utarbetas av såväl Säkerhetsskyddsavdelningen som IT-Stab).

1.5 Referenser, spårbarhet och förtydliganden

För såväl bestämmelser (krav, normativ text) som för informativ (icke normativ) text i denna TjF redovisas i tillämpliga fall referenser i parentes efter det aktuella stycket, t.ex. (Ref: 2 kap. 2 § SSL).

Referenser till författningskrav följer principen att endast källan "närmast" FMV anges, t.ex. FFS-SäkS. Dessa krav bygger ibland på krav i SSF, som i sin tur bygger på krav i SSL. Fullständig spårbarhet finns dokumenterad och kan redovisas på begäran.

När inget annat anges är det FMV som är källan till uppgifterna i denna TjF.

[Förtydligande hjälptext inom hakparenteser] har vid behov tillförts definitioner, citat ur annan författning eller annan text som betjänas av detta.

1.6 Bilageförteckning

Bilaga 1 Instruktion och beslutsmall för lokal delegeringsordning

Bilaga 2 Krav för ytor och förvaringsenheter (byggnads- och förvaringsnormer)

Bilaga 3 Godkända id-handlingar

Bilaga 4 Godkända signalskydds- och kryptosystem

Bilaga 5 Godkända förstöringsmetoder

Bilaga 6 Anteckningar om sekretess respektive säkerhetsskyddsklass

Bilaga 7 Skyddad transport - Transportnivåer

2 Termer, definitioner och förkortningar

2.1 Termer och definitioner

Allmän handling

Handling som förvaras hos myndighet och är att anse som inkommen till eller upprättad hos myndighet.
(Ref: 2-1 kap. 3 § TF)

Delegeringsordning

Beslut om delegering av befogenhet att fatta viss typ av beslut.

Chef

Anställd som har verksamhetsansvar och arbetsgivaransvar samt i regel även ekonomiskt ansvar för en resultatenhet.
(Ref: sid. 5 ArbO FMV)

Not: I denna TjF avses med termen chef normalt verksamhetsansvarig chef enligt definitionen ovan. I några fall specialiseras termen med ett diskriminerade förled för ökad tydlighet, t.ex. personalansvarig chef.

Delgivning

Det att yppa eller på annat sätt tillgängliggöra/överföra säkerhetsskyddsklassificerade uppgifter.

Not: Termen delgivning avser överföring av uppgifter inom ramen för FMV:s verksamhet, alternativt inom ramen för säkerhetskyddsavtal, internationella säkerhetsskyddsåtaganden eller internationella säkerhetsskyddsöverenskommelser.

Distribution

Förmedling av försändelse.

Elektronisk handling

Upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel (upptagning för automatiserad behandling).
(Ref: 1 kap. FFS-SäkS)

Elektroniskt kommunikationsnät

Ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.
(Ref: 1 kap. FFS-SäkS)

Enskild verksamhetsutövare

Privat eller statligt bolag.
(Ref: Säpo websida Registerkontroll och säkerhetsklass, 2019-05-20)

FMV personal

Vid FMV anställd och inhyrd personal.

Gemensam användning

Arrangemang där flera personer bemyndigats tillgång till utpekad resurs (handling, lagringsmedium, materiel etc.) som omfattas av sekretess eller säkerhetsskydd.

Handling

Framställning [av uppgifter] i skrift, bild eller upptagning som kan läsas, avlyssnas eller uppfattas med något tekniskt hjälpmedel.
(Ref: 2-1 kap. 3 § TF)

Not: Under termen handling faller, förutom olika former av fysiska dokument, även elektroniska handlingar.

Incidör

Den "felande parten" i en incident.

Informationssystem

Ett system av sammansatt program- och maskinvara som behandlar information.
(Ref: 1 kap. 5 § SSF)

Inhyrd personal

Uppdragstagare som arbetsleds av FMV. Utgör normalt resursförstärkning som löser uppgifter som FMV-anställda annars skulle lösa.

IT-utrymme

Utrymme som innehåller växlar, korskopplingar och servrar, samt datorhallar.
(Ref: 1 kap. FFS-SäkS)

Lagringsmedium

Permanent eller redigerbar databärarare som används för att lagra uppgifter.
(Ref: 1 kap. FFS-SäkS)

Medförande

Förfarande då behörig innehavare tar med sig handling, lagringsmedium eller materiel utanför FMV:s lokaler/verksamhetsställe.

Registerkontroll

Utdrag av uppgifter från belastningsregistret, misstankeregistret samt uppgifter som behandlas med stöd av lagen om polisens behandling av personuppgifter inom brottsdatalagens område.
(Ref: 3 kap. 13 § SSL)

Samförvaring

När flera personer genom behörighetsbeslut bemyndigas nyttjande av gemensamt förvaringsutrymme, inom vilket respektive person kan hantera sina skyddsvärda tillgångar separat.

Not: Exempel är användning av ett säkerhetsskåp med låsbara innerfack.

Sekretess

Förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling **eller på något annat sätt**.
(Ref: 3 kap. 1 § OSL)

Skadlig kod

Otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett informationssystem.
(Ref: 1 kap. FFS-SäkS)

Skydd

Egenskap eller mekanism som motverkar eller förhindrar oönskad händelse och/eller dess konsekvens.

Skyddsklass

Byggnorm enligt Stöldskyddsföreningen.

Sveriges säkerhet

Säkerhet för nationens oberoende och bestånd.
(Ref: Säpo Vägledning - Introduktion till säkerhetsskydd 2019)

Säkerhet

Tillstånd med acceptabel risk.

Säkerhetskänslig befattning

Anställning eller annat deltagande i säkerhetskänslig verksamhet.

Säkerhetskänslig materiel

Materiel som innehåller/avspeglar säkerhetsskyddsklassificerade uppgifter eller som är oundgänglig för bedrivande av säkerhetskänslig verksamhet.

Säkerhetskänslig verksamhet

Verksamhet som är av betydelse för Sveriges säkerhet, eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.
(Ref: 1 kap. 1 § SSL)

Säkerhetsskydd

Skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd, i andra fall, av säkerhetsskyddsklassificerade uppgifter.
(Ref: 1 kap. 2 § SSL)

Säkerhetsskyddsavdelningen

Avdelning inom FMV:s Juridik- och säkerhetsstab.

Säkerhetsskyddsfunktionen

Den samlade säkerhetsskyddsverksamheten i FMV.

Särskilt säkerhetskänslig verksamhet

Verksamhet som anses vara särskilt säkerhetskänslig.

Handling med säkerhetsskyddsklassificerade uppgifter

Handling som innehåller säkerhetsskyddsklassificerade uppgift.
(Ref: 1 kap. 4 § SSF)

Not: I Säkerhetsskyddsförordningen och i Försvarsmakten används termen Säkerhetsskyddsklassificerad handling. Termen används inte i denna TjF, då det enligt SSL är uppgifter som är säkerhetsskyddsklassificerade.

Säkerhetsskyddsklassificerade uppgifter

Uppgifter som rör säkerhetskänslig verksamhet enligt SSL.
(Ref: 1 kap. 2 § SSL)

Lagringsmedium med säkerhetsskyddsklassificerade uppgifter

Lagringsmedium som innehåller eller är avsett att innehålla säkerhetsskyddsklassificerade uppgifter.

Not: I Försvarsmakten används termen Säkerhetsskyddsklassificerat lagringsmedium. Termen används inte i denna TjF, då det enligt SSL är uppgifter som är säkerhetsskyddsklassificerade.

Säkerhetsskyddsåtgärd

Något som görs för att öka förmågan i säkerhetsskyddet.

Uppdragstagare

Av FMV anlitad aktör (leverantör, uppdragskonsult, etc.)

Uppgift

Information eller upplysning (fakta, antagande) om sakförhållande.

2.2 Förkortningar

Se även kapitel 1.2 för förkortningar avseende kravkällor.

CIO

Cheif information officer

FMV

Försvarets materielverk

GD

Generaldirektör

Jurstab

Juridik- och säkerhetsstab

OrgE

Organisationsenhet

Säpo

Säkerhetspolisen

TjF

Tjänsteföreskrift

VerkO/CS

Verksamhetsområde/Central stab

3 Allmänt om säkerhetsskydd och sekretess

3.1 Säkerhetsskydd

Av 1 kap. 2 § SSL framgår att med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten, samt skydd i andra fall [än ovan] av säkerhetsskyddsklassificerade uppgifter.

3.2 Sekretess

Med sekretess avses tystnadsplikt i det allmännas verksamhet och förbud att lämna ut skyddsvärda uppgifter.

Sekretessbestämmelser avser förbud att röja uppgift, vare sig detta sker muntligen, genom utlämnande av allmän handling eller på något annat sätt.

OSL redovisar bestämmelser/kriterier avseende vilka typer av uppgifter som kan vara föremål för sekretess.
(Ref: 1 kap. 1 §, 2 kap. 1 § OSL)

3.3 Hantering av krav på säkerhetsskydd resp. sekretess i denna TjF

För att underlätta läsning och efterlevnad av bestämmelserna i denna TjF tillämpas i flera kapitel principen att först hantera sekretessrelaterade krav och därefter, i tillämpliga fall och under särskild rubrik, hantera säkerhetsskyddsrelaterade krav.

4 Ansvar och beslutsbefogenheter

4.1 Allmänt

4.1.1 Verksamhetslogik för ansvar och beslutsbefogenheter

- Ansvaret för att krav uppfylls åvilar chef. Se avsnitt 4.2.
- Behörig beslutsfattare framgår av lokalt beslut om delegeringsordning för varje VerkO/CS. Se avsnitt 4.3.
- I denna TjF förekommande explicita krav avseende behörig beslutsfattare (t.ex. avseende hantering av Kvalificerat hemliga uppgifter) begränsar i vissa fall handlingsutrymmet för lokala delegeringsordningar enligt ovan.
- Vissa beslut (t.ex. avseende hantering av Kvalificerat hemliga uppgifter) är inte fritt delegeringsbara. Sådana beslut är föreskrivna i denna TjF.

4.2 Ansvar för säkerhetsskyddet

Enligt ArbO FMV har chef verksamhetsansvar för säkerhetsskyddet vid FMV.

4.2.1 Chefers ansvar

Chef ansvarar för att vidta erforderliga säkerhetsskyddsåtgärder, inklusive att genomföra och förvalta säkerhetsskyddsplanering för den egna verksamheten.
(Ref: sid. 5 ArbO FMV)

Not: Vad som utgör erforderliga åtgärder framgår av fattade riskhanteringsbeslut.

Chef VerkO/CS ska utarbeta kompletterande säkerhetsbestämmelser för egen verksamhet inom VerkO/CS, om behov föreligger (identifieras i verksamhetens säkerhetsskyddsplanering).

Chef ansvarar för att lokal säkerhetsskyddsinstruktion och/eller lokal signalskyddsinstruktion beslutas, när behov föreligger.

Not: För beslut som innebär avsteg från bestämmelserna i denna TjF, se avsnitt 21.1.

Chef ansvarar för säkerhetsskyddet för FMV:s projekt.

4.2.2 Övrigas ansvar

Samtliga personer som deltar i FMV:s verksamhet som anställda eller inhyrd personal ansvarar för att:

- uppgifter som bedöms omfattas av säkerhetsskydd och/eller sekretess skyddas i enlighet med kraven i denna TjF, samt att
- meddela närmaste chef om händelser och omständigheter som kan påverka säkerhetsskyddet eller sekretessen.

(Ref: sid. 17 ArbO FMV)

4.3 Beslutsbefogenheter

4.3.1 Allmänt

Formalia kring beslut framgår av ArbO FMV. Där framgår hur beslut ska vara utformade samt att dessa ska dokumenteras.

4.3.2 Delegeringsordning

Chef VerkO/CS ska besluta om en delegeringsordning avseende beslutsbefogenheter enligt denna TjF, som är anpassad till egen verksamhet och organisation. För organisationsenheten GD/ÖD hanteras beslutsbefogenheter i särskild ordning.

5 Säkerhetsskyddsorganisation

5.1 Allmänt

Med säkerhetsskyddsorganisation avses roller, ansvar, mandat och befogenheter inom säkerhetsskydds-funktionen vid FMV.

Chef VerkO/CS ska besluta om vilken säkerhetsskyddsorganisation som behövs för att upprätthålla ett erforderligt säkerhetsskydd inom eget ansvarsområde.

Chef VerkO/CS skall utse säkerhetsskyddskoordinator (se avsnitt 5.3).

5.2 Säkerhetsskyddschef

Säkerhetsskyddschef är den befattning som har det övergripande ansvaret att leda och samordna arbetet med säkerhetsskydd i FMV. FMV:s säkerhetsskyddschef rapporterar direkt till GD.

Säkerhetsskyddschefen placerad på Juridik- och säkerhetsstaben.
(Ref: sid. 7 ArbO FMV, 2 kap. 2 § SSF)

Av ArbO FMV framgår att säkerhetsskyddschefen ska redovisa status avseende FMV:s säkerhetsskydd för GD vid ordinarie verksamhetsuppföljning.
(Ref: sid. 7 ArbO FMV)

5.3 Säkerhetsskyddskoordinator

Säkerhetsskyddskoordinator stödjer Chef VerkO/CS i frågor rörande säkerhetsskydd.

Chef VerkO/CS ansvarar för att säkerhetsskyddskoordinatorn erhåller erforderlig utbildning.

5.4 Signalskyddschef

Signalskyddschefen har till uppgift att ansvara för ledning och samordning av signalskyddstjänsten vid FMV.
(Ref: 1 kap. 8 § FFS-SigSky)

Signalskyddschefen är placerad i Säkerhetsskyddsavdelningen.

Not: FMV:s signalskyddsorganisation framgår av SSI.

6 Säkerhetsskyddsplanering

6.1 Allmänt

Säkerhetsskyddsplanering är en samlande term för de analyser, planer och åtgärder som vidtas av FMV för att utreda vilket säkerhetsskydd som behövs i verksamheten.

Säkerhetsskyddsplanering är den process som syftar till ta fram en säkerhetsskyddsanalys och säkerhets-skyddsplan.

Säkerhetskyddsplanering omfattar:

- Säkerhetsskyddsanalys (inkl. verksamhetsbeskrivning). Se avsnitt 6.2.
- Säkerhetsskyddsplan. Se avsnitt 6.3.
- Säkerhetsskyddsåtgärder (inkl. ev. utfärdande av säkerhetsskyddsbestämmelser). Se avsnitt 6.4.

Säkerhetsskyddschefen ansvarar för att övergripande säkerhetsskyddsplanering för FMV genomförs och att denna utvärderas vartannat år eller vid behov.
(Ref: 2 kap. 2 § FFS-SäkS)

Chef VerkO/CS ansvarar för att säkerhetsskyddsplanering för den egna verksamheten finns beslutad.

För varje uppdrag/projekt ska en dokumenterad och beslutad säkerhetsskyddsplanering finnas.

Den som genomför säkerhetsplanering ska ha av chef bedömt erforderliga kunskaper i säkerhetsskydds-planering.

6.2 Säkerhetsskyddsanalys

För all verksamhet vid FMV ska behovet av säkerhetsskydd utredas. Utredningsaktiviteten och dess resulterande dokumentation benämns båda säkerhetsskyddsanalys.
(Ref: 2 kap. 1 § SSF)

Säkerhetsskyddsanalysen ska:

- omfatta säkerhetsskyddsklassificerade uppgifter och vad som i övrigt behöver ett säkerhetsskydd
- identifiera de delar av verksamheten som är skyddsvärda med hänsyn till Sveriges säkerhet eller relationer till omvärlden
- beakta Försvarsmaktens dimensionerande hotbeskrivning och ta fram en för analysen relevant hotbild, anpassad och aktuell i förhållande till den av FMV analyserade verksamheten.
- identifiera de hot och sårbarheter som finns kopplade till FMV skyddsvärden
- innehålla en bedömning av vilka säkerhetsskyddsåtgärder som är nödvändiga
- dokumenteras och uppdateras

(Ref: 2 kap. 3 § FFS-SäkS)

6.2.1 Verksamhetsbeskrivning

En säkerhetsskyddsanalys ska utgå ifrån en verksamhetsbeskrivning av den verksamhet och organisation som analysen avser, samt dess identifierade skyddsvärden.
(Ref: 2 kap. 3 § FFS-SäkS)

6.3 Säkerhetsskyddsplan

Av säkerhetsskyddsplanen ska det framgå:

- vilka säkerhetsskyddsåtgärder som ska vidtas, vem eller vilka som är ansvariga för att åtgärder genomförs och tidpunkter då åtgärder ska vara genomförda.
- behov av resurser, ansvarsfördelning, organisation, utbildning, övning samt rutiner och säkerhetsskyddsbestämmelser.
- vilka åtgärder som behöver vidtas inför, under eller efter sådana avbrott och störningar i FMV:s säkerhetskänsliga verksamhet som kan medföra mer än ringa skada (kontinuitetsplan).

Planen ska beslutas av verksamhetsansvarig chef.
(Ref: 2 kap. 4 § FFS-SäkS)

6.3.1 Riskhantering

Säkerhetsskyddsplanen omfattar de säkerhetsskyddsåtgärder som chef beslutar att genomföra med utgångspunkt från gjord säkerhetsanalys. Kvarstående risk, efter genomförande av säkerhetsskyddsåtgärder, utgör grund för riskhanteringsbeslut, som kan innebära att risken accepteras alternativ ytterligare begränsas eller överförs till annan part. Kvarstående risk redovisas inom ramen för gjord säkerhetsanalys. Behöver risk eskaleras till verksledningen sker detta enligt fastställa principer för myndighetens övergripande riskhantering.

6.4 Säkerhetskyddsåtgärder

Säkerhetsskyddschefen ska, inom ramen för beredning av FMV:s säkerhetsskyddsplanering, orientera FMV ledning om denna innan den fastställs.
(Ref: 2 kap. 5 § FFS-SäkS)

Chef ska genomföra planerade säkerhetsskyddsåtgärder. Vid behov ska säkerhetsskyddsbestämmelser utges.
(Ref: 2 kap. 1 § SSL)

6.4.1 Säkerhetskyddsbestämmelser

Den som ansvarar för en säkerhetsskyddsplanering ska, om genomförd analys påvisar behovet, utge nödvändiga säkerhetsskyddsbestämmelser för aktuell verksamhet.

För en verksamhet (linje/uppdrag/projekt) ska eventuella säkerhetsskyddsbestämmelser omfatta en informationsklassificeringsguide, som beskriver vilka uppgifter/materiel inom verksamheten som omfattas av sekretess eller krav på säkerhetsskydd.

7 Personalsäkerhet

7.1 Allmänt

FMV personalsäkerhetsverksamhet har som mål att

- förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig, och
- säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd.

(Ref: 2 kap. 4 § SSL)

Med termen "Säkerhetskänslig befattning" avses i denna tjänsteföreskrift "anställning eller annat deltagande [annan medverkan] i säkerhetskänslig verksamhet".

7.1.1 Verksamhetslogik för personalsäkerhet vid FMV

- Identifierade säkerhetskänsliga befattningar placeras i säkerhetsklass. Se avsnitt 7.3.
- Person som avses att tillsättas till en säkerhetskänslig befattning säkerhetsprövas. Se avsnitt 7.4.
- Person tillsätts till säkerhetskänslig befattning. Se avsnitt 7.5.

Not: Formellt är det alltid befattningar som är placerade i säkerhetsklass – aldrig personer
(Ref: Avsnitt 3.4 Säpo Vägledning säkerhetsskydd - Personalsäkerhet)

7.2 Chefs ansvar

Personalansvarig chef ska tillse att säkerhetsprövning genomförs innan en person genom anställning eller på annat sätt deltar i FMV:s säkerhetskänsliga verksamhet.

Personalansvarig chef ska förebygga och vidta rimliga skyddsåtgärder för att minska sårbarheter hos personer som deltar i FMV:s säkerhetskänsliga verksamhet.
(Ref: 6 kap. 7 § FFS-SäkS)

7.3 Identifiering av säkerhetskänsliga befattningar

7.3.1 Analys av befattning

Chef ska analysera vilka säkerhetskänsliga befattningar som finns inom verksamheten, vilka av dessa som ska placeras i säkerhetsklass, samt vilket övrigt deltagande i den säkerhetskänsliga verksamheten som endast ska vara föremål för säkerhetsprövning.

Analysen ska utgå från verksamhetens säkerhetsskyddsanalys och särskilt beakta förekomsten av internationella åtaganden om säkerhetsskydd.

Av analysen ska skälet till placering i säkerhetsklass framgå.

Analysen ska vara beslutad av chef.
(Ref: 6 kap. 3 § FFS-SäkS)

Analysen ska omfatta eventuella begränsningar på grund av dubbelt medborgarskap.

7.3.2 Placering av säkerhetskänslig befattning i säkerhetsklass

En säkerhetskänslig befattning ska placeras i säkerhetsklass 1, om den som innehar befattningen

- i en omfattning som inte är ringa får del av uppgifter i säkerhetsskyddsklassen Kvalificerat hemlig, eller
- till följd av sitt deltagande i verksamheten har möjlighet att orsaka synnerligen allvarlig skada.

(Ref: 5 kap. 7 § SSF)

En säkerhetskänslig befattning ska placeras i säkerhetsklass 2, om den som innehar befattningen

- i en omfattning som inte är ringa får del av uppgifter i säkerhetsskyddsklassen Hemlig,
- i ringa omfattning får del av uppgifter i säkerhetsskyddsklassen Kvalificerat hemlig, eller
- till följd av sitt deltagande i verksamheten har möjlighet att orsaka allvarlig skada.

(Ref: 3 kap. 7 § SSL)

En säkerhetskänslig befattning ska placeras i säkerhetsklass 3, om den som innehar befattningen

- får del av uppgifter i säkerhetsskyddsklassen Konfidentiell,
- i ringa omfattning får del av uppgifter i säkerhetsskyddsklassen Hemlig, eller
- till följd av sitt deltagande i verksamheten har möjlighet att orsaka en inte obetydlig skada.

(Ref: 3 kap. 8 § SSL)

En säkerhetskänslig befattning ska också i andra fall än sådana som följer av ovan placeras i en säkerhetsklass som motsvarar de krav på säkerhetsprövning som följer av ett internationellt åtagande om säkerhetsskydd.
(Ref: 3 kap. 9 § SSL)

7.3.3 Omprövning/ändring av placering av befattning i säkerhetsklass

Placering av säkerhetskänslig befattning i säkerhetsklass ska omprövas om förutsättningarna för placeringen väsentligen har ändrats.

Om den säkerhetskänsliga befattningens placering i säkerhetsklass ändras, ska ansvarig chef skyndsamt rapportera ändrade förhållanden till Säkerhetsskyddsavdelningen, för vidare anmälan till Säpo.
(Ref: 5 kap. 22 § SSF)

7.4 Säkerhetsprövning av person

Verksamhetsansvarig chef ansvarar för att den som avses inneha en säkerhetskänslig befattning, eller på något annat sätt ska delta i säkerhetskänslig verksamhet inom FMV, är säkerhetsprövad. Detta gäller oavsett formen för deltagandet (anställd, inhyrd personal, samarbetspartner, etc.).

Säkerhetsprövning ska genomföras av personalansvarig chef med stöd av för uppgiften särskilt utbildad personal.
(Ref: 6 kap. 2 § FFS-SäkS)

Säkerhetsprövningen ska dokumenteras.
(Ref: 6 kap. 1 § FFS-SäkS)

Not: Säkerhetsprövningen syftar till att klarlägga om en person kan antas vara lojal mot FMV:s intressen och i övrigt pålitlig från säkerhetssynpunkt.
(Ref: 3 kap. 2 § SSL)

Not: Särskilda regler gäller i förhållandet mellan Försvarsmakten och FMV avseende säkerhetsprövning.
(Ref: Annex A.11.4 SAMO)

7.4.1 Allmänt om säkerhetsprövning

Av 3 kap. 3 § SSL framgår att säkerhetsprövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas.

Not: Den som har fått del av uppgifter som förekommer i säkerhetsprövningsärende får inte obehörigen röja eller utnyttja dessa uppgifter.
(Ref: 5 kap. 1 § SSL)

Av 3 kap. 2 § SSL framgår att vid säkerhetsprövningen ska sådana omständigheter beaktas som kan antas innebära sårbarheter i säkerhetshänseende.

Vid säkerhetsprövning av personer som ska tillsättas till befattning i säkerhetsklass 1 ska Säkerhetsskydds-avdelningen medverka vid säkerhetsprövningssamtalet.

7.4.2 Omfattning av säkerhetsprövning

Säkerhetsprövningen ska normalt innefatta en grundutredning och ofta även en registerkontroll. I vissa fall genomförs dessutom en särskild personutredning.
(Ref: 3 kap. 3 § SSL)

Not: Av 3 kap. 3 § SSL framgår att om det finns särskilda skäl får säkerhetsprövningen göras mindre omfattande.

Not: Bestämmelser om registerkontroll och särskild personutredning för person avsedd för tillsättning i säkerhetskänslig befattning med placering i säkerhetsklass, finns i 5 kap. 12–22 §§ SSF.
(Ref: 5 kap. 3 § SSF)

7.4.3 Krav på samtycke

Chef som ansöker om registerkontroll ansvarar för att samtycke enligt 3 kap. 18 § SSL har inhämtats.
(Ref: 5 kap. 17 § SSF)

7.4.4 Grundutredning

Med grundutredning avses en utredning om personliga förhållanden av betydelse för säkerhetsprövningen.
(Ref: 5 kap. 2 § SSF)

En grundutredning inför en möjlig tillsättning till en säkerhetskänslig befattning som är placerad i säkerhetsklass ska innefatta en säkerhetsprövningsintervju.

Grundutredningen ska dokumenteras.
(Ref: 6 kap. 5 § FFS-SäkS)

Av 5 kap. 2 § SSF framgår att grundutredningen ska omfatta betyg, intyg, referenser och uppgifter som den som prövningen gäller har lämnat, samt andra uppgifter i den utsträckning det är relevant för prövningen. Vid behov ska en identitetskontroll göras.

Av 5 kap. 3 § SSF framgår att om det redan efter grundutredningen står klart att den som prövningen gäller inte uppfyller kraven för en godkänd säkerhetsprövning, ska registerkontroll och särskild personutredning inte göras.

7.4.5 Registerkontroll

Registerkontroll av person tilltänkt för en säkerhetskänslig befattning ska göras om den säkerhetskänsliga befattningen är placerad i säkerhetsklass.
(Ref: 5 kap. 12 § SSF)

Not: Bestämmelser om registerkontroll finns också i 4 kap. SSL om internationell säkerhetsskyddssamverkan och säkerhetsintyg.
(Ref: 3 kap. 16 § SSL)

Av 5 kap. 14 § SSF framgår att en ansökan om registerkontroll får göras endast om den som säkerhetsprövningen gäller kan antas komma att anställas eller på annat sätt delta i den aktuella verksamheten. Om det finns synnerliga skäl får en ansökan göras utan ett sådant antagande.

7.4.6 Särskild personutredning

Av 3 kap. 17 § SSL framgår att en särskild personutredning ska göras vid en registerkontroll som avser tillsättande av person till en säkerhetskänslig befattning som är placerad i säkerhetsklass 1 eller 2.

Utredningen ska omfatta en undersökning av den kontrollerades ekonomiska förhållanden. I övrigt ska utredningen ha den omfattning som behövs.
(Ref: 5 kap. 12 § SSF)

Not: Säpo:s uppgift att utföra registerkontrollen innefattar även uppgiften att göra en särskild personutredning.
(Ref: 5 kap. 18 § SSF)

När den särskilda personutredningen gäller person avsedd att tillsättas till en säkerhetskänslig befattning som har placerats i säkerhetsklass 1, ska Säkerhetspolisen hålla ett personligt samtal med den som prövningen gäller, om det inte står klart att samtalet inte behövs.
(Ref: 5 kap. 19 § SSF)

7.4.7 Underlag för bedömning

Av 3 kap. 4 § SSL framgår att säkerhetsprövningen ska utgå från uppgifter som kommit fram när grundutredningen gjordes och den kännedom som i övrigt finns om den som ska prövas, uppgifter som har lämnats ut efter registerkontroll och särskild personutredning, arten av den verksamhet som prövningen gäller samt omständigheterna i övrigt.

7.4.8 Bedömning av person

Bedömningen ska göras av den chef som beslutar om tillsättning av person till säkerhetskänslig befattning (genom anställning eller annat deltagande i den säkerhetskänsliga verksamheten).
(Ref: 3 kap. 4 § SSL)

Not: Om FMV har det bestämmande inflytandet över den prövades lämplighet att delta i säkerhetskänslig verksamhet hos en enskild verksamhetsutövare, är det FMV som gör den slutliga bedömningen.
(Ref: 3 kap. 4 § SSL)

7.4.9 Uppföljning av säkerhetsprövning

Chef ska minst årligen eller vid behov genomföra uppföljande säkerhetsprövning. Prövningen ska fördjupa personkännedomen och särskild vikt ska vid en bedömning läggas vid personliga förhållanden.

Den uppföljande säkerhetsprövningen ska dokumenteras.
(Ref: 6 kap. 6 § FFS-SäkS)

Av 3 kap. 3 § SSL framgår att säkerhetsprövningen ska följas upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.

7.5 Tillsättande av person till säkerhetskänslig befattning

7.5.1 Behörighet att delta i säkerhetskänslig verksamhet

Den som ges behörighet att delta i FMV:s säkerhetskänsliga verksamhet ska

- ha bedömts pålitlig från säkerhetssynpunkt,
- ha tillräckliga kunskaper om säkerhetsskydd, och
- ha behov av tillgång till den säkerhetskänsliga verksamheten för att kunna utföra sitt arbete, samt
- ha undertecknat FMV:s sekretessbevis.

(Ref: 2 kap. 3 § SSF)

7.5.2 Beslut om tillsättande av person till säkerhetskänslig befattning

Beslut om tillsättande av behörig person till befattning placerad i säkerhetsklass grundar sig på en avvägning av det som framkommit vid säkerhetsprövningens samtliga delar.

Säkerhetsskyddsavdelningen ska bedöma resultatet av genomförd registerkontroll och meddela bedömningen till personalansvarig chef.
(Ref: 5 kap. 8 § SSF)

Not: FMV roll vid tillsättande av person till säkerhetskänslig befattning placerad i säkerhetsklass 2 och 3 hos en leverantör, med vilken FMV har ingått ett säkerhetsskyddsavtal, regleras i ISM.

Personalansvarig chef ska fatta beslut om tillsättande av person till säkerhetskänslig befattning (oavsett om denna är placerad i säkerhetsklass eller ej) enligt delegeringsordning med följande begränsningar:

- för säkerhetsklass 1 - Lägst Chef VerkO/CS
- vid avrådan från Säkerhetsskyddsavdelningen ska beslut tas av högre chef efter samråd med Säkerhetsskyddschefen.

Not: Beslut om tillsättande av person till befattning placerad i säkerhetsklass gäller även för uppdragstagare som deltar i FMV:s säkerhetskänsliga verksamhet.

En säkerhetskänslig befattning i FMV i säkerhetsklass 1 och 2 får endast innehas av den som är svensk medborgare.
(Ref: 3 kap. 11 § SSL)

Beslut om anställning för tjänster/befattningar som är inplacerade i säkerhetsklass får inte fattas innan säkerhetsprövning (innefattande grundutredning, registerkontroll och eventuell särskild personutredning) genomförts med godkänt resultat.

Not: För provanställning, där personen avses att tillsättas till en säkerhetskänslig befattning placerad i säkerhetsklass 3, kan särskilda regler förekomma.

7.5.3 Uppföljning/omprövning/ändring av tillsättande

Chef ska följa upp beslutad tillsättning av person till säkerhetskänslig befattning.

Av 3 kap. 4 § SSL framgår att om det finns anledning till det, ska en tidigare gjord bedömning av en persons lämplighet att delta i den säkerhetskänsliga verksamheten omprövas.

Om personen omplaceras till annan säkerhetskänslig befattning med lägre säkerhetsklass, ska chef skyndsamt anmäla ändrade förhållanden till Säkerhetsskyddsavdelningen, för vidare befordran till Säpo.
(Ref: 5 kap. 22 § SSF)

Om befattningens placering i säkerhetsklass ändras, ska ett beslutat tillsättande omedelbart omprövas.

7.5.3.1 Omsättning av tidigare fattade beslut

Följande beslut enligt tidigare säkerhetsskyddsförordning ska omsättas i förnyade beslut enligt SSL senast 2024:

- placering av säkerhetskänslig befattning i säkerhetsklass
- säkerhetsprövning av person
- tillsättande av person till säkerhetskänslig befattning

(Ref: Not 3 & 4 SSL)

7.6 Dokumentation inom personalsäkerhet

Chefen för säkerhetsskyddsavdelningen ska tillse att förteckning finns av de säkerhetskänsliga befattningar som har placerats i säkerhetsklass, eller det övriga deltagande i säkerhetskänslig verksamhet som endast ska föregås av säkerhetsprövning.
(Ref: 6 kap. 4 § FFS-SäkS)

Resultatet av säkerhetsprövningen ska dokumenteras i de fall en person har bedömts vara pålitlig från säkerhetssynpunkt och beslut har fattats om tillsättande av personen i säkerhetskänslig befattning.
(Ref: 5 kap. 5 § SSF)

7.6.1 Sekretess för uppgifter om säkerhetsprövning

Uppgifter som framkommer i samband med säkerhetsprövning av person omfattas av sekretess enligt 35 kap. 1 § OSL. Se även avsnitt 7.12 Tystnadsplikt.

7.7 Frånvaro från säkerhetskänslig verksamhet

När en enskild medarbetarehar varit eller förväntas vara frånvarande i mer än 12 månader ska chef tillse att medarbetarens handlingar/lagringsmedier/materiel som innehåller sekretessbelagda eller säkerhetsskydds-klassificerade uppgifter återlämnas.

7.8 Avslutande av deltagande i säkerhetskänslig verksamhet

När en persons deltagande i säkerhetskänslig verksamhet upphör ska detta meddelas till Säkerhetsskydds-avdelningen, så att registerkontroll och ev. förekommande placering i säkerhetsklass kan avslutas.

Chef ska genomföra ett avslutande samtal när personens deltagande i den säkerhetskänsliga verksamheten upphör.

Det avslutande samtalet ska dokumenteras.

Om personen har tagit del av säkerhetsskyddsklassificerade uppgifter ska denne upplysas om räckvidden och innebörden av den sekretess och tystnadsplikt som följer av OSL och SSL.

Ett sådant samtal behöver inte genomföras om det är uppenbart obehövligt.
(Ref: 6 kap. 8 § FFS-SäkS)

När en enskild medarbetare avslutar sin tjänst ansvarar chef för att medarbetarens utkvitterade handlingar/ lagringsmedier/materiel återlämnas.

7.9 Beslut i personärende

Beslutsfattande om att en person inte bedöms som pålitlig från säkerhetssynpunkt, och därmed inte kan tillsättas till säkerhetskänslig befattning eller måste avsättas från tidigare beslutad tillsättning, görs enligt följande:

- vid nyrekrytering är det den chef som ansvarar för rekryteringen som fattar beslutet efter samråd med FMV:s Säkerhetsskyddschef
- för redan anställd personal som innehar tjänst placerad i säkerhetsklass är det Chef VerkO/CS som fattar beslutet efter samråd med FMV:s Säkerhetsskyddschef

Not: Se även avsnitt 7.5.3.

7.10 Säkerhetsklarering i samband med utlandsresa

Vid besök vid utländsk myndighet/företag ska, när så krävs, säkerhetsklarering (Personell Security Clearance, PSC) bifogas besöksansökan. Ansökan om säkerhetsklarering ska i god tid sändas till Säkerhetsskyddsavdelningen, som utfärdar klareringen.

Not: Ansökan om besökstillstånd vid utländskt företag/myndighet regleras i bi-/multilaterala avtal.

7.11 Sekretessbevis

Innan uppgifter som omfattas av sekretess delges behörig person ska ansvarig chef tillse/verifiera att sekretessbevis har undertecknas.

I samband med tecknande av sekretessbevis ska ansvarig chef förvissa sig om att den person som sekretessbeviset gäller förstår innebörden av sekretess och tystnadsplikt.

7.12 Tystnadsplikt

Tystnadsplikt enligt OSL gäller för FMV:s anställda, inhyrd personal, uppdragstagare samt de som på annat sätt deltar i FMV:s verksamhet, i enlighet med bestämmelserna i 2 kap. 1 § offentlighets- och sekretesslagen (2009:400).

Not: Den som på grund av sin anställning i FMV eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet får inte obehörigen röja eller utnyttja säkerhetsskyddsklassificerade uppgifter.
(Ref: 5 kap. 2 § SSL)

8 Informationssäkerhet

8.1 Allmänt

Det övergripande målet med FMV:s informationssäkerhetsarbete är att säkerställa ett tillräckligt skydd för egen, uppdragsgivares, leverantörers och övriga intressenters informationstillgångar såväl inom som utom landet. Se vidare FMV:s Informationssäkerhetspolicy (15FMV6009-1:1)

8.1.1 Verksamhetslogik för informationssäkerhet

- Informationssäkerhet omfattar konfidentialitet, integritet och tillgänglighet för uppgifter (information).
- Fokus för FMV:s TjF säkerhetsskydd och sekretess ligger i första hand på uppgifters konfidentialitet.
- Alla uppgifter i FMV:s verksamhet är i någon mening skyddsvärda och hanteras därför med lämplig omsorg, för att tillgodose krav på informationssäkerhet enligt första punkten.
- Vissa uppgifter omfattas av olika skäl av sekretess enligt OSL. Sådana uppgifter omfattas av bestämmelser om sekretess i denna TjF.
- Vissa uppgifter som omfattas av sekretess rör säkerhetskänslig verksamhet och omfattas därför av krav på säkerhetsskydd enligt SSL. Sådana uppgifter omfattas av bestämmelser om säkerhetsskydd i denna TjF.

8.1.2 Offentlighets- och sekretesslagen OSL

OSL innehåller bestämmelser om myndigheters och vissa andra organs handläggning vid registrering, utlämnande och övrig hantering av allmänna handlingar.

OSL innehåller vidare bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar. Dessa bestämmelser avser förbud att röja uppgift, vare sig detta sker muntligen, genom utlämnande av allmän handling eller på något annat sätt.

Bestämmelserna innebär begränsningar i yttrandefriheten enligt regeringsformen, begränsningar i den rätt att ta del av allmänna handlingar som följer av tryckfrihetsförordningen samt, i vissa särskilt angivna fall, även begränsningar i den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Uppgifter hanterade i FMV:s verksamhet kan omfattas av sekretess enligt OSL. Uppgifter som omfattas av sekretess kan även vara säkerhetsskyddsklassificerade och omfattas av krav på säkerhetsskydd enlig SSL.

Vid sekretessbedömning klarläggs vilket eller vilka lagrum i OSL som är aktuella att anges som grund för beslut om beläggande av uppgift med sekretess. Se avsnitt 8.2.

8.1.3 Säkerhetsskyddslagen SSL

SSL innehåller bestämmelser till skydd av säkerhetskänslig verksamhet. Ett av huvudområdena i SSL rör informationssäkerhet, som syftar till att

- förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och
- förebygga skadlig inverkan i övrigt på uppgifter.

(Ref: 2 kap. 2 § SSL)

Uppgifter hanterade i FMV:s verksamhet kan vara säkerhetsskyddsklassificerade och omfattas av krav på säkerhetsskydd enligt SSL. Sådana uppgifter omfattas även av sekretess enligt OSL.

Vid säkerhetsskyddsklassificering delas uppgifterna in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra. Se avsnitt 8.3.

8.2 Uppgifter som omfattas av sekretess

8.2.1 Bedömning av sekretess

För varje uppgift som hanteras i FMV ska en bedömning göras huruvida denna omfattas av sekretess.

Sekretessbedömning görs av ansvarig handläggare eller chef.

Not: Sekretessbedömning kan avse såväl en första som en förnyad bedömning.

Sekretess kan endast hävdas om det finns stöd för detta i OSL eller i lag som OSL hänvisar till.

8.2.2 Behörighet att ta del av uppgifter som omfattas av sekretess

Behörig att ta del av uppgifter som omfattas av sekretess är den som

- har tillräckliga kunskaper om sekretess och tystnadsplikt,
- behöver uppgifterna för att kunna utföra sitt arbete, och
- har undertecknat sekretessbevis.

8.2.3 Utlämning av uppgifter som omfattas av sekretess

Utlämning kan ske muntligen, skriftligen eller på annat sätt.

Utlämning av uppgifter som omfattas av sekretess får göras efter beslut av ansvarig handläggare eller chef.

Utlämning av uppgifter som omfattas av sekretess får endast ske till den som är behörig. Se avsnitt 8.2.2.
(Ref: 2 kap. 4 § SSF)

Utlämning av uppgifter som omfattas av sekretess ska ske på ett sådant sätt att uppgiften inte kommer obehöriga till del.

Innan utlämning av uppgifter som omfattas av sekretess får ske ska den som avser att lämna ut uppgifterna kontrollera att inga hinder för utlämning föreligger med anledning av avtal med annan stat eller mellanfolklig organisation.

8.2.4 Utlämning av uppgifter som omfattas av sekretess till utlandet

Uppgifter som omfattas av sekretess enligt OSL får inte lämnas ut till en utländsk myndighet, en enskild eller en mellanfolklig organisation, om inte

- utlämnande sker i enlighet med särskild föreskrift i lag eller förordning, eller
- uppgifterna i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt FMV:s prövning står klart att det är förenligt med svenska intressen att uppgifterna lämnas till den utländska myndigheten, den enskilde eller den mellanfolkliga organisationen.

(Ref: 8 kap. 3 § OSL)

Uppgift för vilken sekretess gäller enligt 15 kap. 2 § OSL får FMV lämna ut till en utländsk myndighet som deltar i ett samarbete inom Försvarsdepartementets verksamhetsområde enligt en sådan överenskommelse som avses i 10 kap. 1 § regeringsformen, om överenskommelsen har ingåtts av

- regeringen, eller
- en förvaltningsmyndighet efter uppdrag från regeringen enligt 10 kap. 2 § regeringsformen.

(Ref: 1 § SFS 2010:649)

Not: En uppgift får lämnas ut endast om det enligt FMV:s prövning är nödvändigt för att genomföra samarbetet. FMV får inte lämna ut uppgift som är av synnerlig betydelse för rikets säkerhet eller som kan ge underlag för utveckling av motmedel mot Sveriges försvarssystem. Förordning (2011:78).
(Ref: 1 § SFS 2010:649)

8.2.5 Hantering av handling med uppgifter som omfattas av sekretess

Vad som i detta avsnitt och underavsnitt anges gäller såväl för fysiska handlingar (papper) som elektroniska handlingar om det inte explicit anges något annat.

8.2.5.1 Markering avseende sekretess

Om det kan antas att uppgifterna i en allmän handling inte får lämnas ut på grund av en bestämmelse om sekretess, ska detta markeras genom att en anteckning om sekretess görs på handlingen. Bilagor ska hanteras på samma sätt som huvudhandling. Se bilaga 6.
(Ref: 5 kap. 5 § OSL)

Not: En anteckning om sekretess kallas även sekretessmarkering.

Anteckning om sekretess ska ange

- tillämplig sekretessbestämmelse,
- datum då anteckningen gjordes, och
- att det är FMV som har gjort anteckningen.

(Ref: 5 kap. 5 § OSL)

Upplysning om sekretess ska framgå på samtliga sidor i en handling. Se bilaga 6.

8.2.5.2 Hävande av sekretess (ändring av tidigare bedömning)

I det fall sekretessbedömningen för en uppgift ändras ska beslut om hävande av sekretess fattas av ansvarig handläggare eller chef och antecknas på huvudexemplaret av den handling som innehåller uppgiften. Beslut om hävande av sekretess ska meddelas till registratorsfunktionen eller ansvarig för det register där handlingen hanteras.

8.2.5.3 Distribution av handling med sekretessbelagda uppgifter

Distribution av handling med uppgifter som omfattas av sekretess ska ske på sådant sätt att obehöriga hindras ta del av innehållet.

8.2.5.4 Medförande av handling med sekretessbelagda uppgifter

Medförande av handling med uppgifter som omfattas av sekretess utanför FMV:s lokaler ska ske endast vid behov.

Den som medför handling med uppgifter som omfattas av sekretess utanför FMV:s lokaler ska hålla handlingen under omedelbar uppsikt eller förvara den på sådant sätt att obehöriga hindras ta del av innehållet.

Den som ska medföra handling/lagringsmedium/materiel innehållande uppgifter som omfattas av sekretess ansvarar för att det vid FMV finns förtecknat vad som medförs vid det aktuella tillfället.

Inhyrd personal får medföra handling med uppgifter som omfattas av sekretess utanför FMV först efter beslut av ansvarig handläggare eller chef.

8.2.5.5 Förvaring av handling med sekretessbelagda uppgifter

Handling med uppgifter som omfattas av sekretess ska vara under kontroll eller förvaras så att obehöriga ej kan ta del av uppgifterna.

Not: Förvaring i låst tjänsterum eller låst plåtskåp/träkonstruktion, utan obehörigt tillträde, i FMV:s lokaler uppfyller kravet. Alternativt kan förvaring som uppfyller krav för säkerhetsskyddsklassificerade uppgifter användas.

Not: Vid förvaring av elektroniska handlingar med sekretessbelagda uppgifter, där lagringsmediet skyddas med av Säkerhetsskydds-avdelningen godkänd krypteringsmetod, gäller inga särskilda krav.

8.2.5.6 Förstöring av handling med sekretessbelagda uppgifter

Förstöring ska ske i enlighet med bilaga 5.

8.3 Uppgifter som omfattas av krav på säkerhetsskydd

8.3.1 Säkerhetsskyddsklassificering

Syftet med säkerhetsskyddsklassificering är att säkerställa att uppgifter, av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande, erhåller ett adekvat säkerhetsskydd.

Skyddet avser all hantering av uppgifterna, oavsett om de är föremål för utlämning enligt OSL eller ej.

För varje uppgift som hanteras i FMV ska en bedömning göras huruvida den rör säkerhetskänslig verksamhet och därför omfattas av krav på säkerhetsskydd och indelning i säkerhetsskyddsklass (säkerhetsskyddsklassificering).

Beslut om säkerhetsskyddsklassificering fattas enligt delegeringsordning.

En publikation som innehåller säkerhetsskyddsklassificerade uppgifter ska ges det säkerhetsskydd som gäller för en säkerhetsskyddsklassificerad allmän handling.
(Ref: 3 kap. 4 § FFS-SäkS)

När FMV lånar en handling med säkerhetsskyddsklassificerade uppgifter från en annan myndighet ska handlingen ges det säkerhetsskydd som gäller för en allmän handling med motsvarande säkerhetsskydds-klassificering.
(Ref: 3 kap. 5 § FFS-SäkS)

Not: Lån av handlingar förekommer t.ex. i samband med rättssak.

8.3.1.1 Säkerhetsskyddsklasser

Säkerhetsskyddsklasser medför olika hanteringsregler/skyddsmekanismer och bygger på en förtida bedömning av den skada som ett röjande av uppgiften kan medföra. Med säkerhetsskyddsklassificerad uppgift avses uppgift som indelats i någon av säkerhetsskyddsklasserna:

- Kvalificerat hemlig vid risk för en synnerligen allvarlig skada,
- Hemlig vid risk för en allvarlig skada,
- Konfidentiell vid risk för en inte obetydlig skada, eller
- Begränsat hemlig vid risk för endast ringa skada.

(Ref: 2 kap. 5 § SSL)

Säkerhetsskyddsklassificerade uppgifter i FMV:s verksamhet omfattas alltid av sekretess.

Not: Uppgifter i säkerhetsskyddsklass Kvalificerat hemlig anses som regel vara "av synnerlig betydelse för rikets säkerhet" enligt OSL (och omvänt). För dessa uppgifter gäller särskilda regler. Se bilaga 6, avseende anteckning om sekretess.

8.3.1.2 Tidigare gjord klassificering

Handlingar som har märkts enligt tidigare regelverk ska anses innehålla uppgifter enligt nedan intill dess att en förnyad bedömning görs:

- en handling märkt KVALIFICERAT HEMLIG ska anses innehålla uppgifter i säkerhets-skyddsklassen Kvalificerat hemlig
- en handling märkt HEMLIG ska anses innehålla uppgifter i säkerhetsskyddsklassen Hemlig
- en handling märkt HEMLIG/TOP SECRET eller H/TS ska anses innehålla uppgifter i säkerhetsskyddsklassen Kvalificerat hemlig
- en handling märkt HEMLIG/SECRET eller H/S ska anses innehålla uppgifter i säkerhetsskyddsklassen Hemlig
- en handling märkt HEMLIG/CONFIDENTIAL eller H/C ska anses innehålla uppgifter i säkerhetsskyddsklassen Konfidentiell
- en handling märkt HEMLIG/RESTRICTED eller H/R och som innehåller uppgifter som omfattas av sekretess enligt
    - 15 kap. 1 § OSL "med betydelse för rikets säkerhet eller som omfattas av ett internationellt säkerhetsskyddsåtagande" eller
    - 15 kap. 2 § OSL

  ska anses innehålla uppgifter i säkerhetsskyddsklassen Begränsat hemlig

- en handling märkt HEMLIG/RESTRICTED eller H/R och som innehåller uppgifter som omfattas av sekretess enligt
    - 15 kap. 1 § OSL "utan betydelse för rikets säkerhet eller som inte omfattas av ett internationellt säkerhetsskyddsåtagande" eller
    - annat lagrum än 15 kap. 1-2 §§ OSL

  ska anses innehålla uppgifter som enbart omfattas av sekretess (uppgifterna anses ej vara säkerhetsskyddsklassificerade).

8.3.1.3 Ändring av säkerhetskyddsklass (inkl. hävande)

Om klassificeringen av uppgifterna i en registrerad handling ändras till annan säkerhetsskyddsklass än vad som anges på handlingen, inklusive hävande av tidigare klassificering, ska detta beslutas enligt delegeringsordning med följande begränsning:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef VerkO/CS

Beslutet ska antecknas på handlingen. Anteckningen på handlingen ska innehålla:

- den nya säkerhetsskyddsklassen (utom vid hävande),
- Försvarets materielverk (myndighetens namn),
- datum för beslutet, samt
- vem som fattat beslutet.

Tidigare anteckning avseende säkerhetsskyddsklass ska överkorsas.

Ändring ska meddelas till den som är ansvarig för det register där handlingen är registrerad. Om handlingen är allmän ska beslutet om ändring av säkerhetsskyddsklass föras in i det register där handlingen är registrerad.

Ändring respektive borttagning av märkning av säkerhetsskyddsklass som gäller för en handling med uppgifter i säkerhetskyddsklassen Kvalificerat hemlig får ske först efter hörande av den myndighet som har upprättat handlingen.
(Ref: 3 kap. 10 § FFS-SäkS)

8.3.1.4 Uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd

Säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd ska delas in i säkerhetsskyddsklass enligt ovan (se avsnitt 8.3.1.1) utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation. Om uppgifterna i fråga redan har klassificerats av en annan stat eller en mellanfolklig organisation, ska hanteringen av uppgifterna göras enligt de för åtagandet mellan parterna överenskomna principerna.
(Ref: 2 kap. 5 § SSL)

8.3.2 Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter

Behörig att ta del av säkerhetsskyddsklassificerade uppgifter är, om inte något annat följer av bestämmelser i lag, endast den som

- har bedömts pålitlig från säkerhetssynpunkt,
- har tillräckliga kunskaper om säkerhetsskydd,
- behöver uppgifterna för att kunna utföra sitt arbete, och
- har undertecknat sekretessbevis.

(Ref: 2 kap. 3 § SSF)

Beslut om behörighet att ta del av säkerhetsskyddsklassificerade uppgifter fattas enligt delegeringsordning med följande begränsning:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning

Aktuella behörighetslistor för respektive säkerhetsskyddsklassen Kvalificerat hemlig och för säkerhetsskyddsklasserna Hemlig och Konfidentiell ska upprättas och fastställas av personalansvarig chef, samt finnas tillgängliga vid registratorsfunktionen. Listorna ska revideras årligen.
(Ref: 3 kap. 1 § FFS-SäkS)

Behörighetslista Kvalificerat hemlig enligt ovan ska indelas i säkerhetsskyddsklass Konfidentiell.

Behörighetslista Hemlig/Konfidentiell enligt ovan ska indelas i säkerhetsskyddsklass Begränsat hemlig, om det inte finns skäl för annan bedömning.

För båda typerna av lista gäller sekretess enligt 18 kap. 8 § OSL, om det inte finns skäl för annan bedömning.

8.3.3 Delgivning av säkerhetsskyddsklassificerade uppgifter

Ansvarig chef ska upplysa den som tillåts ta del av säkerhetsskyddsklassificerade uppgifter om räckvidden och innebörden av sekretess och tystnadsplikt.
(Ref: 2 kap. 4 § SSF)

Kvittering på delgivningslista ska användas vid delgivning av uppgifter placerade i säkerhetsskyddsklass Konfidentiell eller högre. Delgivningslistan ska arkiveras med huvudexemplaret av eventuell handling.

Vid delgivning av säkerhetsskyddsklassificerade uppgifter ska hänsyn även tas till förekommande sekretessreglering av samma uppgifter.

8.3.3.1 Delgivning av säkerhetsskyddsklassificerade uppgifter inom FMV

Delgivning av säkerhetsskyddsklassificerade uppgifter till FMV personal får ske först efter beslut enligt delegeringsordning med följande begränsningar:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning

8.3.3.2 Utrymmen för muntlig delgivning av säkerhetsskyddsklassificerade uppgifter

Chef Jurstab ska fatta beslut om kraven på de kategorier av utrymmen som är godkända för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass Konfidentiell eller högre.

Av beslutet ska det för varje kategori framgå hur endast behöriga personer ges tillträde till utrymmet samt vilken utrustning som får medföras eller finnas i utrymmet. Se bilaga 2.
(Ref: 5 kap. 20 § FFS-SäkS)

Chef VerkO/CS ska identifiera vilka utrymmen inom den egna verksamheten som uppfyller kraven för kategorierna ovan.

8.3.3.3 Delgivning av säkerhetsskyddsklassificerade uppgifter utanför FMV inom Sverige

Delgivning av säkerhetsskyddsklassificerade uppgifter till svensk myndighet får ske först efter beslut enligt delegeringsordning med följande begränsningar:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning

Delgivning av säkerhetsskyddsklassificerade uppgifter till svenskt företag får ske först efter beslut enligt delegeringsordning med följande begränsningar:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning

Not: Sådan delgivning kräver dessutom att säkerhetsskyddsavtal är undertecknat mellan företaget och FMV.

8.3.3.4 Delgivning av säkerhetsskyddsklassificerade uppgifter till utlandet

För delgivning av säkerhetsskyddsklassificerade uppgifter till utländsk part krävs (i tillämpliga delar) att:

- utbyte av säkerhetsskyddsklassificerade uppgifter mellan staterna är reglerat i bi-/multilateralt avtal
- regeringen gett FMV tillstånd att lämna ut uppgifterna till utländsk mottagare
- beslut om delgivning har fattats enligt delegeringsordning
- yttrande från informationsägaren har inhämtas för uppgifter som omfattas av sekretess enligt 15 kap. 1 § OSL
- mottagande person vid behov kan styrka sin behörighet genom godkänd säkerhetsklarering, t.ex. med Personnel Security Clearance (PSC),
- den utländska delgivna parten (ofta en leverantör) har godkänts genom kontroll enligt den andra statens säkerhetsskyddslagstiftning

(Ref: 3 kap. 9 § SSF)

8.3.4 Hantering av handling med säkerhetsskyddsklassificerade uppgifter

Vad som i detta avsnitt och underavsnitt anges gäller såväl för fysiska handlingar (papper) som elektroniska handlingar om det inte explicit anges något annat.

Vissa krav avseende handlingar med säkerhetsskyddsklassificerade uppgifter gäller även för lagringsmedier med säkerhetsskyddsklassificerade uppgifter och för säkerhetskänslig materiel. Därför förekommer i detta avsnitt ibland hänvisning till handling/lagringsmedium/materiel.

Arbete med handling/lagringsmedium/materiel med säkerhetsskyddsklassificerade uppgifter ska ske på sådant sätt att obehörig inte får del av innehållet.

Vidare ska det dokumenteras vilka personer som tagit del av handling/lagringsmedium/materiel med uppgifter i säkerhetsskyddsklass Konfidentiell eller högre.

8.3.4.1 Anteckning om säkerhetsskyddsklass

En handling med säkerhetsskyddsklassificerade uppgifter ska på första sidan förses med en anteckning (märkning) om den högsta säkerhetsskyddsklassen som uppgifterna i handlingen är indelade i. Bilagor ska hanteras på samma sätt som huvudhandling. Se bilaga 6.

Övriga sidor i handlingen ska vara märkta med samma säkerhetsskyddsklass som första sidan av handlingen eller bilagan, eller vara märkta med den högsta säkerhetsskyddsklassen som uppgifterna på den aktuella sidan är indelade i.

En elektronisk handling med säkerhetsskyddsklassificerade uppgifter får istället förses med märkning om säkerhetsskyddsklass på lämpligt sätt med hänsyn till de informationssystem som handlingen behandlas i. En sådan märkning ska då den elektroniska handlingen visas, så långt som möjligt uppfylla kraven i första och andra stycket ovan.
(Ref: 3 kap. 7 § FFS-SäkS)

En allmän handling med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre ska på första sidan märkas med handlingens beteckning, exemplarnummer, antal sidor samt bilagor, om sådana följer med.

Av bilaga och blad i bok med lösbladssystem ska framgå till vilken handling bilagan respektive bladet hör.

För en elektronisk allmän handling med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre får märkning enligt första stycket istället göras på lämpligt sätt med hänsyn till de informationssystem som handlingen behandlas. Märkningen behöver inte omfatta exemplarnummer och antal sidor.
(Ref: 3 kap. 11 § FFS-SäkS)

En allmän handling med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre ska på handlingens sändlista märkas med hur många exemplar av handlingen som har framställts och vilka som är mottagare av respektive exemplar. Motsvarande uppgifter ska anges i diariet där handlingen är diarieförd, eller i ett register för uppföljning av exemplar av allmänna handlingar med säkerhetsskyddsklassificerade uppgifter.

Kraven i det föregående stycket gäller inte för elektroniska allmänna handlingar med säkerhetsskydds-klassificerade uppgifter.
(Ref: 3 kap. 12 § FFS-SäkS)

Om en handling som innehåller säkerhetsskyddsklassificerade uppgifter kan antas komma att lämnas över till utländska myndigheter eller leverantörer, ska den förses med en anteckning om handlingens ursprungs-land, om det inte är olämpligt.
(Ref: 3 kap. 7 § SSF)

Om FMV har beslutat att en handling med säkerhetsskyddsklassificerade uppgifter får delges till någon utländsk myndighet eller mellanfolklig organisation får handlingens första sida märkas med en sådan upplysning.

En elektronisk handling med säkerhetsskyddsklassificerade uppgifter får istället märkas (enligt första och andra stycket närmast ovan) på lämpligt sätt med hänsyn till de informationssystem som handlingen behandlas i.
(Ref: 3 kap. 27 § FFS-SäkS)

En handling som förses med anteckning om säkerhetsskyddsklass ska även förses med sekretessmarkering enligt avsnitt 8.2.5.1.

8.3.4.2 Registrering och kvittering

När en allmän handling som innehåller uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre lämnas ut, ska mottagandet kvitteras med underskrift, namnförtydligande och datum. Ett namnförtydligande får vara en kod.

När en allmän handling som innehåller uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre återlämnas ska detta kvitteras.
(Ref: 3 kap. 15 § FFS-SäkS)

Not: Vad som föreskrivs ovan avseende kvittering gäller inte

- *när arkiv-, expeditions-, sambands- eller tryckeripersonal, för registrering, kopiering, distribution, arkivering eller förstöring, tar emot en allmän handling eller ett lagringsmedium som innehåller säkerhetsskyddsklassificerade uppgifter, om inte den som lämnar över handlingen begär det, eller*
- *för personal som arbetar med drift av informationssystem, vad avser sådana lagringsmedier som innehåller säkerhetsskyddsklassificerade uppgifter och som hanteras i driften av informationssystemen.*

(Ref: 3 kap. 16 § FFS-SäkS)

Not: Mottagande av en elektronisk handling med säkerhetsskyddsklassificerade uppgifter behöver inte kvitteras om mottagandet sker i ett informationssystem där det i en säkerhetslogg noteras vem som tagit del av handlingen. Se avsnitt 9.4.5.1.
(Ref: 3 kap. 15 § FFS-SäkS)

I det diarium där en säkerhetsskyddsklassificerad allmän handling med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre är diarieförd ska anges vem som förvarar handlingen eller om handlingen har förkommit, arkiverats eller gallrats. Uppgifterna får istället för i diariet antecknas i ett register för uppföljning av exemplar av allmänna handlingar med säkerhetsskyddsklassificerade uppgifter.

För elektroniska allmänna handlingar med säkerhetskyddsklassificerade uppgifter får det istället anges i vilket informationssystem och av vem handlingen behandlas.
(Ref: 3 kap. 18 § FFS-SäkS)

Exemplarhantering, kvittering och överlämning av registrerad handling med uppgifter i säkerhetskyddsklass Konfidentiell eller högre ska ske vid registratorsfunktionen eller i informationssystem med stöd för dessa funktioner.

Vid kvittering och överlämning av handling med säkerhetsskyddsklassificerade uppgifter ska mottagaren kunna styrka sin identitet med av FMV godkänd ID-handling, enligt bilaga 3.

Information om hur och var registrering och kvittering av handling med säkerhetsskyddsklassificerade uppgifter ska ske vid respektive verksamhetsställe ska framgå av lokal säkerhetsskyddsinstruktion.

Kvitto för en handling med, eller delgivning av, uppgifter som är placerade i säkerhetsskyddsklassen

- Konfidentiell eller Hemlig ska bevaras i minst 10 år,
- Kvalificerat hemlig ska bevaras i minst 25 år.

(Ref: 3 kap. 15 § FFS-SäkS)

8.3.4.3 Gemensam användning

Beslut om gemensam användning får endast fattas av ansvarig chef och om det är nödvändigt för verksamheten. Samtliga personer som omfattas av beslutet ska vara behöriga till alla uppgifter som beslutet avser. Av beslutet ska det framgå

- vilka personer som är behöriga,
- vilka säkerhetsskyddsklassificerade uppgifter, handlingar eller lagringsmedier/materiel som avses, samt
- i förekommande fall vilket förvaringsutrymme som skall användas för handlingarna/lagrings-medierna/materielen.

Varje handling/lagringsmedium/materiel som gemensamt ska användas ska kvitteras av verksamhetsansvarig chef (som själv ska ingå i gruppen av behöriga enligt beslutet), som då också ansvarar för handlingen/lagringsmediet/materielen.

De personer som omfattas av ett beslut om gemensam användning ansvarar var för sig för att upprätthålla skyddet av de uppgifter som ingår i de berörda handlingarna/lagringsmedierna/materielen.

Beslut om gemensam användning av handlingar/lagringsmedier/materiel fattas enligt delegeringsordning med följande begränsning:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning.

8.3.4.4 Kopiering, utdrag

Beslut om kopiering/utdrag ur handling fattas enligt delegeringsordning med följande begränsning:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning
- för uppgifter i övriga säkerhetsskyddsklasser krävs inget beslut.

Not: Beslut om kopiering sammanfaller ofta med beslut om delgivning.

Har en kopia av en allmän handling med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre gjorts, ska uppgift om detta liksom uppgift om till vem kopian eller utdraget har lämnats antecknas i det register eller liggare där handlingen är diarieförd eller i ett register för uppföljning av exemplar av allmänna handlingar med säkerhetsskyddsklassificerade uppgifter.
(Ref: 3 kap. 14 § FFS-SäkS)

Kopiering av handling med säkerhetsskyddsklassificerade uppgifter får endast ske på av FMV tillhandahållen kopieringsmaskin godkänd för aktuell säkerhetsskyddsklass.

Not: Observera att i FMV förekommer kopieringsmaskiner godkända för olika säkerhetsskyddsklasser.

8.3.4.5 Förvaring

Krav på förvaringsutrymmen framgår av bilaga 2.

Handlingar/lagringsmedier/materiel med säkerhetsskyddsklassificerade uppgifter ska vara under kontroll alternativt förvaras i av FMV godkänd lokal eller godkänt förvaringsutrymme som uppfyller de krav som ställs i bilaga 2, kapitel 3 och 4.
(Ref: 5 kap. 15-17 §§ FFS-SäkS)

Handling/lagringsmedium/materiel med uppgifter i säkerhetsskyddsklass Hemlig eller lägre får under ordinarie arbetstid lämnas framme i arbetsrum/möteslokal under kortare tid (minuter), förutsatt att

- ingen obehörig vistas i rummet,
- handling/lagringsmedium/materiel inte kan läsas/observeras av obehörig,
- rummet är låst med nyckel eller passagekontrollsystem och
- huvudnycklar och reservnycklar förvaras så att inga obehöriga kan komma åt dem.

(Ref: 5 kap. 19 § FFS-SäkS)

8.3.4.5.1 Samförvaring

Beslut om samförvaring får endast omfatta personer som är behöriga att ta del av uppgifter i samma eller högre säkerhetsskyddsklass som/än de samförvarade uppgifterna. Samförvaring får endast ske i ett godkänt förvaringsutrymme där respektive person har separat låsbart innerfack/utrymme.

Beslut om samfövaring av handlingar/lagringsmedier/materiel fattas enligt delegeringsordning med följande begränsning:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning.
- för uppgifter i säkerhetsskyddsklass Begränsat hemlig krävs inget beslut.

Av beslut om samförvaring ska det framgå vilket förvaringsutrymme och vilka personer som omfattas av beslutet, samt vilken högsta lägsta säkerhetskyddsklass de samförvarade uppgifterna får vara indelade i.

8.3.4.6 Nycklar, kort och koder

Av 5 kap. 7 § FFS-SäkS framgår att nycklar, kort och koder som var för sig ger tillträde till säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig verksamhet ska vara under kontroll eller förvaras i motsvarande skyddsklass som den de ger tillträde till.
(Ref: 5 kap. 7 § FFS-SäkS)

Av 5 kap. 8 § FFS-SäkS framgår att en kod ska bestämmas och ställas in av den som har tilldelats ett utrymme där säkerhetsskyddsklassificerade uppgifter förvaras eller där säkerhetskänslig verksamhet bedrivs.

En nyckel, ett kort eller en kod får innehas endast av den som har ansvaret för utrymmet, om inte ansvarig chef har beslutat annat.
(Ref: 5 kap. 9 § FFS-SäkS)

Det ska finnas en förteckning över samtliga nycklar, kort och koder till områden, byggnader eller utrymmen som

- innehåller säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass Konfidentiell eller högre, eller
- används för säkerhetskänslig verksamhet där en inträffad skada kan vara mer än "inte obetydlig".

Av förteckningen ska framgå till vem och när en nyckel, ett kort eller en kod har lämnats samt var reservnyckel och kod eller kort i reserv förvaras.
(Ref: 5 kap. 10 § FFS-SäkS)

Om det finns anledning att anta att en nyckel eller ett kort har förlorats eller kopierats, att en kod har röjts eller att en nyckel, kort eller kod har använts av någon obehörig person, ska förhållandet omedelbart rapporteras till Säkerhetsskyddsavdelningen.
(Ref: 5 kap. 11 § FFS-SäkS)

Förvaring av eventuella reservnycklar/-kort/-koder ska regleras i lokal säkerhetsskyddsinstruktion.

I det fall den som ansvarar för förvaringsutrymmet inte är närvarande får användande av reservnyckel/-kort/-kod till förvaringsutrymme där handling/lagringsmedium/materiel med uppgifter i säkerhetsskyddsklass Begränsat hemlig eller högre förvaras endast ske efter beslut av berörd chef. Förvaringsutrymmet får då endast öppnas i vittnes närvaro. Ett meddelande om genomförd öppning ska lämnas i förvaringsutrymmet.

8.3.4.7 Inventering

Krav avseende inventering gäller för allmänna handlingar, publikationer och standarder med säkerhetsskyddsklassificerade uppgifter.
(Ref: 3 kap. 8 § SSF)

Allmän handling, lagringsmedium eller materiel med uppgifter i säkerhetsskyddsklass Kvalificerat hemlig ska inventeras minst varje år.
(Ref: 3 kap. 8 § SSF)

Chef ansvarar för att enskilda medarbetares innehav av handling/lagringsmedium/materiel med uppgifter i säkerhetsskyddsklass Hemlig eller Konfidentiell inventeras vid behov, dock minst en gång per år.

Resultatet av genomförd inventering ska dokumenteras och redovisas till registratorsfunktionen i enlighet med av registratorsfunktionen utfärdade direktiv.

Elektroniska handlingar med säkerhetsskyddsklassificerade uppgifter behöver inte inventeras.
(Ref: 3 kap. 8 § SSF)

Chef ansvarar för att inventering och kontroll av handlingar/lagringsmedier/materiel, tilldelade uppdragstagaren för arbete inom FMV:s lokaler, genomförs på motsvarande sätt som ovan.

I det fall en inventeringspliktig handling/lagringsmedium/materiel inte kan redovisas, ska en rapport om säkerhetsincident skyndsamt insändas till Säkerhetsskyddsavdelningen och den som ansvarar för det register där handling/materiel är registrerad informeras.

Av 3 kap. 8 § SSF framgår att för arkiverade handlingar gäller kravet på inventering enbart för handlingar med uppgifter i säkerhetsskyddsklassen Kvalificerat hemlig.

8.3.4.8 Förstöring av handlingar

Förstöring av handlingar med säkerhetsskyddsklassificerade uppgifter ska ske så att återskapande av uppgifterna omöjliggörs.

Förstöring av allmänna handlingar med säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklassen Konfidentiell eller högre ska dokumenteras.
(Ref: 3 kap. 24 § FFS-SäkS)

Förstöring av allmän handling eller lagringsmedium med säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig materiel ska ske i av Säkerhetsskyddsavdelningen godkänd destruktör eller godkänd metod. Se bilaga 5.

Förstöring av icke allmän handling med uppgifter i säkerhetskyddsklass sker på respektive anställds/ uppdragstagares eget ansvar. Destruktion ska ske enligt godkänd metod. Se bilaga 5.

8.3.4.9 Distribution

8.3.4.9.1 Allmänt

Chef ska se till att nödvändiga skyddsåtgärder vidtas under distribution.

En försändelse bestående av handlingar med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre ska sändas med en distributör som har tecknat säkerhetskyddsavtal med FMV.

En sådan distributör ska kunna verifiera att försändelsen har levererats till mottagaren.

Ovanstående gäller inte för elektroniska handlingar med säkerhetsskyddsklassificerade uppgifter.
(Ref: 3 kap. 25 § FFS-SäkS)

8.3.4.9.2 Handkurir

För distribution med hjälp av handkurir av handling/lagringsmedium/materiel med säkerhetsskydds-klassificerade uppgifter krävs att:

- FMV har ett säkerhetsskyddsavtal Nivå 1 med avsändande/mottagande företag, samt att
- handkuriren innehar en säkerhetskänslig befattning som är placerad i lägst säkerhetsklass 3.

8.3.4.9.3 Inom Sverige

Distribution av handling med säkerhetsskyddsklassificerade uppgifter ska ske med något av följande alternativ:

- av Säkerhetsskyddsavdelningen godkänd krypterad överföring (se kapitel 11 Signalskydd och bilaga 4 till denna TjF)
- av Säkerhetsskyddsavdelningen godkänd distributör som har erforderligt säkerhetsskyddsavtal med FMV.
- handkurir enligt beskrivning ovan.

8.3.4.9.4 Utanför Sverige

För försändelser till och från utlandet omfattande handlingar med säkerhetsskyddsklassificerade uppgifter och som inte skyddas av kryptografiska funktioner enligt 11, ska Utrikesdepartementets kurirförbindelser anlitas.
(Ref: 3 kap. 10 § SSF)

Not: FMV får inom ramen för ett samarbete med ett annat land eller en mellanfolklig organisation komma överens om att distribuera handlingar med säkerhetsskyddsklassificerade uppgifter på annat sätt än vad som föreskrivs ovan.
(Ref: 3 kap. 29 § FFS-SäkS)

Distribution till utländsk myndighet/företag av handling/lagringsmedium/materiel med uppgifter i säkerhetsskyddsklass Hemlig, Konfidentiell eller Begränsat hemlig får ske i enlighet med de krav som framgår av avsnitt 8.3.3.4.

8.3.4.10 Medförande

8.3.4.10.1 Allmänt

Handlingar och lagringsmedier med säkerhetsskyddsklassificerade uppgifter som medförs från FMV ska vara under kontroll eller förvaras på ett sätt som motsvarar den skyddsklass som gäller för förvaringen av handlingarna respektive lagringsmedierna inom FMV:s lokaler.

En handling eller ett lagringsmedium med säkerhetsskyddsklassificerade uppgifter som har medförts utanför myndighetens lokaler eller områden ska snarast möjligt återföras eller överlämnas till den som ska förvara handlingen eller lagringsmediet.
(Ref: 3 kap. 20 § FFS-SäkS)

Not: Angående förteckning över medförda handlingar/lagringsmedier/materiel, se avsnitt 8.2.5.4.

Not: Lån av handlingar förekommer t.ex. i samband med rättssak.

8.3.4.10.2 Inom Sverige

Beslut om medförande av handling/lagringsmedium/materiel utanför FMV:s lokaler fattas enligt delegeringsordning med följande begränsning:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning.
- för uppgifter i säkerhetsskyddsklass Begränsat hemlig krävs beslut endast för inhyrd personal.

Beslut om medförande enligt ovan ska lägst åsättas säkerhetsskyddsklass Begränsat hemlig och sekretessmarkeras 18 kap. 8 § OSL, om det inte finns skäl för annan bedömning.

8.3.4.10.3 Utanför Sverige

Beslut om medförande utanför Sverige av handling/lagringsmedium/materiel, vilken ska återföras till FMV, fattas enligt delegeringsordning med följande begränsning:

- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef VerkO/CS i samråd med säkerhetsskyddschef eller av denne utsedd, alternativt högre chef
- för FMV-anställds medförande av uppgifter i säkerhetsskyddsklass Begränsat hemlig krävs inget beslut
- för inhyrd personals medförande, oavsett säkerhetsskyddsklass, krävs beslut.

Beslut om medförande enligt ovan ska lägst åsättas säkerhetsskyddsklass Begränsat hemlig och sekretess-markeras 18 kap. 8 § OSL, om det inte finns skäl för annan bedömning.

8.3.4.11 Transport

8.3.4.11.1 Allmänt

Chef ska besluta hur transport av handlingar/lagringsmedium/materiel med säkerhetsskyddsklassificerade uppgifter ska genomföras.
(Ref: 3 kap. 26 § FFS-SäkS)

När handlingar/lagringsmedier/materiel med säkerhetsskyddsklassificerade uppgifter ska transporteras, distribueras eller förflyttas, ska erforderligt skydd finnas.

8.3.4.11.2 Transportsäkerhetsanalys

Den chef som avser genomföra transport av handlingar/lagringsmedier/materiel med säkerhetsskydds-klassificerade uppgifter ska göra en transportsäkerhetsanalys och besluta transportnivån i enlighet med bilaga 7 till denna TjF före varje sådan transport.

8.3.4.11.3 Transportsäkerhetsplan

Inför en transport i transportnivå 2, 3 eller 4 ska chef låta planera transporten och upprätta en transport-säkerhetsplan. Transportsäkerhetsplanen ska innehålla detaljer om transporten och minst innehålla färdväg, deltagare och eventuella rastplatser.

Transportsäkerhetsplanen ska dokumenteras.

8.3.4.11.4 Meddelande till andra myndigheter

Innan en skyddad transport i transportnivå 3 eller 4 påbörjas ska den som organiserar transporten informera nedanstående om att en skyddad transport ska genomföras:

- mottagaren av godset,
- Polismyndigheten och
- Försvarsmakten, i de fall transporten berör Försvarsmakten.

8.3.4.11.5 Genomförande av skyddad transport

Vid en skyddad transport ska om möjligt nycklar eller koder till förvaringsutrymmen som ingår i transporten tillställas mottagaren i en separat försändelse eller överföras med krypterat sambandsmedel.

Om nycklar eller koder följer med transporten, ska de förvaras dolda i en följebil eller hos transportskydds-styrkan. När följebil eller transportskyddsstyrka inte finns ska nycklar eller koder förvaras dolda i transport-fordonet.

Vid uppehåll under transporten ska samma skydd upprätthållas som gäller för transporten.

9 Informationssäkerhet i och kring informationssystem (IT-säkerhet)

Användning av informationssystem inom FMV regleras av TjF för användning av FMV:s IT-system.

Metod för godkännande av FMV:s IT-system beskrivs i Ackrediteringsmetod FMV IT-system (18FMV34237-3:1).

Not: Av 4 kap. 1 § FFS-SäkS framgår att vad som anges om informationssystem gäller även för sådana informationssystem som utgörs endast av ett elektroniskt kommunikationsnät.
(Ref: 4 kap. 1 § FFS-SäkS)

9.1 Verksamhetslogik för informationssäkerhet i och kring informationssystem

- Utgående från analys av den verksamhet som skall bedrivas och stödjas av ett informationssystem formuleras krav på säkerhetsskyddsegenskaper och säkerhetsskyddsåtgärder.
- Informationssystemet konstrueras och konfigureras tekniskt och administrativt för att uppfylla ställda krav.
- Kravuppfyllnad verifieras på lämpligt sätt, understödd av dokumentation och ev. annan evidens.
- Beslut fattas om ackreditering.

9.2 Hantering av uppgifter som omfattas av sekretess

Uppgifter som omfattas av sekretess får endast hanteras i för ändamålet av FMV godkända informationssystem.

9.3 Hantering av säkerhetsskyddsklassificerade uppgifter

Säkerhetsskyddsklassificerade uppgifter får endast hanteras i för ändamålet av FMV godkända informationssystem.

9.4 Säkerhetskrav för informationssystem som har betydelse för säkerhetskänslig verksamhet

9.4.1 Säkerhetsfunktioner i och säkerhetsskyddsåtgärder för informationssystem

9.4.1.1 Behörighetskontroll

FMV:s informationssystem ska ha förmåga att verifiera användares identitet och behörighet innan dessa ges tillgång till systemet, samt styra åtkomst till uppgifter, funktioner och resurser i systemet enbart till de användare som har tilldelats behörighet till dessa.
(Ref: 4 kap. 15 § FFS-SäkS)

Not: Vad som gäller för användare i första stycket gäller också för informationssystem och processer i informationssystem som ges tillgång till uppgifter, funktioner och resurser.

Tilldelning av identiteter och behörigheter i informationssystem ska vara möjlig att granska för att klarlägga vilka användare eller resurser som har tillgång till systemet och vilka behörigheter som de har tilldelats i systemet. Systemansvarig chef ska regelbundet granska behörigheterna för att se till att de är ändamålsenliga och aktuella.
(Ref: 4 kap. 16 § FFS-SäkS)

9.4.1.2 Loggning

FMV:s informationssystem ska ha förmåga att i säkerhetsloggar registrera händelser i eller kring systemet som är av betydelse för säkerheten. Systemansvarig chef ska regelbundet genomföra analys av säkerhetsloggar för informationssystem som är avsedd att användas av flera personer. Analysen ska dokumenteras.
(Ref: 4 kap. 17 § FFS-SäkS)

Not: Av RA-MS 2018:42 framgår vad som ska loggas

9.4.1.3 Intrångsdetektion och avvärjande

FMV:s informationssystem ska ha förmåga att detektera och avvärja intrång, försök till intrång eller skadlig inverkan på systemet samt detektera och avvärja obehörig kommunikation med systemet.
(Ref: 4 kap. 19 § FFS-SäkS)

9.4.1.4 Separation

Inom FMV förekommande informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara separerade från övriga informationssystem som inte omfattas av krav på säkerhetsskydd.
(Ref: 4 kap. 20 § FFS-SäkS)

9.4.1.5 Kommunikation

För informationssystem som har betydelse för säkerhetskänslig verksamhet ska systemansvarig chef vidta skyddsåtgärder som ger förmåga att försvåra att uppgifter kommer obehöriga till del, ändras eller förstörs vid kommunikation mellan informationssystemets delsystem eller vid kommunikation till andra informationssystem.
(Ref: 4 kap. 26 § FFS-SäkS)

9.4.1.6 Skydd mot skadlig/obehörig kod

FMV:s informationssystem ska ha förmåga att försvåra och upptäcka inmatning, försök till inmatning, exekvering eller försök till exekvering av skadlig kod eller annan obehörig kod i systemet.
(Ref: 4 kap. 21 § FFS-SäkS)

9.4.1.7 Integritet

FMV:s informationssystem ska ha förmåga att upptäcka och försvåra obehörig förändring (bevarande av integritet) av informationssystemet och dess säkerhetsskydd.
(Ref: 4 kap. 22 § FFS-SäkS)

9.4.1.8 Tillgänglighet, säkerhetskopiering

FMV:s informationssystem ska ha förmåga att säkerhetskopiera och vid behov återställa mjukvara, konfigurationsdata och andra uppgifter som är av betydelse för verksamheten, informationssystemets funktion eller säkerhetsskyddet, och som inte lätt kan återskapas på annat sätt.
(Ref: 4 kap. 23 § FFS-SäkS)

9.4.1.9 Röjande signaler (RÖS)

CIO ska besluta om säkerhetskrav för skydd mot röjande signaler (RÖS).
(Ref: 4 kap. 25 § FFS-SäkS)

Systemansvarig chef ska beakta risken för röjande signaler och vidta lämpliga skyddsåtgärder för systemet om

- informationssystemet avses behandla uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre, eller
- obehörig åtkomst till informationssystemet kan medföra en icke obetydlig skada.

(Ref: 3 kap. 4 § SSF)

9.4.1.10 Konfiguration

FMV:s informationssystem ska konfigureras för att minska sårbarheter genom att ta bort eller stänga av funktioner och tjänster som inte behövs, använda lämpliga och möjliga säkerhetsfunktioner i systemet samt konfigurera systemet utifrån vedertagna rekommendationer och krav identifierade genom ackrediteringsprocessen.
(Ref: 4 kap. 27 § FFS-SäkS)

9.4.1.11 IT-utrymmen

Om det i IT-utrymmen behandlas säkerhetsskyddsklassificerade uppgifter ska dessa utrymmen uppfylla krav enligt bilaga 2 till denna TjF, avsnitt 3.1.
(Ref: 5 kap. 21-22 §§ FFS-SäkS)

Av 5 kap. 23 § FFS-SäkS framgår att IT-utrymmen ska förses med ett system för inpasseringskontroll.

Av systemet ska det framgå när och vem som har haft tillträde till utrymmet samt andra händelser som är av betydelse för säkerheten.
(Ref: 5 kap. 23 § FFS-SäkS)

Ett IT-utrymme där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan vara allvarlig eller synnerligen allvarlig (motsv. H eller KH), ska uppfylla de krav som gäller för hantering av uppgifter i säkerhetsskyddsklasserna Hemlig resp. Kvalificerat hemlig enligt bilaga 2, avsnitt 3 och 4.
(Ref: 5 kap. 24 § FFS-SäkS)

9.4.2 Dokumentation

Chef ska tillse att dokumentera de informationssystem som har betydelse för säkerhetskänslig verksamhet. System som är av särskild betydelse när Sverige och FMV befinner sig i höjd beredskap ska dokumenteras inom ramen för FMV:s beredskapsplanverk.

Dokumentationen ska beskriva systemets hård- och mjukvara, systemets kommunikation och beroenden, informationsflöden och datautbyten samt de skyddsåtgärder som avser systemet och vad som i övrigt är av betydelse för att kunna upprätthålla säkerheten i och kring systemet.
(Ref: 4 kap. 11 § FFS-SäkS)

9.4.3 Drift och övervakning

Systemansvarig chef ska tillse kontinuerlig övervakning av de informationssystem som är anslutna till ett elektroniskt kommunikationsnät, och som har betydelse för säkerhetskänslig verksamhet, för att kunna upptäcka, analysera och bedöma förändringar och händelser som kan indikera skadlig eller obehörig påverkan, åtkomst eller nyttjande, eller försök till detta, eller obehörig dataöverföring till eller från systemet.
(Ref: 4 kap. 12 § FFS-SäkS)

9.4.4 Förvaltning

Systemansvarig chef ska tillse fortlöpande förvaltning och underhåll av de informationssystem som har betydelse för säkerhetskänslig verksamhet så att säkerhetsskyddet i och kring systemen kan upprätthållas.
(Ref: 4 kap. 10 § FFS-SäkS)

Säkerhetsfunktionerna och säkerhetskyddsåtgärderna i och kring ett informationssystem som ska användas i säkerhetskänslig verksamhet ska fortlöpande anpassas för att möta förändringar i hot och ny kunskap om sårbarheter. Vid behov ska den särskilda säkerhetsskyddsbedömningen och dokumentationen av informationssystemet uppdateras.
(Ref: 4 kap. 13 § FFS-SäkS)

9.4.4.1 Uppföljning av säkerhetsgodkännande

Ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska godkännas från säkerhetsskyddssynpunkt (ackrediteras) på nytt, om det sker förändringar i eller kring systemet som negativt kan påverka säkerheten i systemet. Ett sådant godkännande ska föregås av uppdatering av den särskilda säkerhetsskyddsbedömningen och granskning enligt avsnitt 9.4.7.1.
(Ref: 4 kap. 14 § FFS-SäkS)

9.4.5 Rutiner

I de fall FMV avser att använda ett informationssystem i säkerhetskänslig verksamhet ska systemansvarig chef besluta vilka rutiner, resurser och kompetenser för drift, förvaltning, underhåll, övervakning och hantering av incidenter som är nödvändiga ur säkerhetsskyddssynpunkt under hela systemets livscykel.
(Ref: 4 kap. 10 § FFS-SäkS)

9.4.5.1 Kvittering av elektronisk handling

Vid delgivning av en säkerhetsskyddsklassificerad elektronisk handling skall mottagandet kvitteras.
(Ref: 3 kap. 15 § FFS-SäkS)

Not: Mottagande av en säkerhetsskyddad elektronisk handling inte behöver kvitteras om mottagandet sker i ett informationssystem där det i en säkerhetslogg noteras vem som tagit del av handlingen.
(Ref: 3 kap. 15 § FFS-SäkS)

9.4.5.2 Säkerhetsloggar, säkerhetskopior

Av 4 kap. 18 § FFS-SäkS framgår att säkerhetsloggar och säkerhetskopior av dessa ska skyddas så att de finns tillgängliga när de behövs, att deras riktighet bevaras och att obehörig åtkomst försvåras.
(Ref: 4 kap. 18 § FFS-SäkS)

Av 4 kap. 24 § FFS-SäkS framgår att säkerhetskopior ska förvaras åtskilt från informationssystemet och skyddas så att de finns tillgängliga när de behövs, att deras riktighet bevaras och att obehörig åtkomst till säkerhetskopiorna försvåras.

Av 4 kap. 23 § FFS-SäkS framgår att kontroll av att säkerhetskopior kan återläsas ska genomföras regelbundet.

9.4.6 Hantering av lagringsmedier avsedda för säkerhetsskyddsklassificerade uppgifter

Se kapitel 10.

9.4.7 Förberedande åtgärder inför driftsättning av informationssystem

9.4.7.1 Särskild säkerhetsskyddsbedömning

Systemansvarig chef ska göra särskild säkerhetsskyddsbedömning inför driftsättning av informationssystem, som ska utgå från verksamhetens säkerhetsskyddsanalys och omfatta de hot och sårbarheter som finns i och kring systemet samt en beskrivning av den säkerhetskänsliga verksamhet som systemet ska stödja.

Systemansvarig chef ska i den särskilda säkerhetsskyddsbedömningen, utöver krav på skydd mot röjande av de säkerhetsskyddsklassificerade uppgifter som kommer att hanteras i informationssystemet, också ta ställning till den säkerhetskänsliga verksamhetens krav på tillgänglighet till informationssystemet, och de uppgifter som behandlas i det, och verksamhetens krav på riktighet för dessa uppgifter.
(Ref: 3 kap. 1 § SSF)

Not: Särskild säkerhetsskyddsbedömning innefattar analys, värdering och bedömning.

Systemansvarig chef ska genom granskning eller på annat sätt förvissa sig så långt möjligt om att den maskin- och programvara som ska användas i ett informationssystem som har betydelse för säkerhetskänslig verksamhet bedöms vara tillförlitlig från säkerhetsskyddsynpunkt.
(Ref: 4 kap. 7 § FFS-SäkS)

9.4.7.2 Ackreditering

Systemansvarig chef ska tillse granskning och godkännande av att

- säkerhetsfunktionerna och skyddsåtgärderna i och kring informationssystemet uppfyller de säkerhetskrav som har identifierats i den särskilda säkerhetsskyddsbedömningen och att
- säkerhetsfunktionerna och skyddsåtgärderna som beskrivs i avsnitt 9.4.1 har implementerats och ger avsedd förmåga.

I granskningen ska systemets säkerhetsförmåga testas.

Granskningen och godkännandet ska dokumenteras.

De personer som ansvarar för utvecklingen av systemet får inte ansvara för granskningen och godkännandet av skyddsåtgärderna.

Ett informationssystem får inte godkännas från säkerhetssynpunkt (ackrediteras) innan åtgärderna (ovan, i detta krav) har godkänts.
(Ref: 4 kap. 6 § FFS-SäkS)

Not: Metod för godkännande av FMV:s IT-system beskrivs i Ackrediteringsmetod FMV IT-system (18FMV3427-3:1).

Not: Ackrediteringsbeslut rörande respektive FMV:s IT-tjänster fattas av CIO. För IT-tjänster som tillhandahålls av Försvarsmakten och nyttjas av FMV, fattas IT-förändringsbeslut enligt Försvarsmaktens IT-styrmodell och IT-process. För IT-tjänster som tillhandahålls av FMV och nyttjas av Försvarsmakten, fattas IT-förändringsbeslut enligt FMV:s IT-styrmodell och IT-process.
(Ref: Annex A.10.1 SAMÖ)

9.4.7.3 Samråd med Försvarsmakten

Innan ett informationssystem som kan förutses komma att behandla uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras, ska systemansvarig chef skriftligen samråda med Försvarsmakten.

Samrådsskyldigheten gäller även i fråga om andra informationssystem än sådana som anges i stycket ovan, där obehörig åtkomst till systemen kan medföra en skada som inte är obetydlig.
(Ref: 3 kap. 2 § SSF)

En begäran om samråd enligt ovan ska ställas till Försvarsmakten. De uppgifter som Försvarsmakten efterfrågar ska tillhandahållas av FMV.
(Ref: 4 kap. 9 § FFS-SäkS)

9.4.7.4 Utkontraktering av informationsbehandling

Innan säkerhetsskyddsklassificerade uppgifter behandlas i ett informationssystem utanför i FMV ansvarig chefs kontroll, ska denne försäkra sig om att informationssystemet är godkänt för ändamålet och att säkerhetsskyddet för uppgifterna i systemet är tillräckligt.
(Ref: 3 kap. 5 § SSF)

Not: Utkontraktering kräver normalt reglering i form av säkerhetsskyddsavtal.

10 Lagringsmedier och säkerhetskänslig materiel

10.1 Allmänt

Lagringsmedier för digital hantering av uppgifter, t.ex. i form av elektroniska handlingar, omfattas av krav enligt detta kapitel. Exempel på lagringsmedier är CD- eller DVD-skivor, USB-stickor och hårddiskar. Utdaterat?

Materiel kan (på samma sätt som fysiska handlingar) innehålla explicita uppgifter som kan omfattas av sekretess eller vara säkerhetsskyddsklassificerade.

Materiel kan även ha sådana egenskaper, att det genom observation eller inspektion går att inhämta uppgifter om materielen. Man kan säga att materielen avspeglar dessa uppgifter, eller att uppgifterna kan härledas direkt från materielen. Sådana "avspeglade" uppgifter kan också omfattas av sekretess eller vara säkerhetsskyddsklassificerade.

Med termen Säkerhetskänslig materiel avses i denna TjF materiel som innehåller säkerhetsskydds-klassificerade explicita eller "härledbara" uppgifter, samt materiel som är oundgänglig för att bedriva säkerhetskänslig verksamhet.

10.2 Lagringsmedier

10.2.1 Lagringsmedier för uppgifter som omfattas av sekretess

10.2.1.1 Märkning av lagringsmedier för uppgifter som omfattas av sekretess

Lagringsmedier med uppgifter som omfattas av sekretess och som inte är försedd med av Säkerhetsskydds-avdelningen godkänd kryptering ska om möjligt märkas med upplysning om tillämpligt lagrum enligt OSL.

Not: Exempel på tekniska begränsningar: storlek, material etc.

10.2.2 Lagringsmedier för säkerhetsskyddsklassificerade uppgifter

10.2.2.1 Hantering av lagringsmedier i informationssystem

Ett lagringsmedium avsett för säkerhetsskyddsklassificerade uppgifter får endast hanteras i ett informations-system som uppfyller de krav som gäller för hantering av uppgifter i den högsta säkerhetsskyddsklass som någon av uppgifterna på lagringsmediet har eller kan komma att ha.
(Ref: 4 kap. 2 § FFS-SäkS)

Not: Informationssystemet ska även vara godkänt för användning av ett sådant lagringsmedium samt de säkerhetsskyddsklassificerade uppgifter det innehåller.

Ett lagringsmedium som innehåller eller har innehållit uppgifter i säkerhetsskyddsklass Hemlig eller Kvalificerat hemlig får inte återanvändas i

- informationssystem som är avsedda för behandling av säkerhetsskyddsklassificerade uppgifter som är placerade i lägre säkerhetsskyddsklass, eller
- andra informationssystem (d.v.s. som inte är avsedda för behandling av säkerhetsskydds-klassificerade uppgifter).

(Ref: 4 kap. 3 § FFS-SäkS)

10.2.2.2 Märkning av lagringsmedier för säkerhetsskyddsklassificerade uppgifter

Ett lagringsmedium med säkerhetsskyddsklassificerade uppgifter och som inte är försedd med av Säkerhets-skyddsavdelningen godkänd kryptering ska på höljet förses med en anteckning (märkning) om den högsta säkerhetsskyddsklass lagringsmediet är avsett för.

Om lagringsmediet är fast monterat i utrustning som omöjliggör märkning på lagringsmediet ska märkningen i stället göras på utrustningen eller annan lämplig plats i anslutning till lagringsmediet.
(Ref: 3 kap. 8 § FFS-SäkS)

Ett lagringsmedium med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre ska märkas med identifieringsuppgift på höljet.

Om lagringsmediet är fast monterat i utrustning som omöjliggör märkning på lagringsmediet ska märkningen i stället göras på utrustningen eller annan lämplig plats i anslutning till lagringsmediet.
(Ref: 3 kap. 13 § FFS-SäkS)

Om ett lagringsmedium med säkerhetsskyddsklassificerade uppgifter kan antas komma att lämnas över till utländska myndigheter eller leverantörer ska lagringsmediet förses med en märkning om uppgifternas ursprungsland om det inte är olämpligt. Vem avgör det? Hur?
(Ref: 3 kap. 28 § FFS-SäkS)

10.2.2.3 Registrering och kvittering av lagringsmedier för säkerhetsskyddsklassificerade uppgifter

Lagringsmedier avsedda för hantering av uppgifter i säkerhetsskyddsklass Konfidentiellt eller högre ska registreras vid FMV:s registratorsfunktion eller enligt ackrediteringsbeslut. Av registret ska det framgå lagringsmediets identifieringsuppgifter, vem som förvarar det och om mediet har förkommit, arkiverats eller förstörts.
(Ref: 3 kap. 19 § FFS-SäkS)

Not: Ett lagringsmedium med säkerhetsskyddsklassificerade uppgifter som används endast en gång för omedelbar överföring av säkerhetsskyddsklassificerade uppgifter mellan två informationssystem och som därefter omedelbart förstörs behöver inte föras in i något register.
(Ref: 3 kap. 19 § FFS-SäkS)

När ett lagringsmedium med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre lämnas ut, ska mottagandet kvitteras med underskrift, namnförtydligande och datum. Ett namnförtydligande får vara en kod.

När ett lagringsmedium med säkerhetsskyddsklassificerade uppgifter återlämnas ska detta kvitteras.
(Ref: 3 kap. 15 § FFS-SäkS)

10.2.2.4 Inventering av lagringsmedier för säkerhetsskyddsklassificerade uppgifter

Lagringsmedier med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre ska inventeras en gång per år och vid behov.
(Ref: 3 kap. 22 § FFS-SäkS)

10.2.2.5 Förstöring av lagringsmedier

Förstöring av lagringsmedier med säkerhetsskyddsklassificerade uppgifter ska ske så att återskapande av uppgifterna omöjliggörs.

Förstöring av lagringsmedier med uppgifter i säkerhetsskyddsklass Konfidentiell eller högre ska registreras.
(Ref: 3 kap. 24 § FFS-SäkS)

Not: Om lagringsmediet är registrerat måste det först återlämnas/avregistreras innan destruktion sker.

10.2.2.6 Distribution av lagringsmedier

Distribution av lagringsmedier med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre ska uppfylla de krav som ställs på distribution av handlingar i avsnitt 8.3.4.9.
(Ref: 3 kap. 25 § FFS-SäkS)

10.2.2.7 Medförande av lagringsmedier

Chef ska besluta i vilken omfattning lagringsmedier med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre får medföras från FMV:s lokaler eller områden.

Medförande av lagringsmedier ska i övrigt uppfylla de krav som ställs på medförande av handlingar i avsnitt 8.3.4.10.
(Ref: 3 kap. 20 § FFS-SäkS)

10.3 Säkerhetskänslig materiel

Säkerhetskänslig materiel ska ges ett säkerhetsskydd som motsvarar det som gäller för lagringsmedier som innehåller säkerhetsskyddsklassificerade uppgifter.
(Ref: 3 kap. 3 § FFS-SäkS)

Säkerhetskänslig materiel ska delas in i säkerhetsskyddsklasser utifrån den skada som en förlust av materielens konfidentialitet, integritet eller tillgänglighet skulle innebära för Sveriges säkerhet eller relationer till omvärlden.

Säkerhetskyddsklasserna ska vara desamma som för säkerhetsskyddsklassificerade uppgifter. Se avsnitt 8.3.1.1.

För säkerhetskänslig materiel gäller tillämpliga delar av kraven för lagringsmedier i detta kapitel.

10.3.1 Märkning av materiel med uppgifter som omfattas av sekretess

Materiel med uppgifter som omfattas av sekretess ska om det är lämpligt och möjligt märkas med upplysning om tillämpligt lagrum enligt OSL.

10.3.2 Registrering och kvittering av säkerhetskänslig materiel

Förteckning över materiel med säkerhetsskyddsklassificerade uppgifter ska föras i ett för ändamålet upprättat register av den som ansvarar för materielen.

Materiel med uppgifter i säkerhetskyddsklass Konfidentiell eller högre ska kvitteras. Tidpunkt och vem som kvitterat materielen ska framgå av ovan nämnda register.

11 Signalskydd

Bestämmelser för signalskyddstjänsten framgår av FMV:s Signalskyddsinstruktion (19FMV6857-1:1)

Not: För signalskyddstjänsten inklusive kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet ska Försvarsmaktens föreskrifter om signalskyddstjänsten (FFS 2016:3) tillämpas.
(Ref: 1 kap. 4 § FFS-SäkS)

Endast av Säkerhetsskyddsavdelningen godkänd signalskydds- och kryptomateriel får användas för att förmedla sekretessbelagda eller säkerhetsskyddsklassificerade uppgifter genom telekommunikation (t.ex. tal, telefax, e-post etc.) enligt bilaga 4.

Signalskyddsmateriel ska inventeras vid behov, dock minst en gång per år. Resultatet av genomförd inventering ska dokumenteras och redovisas till Säkerhetsskyddsavdelningen.

12 Fysisk säkerhet

12.1 Allmänt

FMV:s verksamhet avseende fysisk säkerhet har som mål att

- förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs, och
- förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt som avses i första punkten.

(Ref: 2 kap. 3 § SSL)

Ansvarig chef ska vidta de fysiska säkerhetsskyddsåtgärder som krävs för att skydda säkerhetsskydds-klassificerade uppgifter och säkerhetskänslig verksamhet.
(Ref: 5 kap. 1 § FFS-SäkS)

12.2 Verksamhetsställen, byggnader, anläggningar, områden

I skyddslagen (2010:305) finns bestämmelser om förbud mot tillträde till vissa byggnader, andra anläggningar, områden och objekt.
(Ref: 1 kap. 5 § SSL)

Av 4 kap. 1 § SSF framgår att områden, byggnader och andra anläggningar eller objekt där säkerhetsskydds-klassificerade uppgifter förvaras eller annars behandlas, eller där säkerhetskänslig verksamhet i övrigt bedrivs, ska vara försedda med funktioner för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan utifrån ett identifierat säkerhetsskyddsbehov.

12.2.1 Skyddsobjekt

Chef ansvarig för säkerhetskänslig verksamhet ska i samråd med Säkerhetsskyddsavdelningen besluta om ansökan om skyddsobjekt enligt skyddslagen (2010:305) för berörd anläggning eller berört område där verksamhet bedrivs.

Chef ska föra en förteckning över vilka skyddsobjekt med tillhörande beslut som denne ansvarar för och minst årligen delge förteckningen till Säkerhetsskyddsavdelningen.

Av 22 § SKL framgår att den som ansvarar för eller nyttjar ett skyddsobjekt ansvarar för att objektet bevakas och för att upplysning om beslutet om skyddsobjekt lämnas genom tydlig skyltning eller på annat sätt.

Av lokal säkerhetsskyddsinstruktion ska det framgå hur och vem som har rätt att fatta beslut om avsteg från krav i beslutet om skyddsobjekt.

Exempel: Tillfälligt eller permanent undantag från fotoförbud.

För varje skyddsobjekt som FMV disponerar ska det finnas en bevakningsinstruktion. I denna ska särskilt anges vilka kriterier som ska ligga till grund för att medge tillträde till skyddsobjektet.

När byggnader, andra anläggningar och områden nyttjas både av Försvarsmakten och av myndigheter som bedriver civil verksamhet, ska samråd ske med Försvarsmakten. I andra fall ska ett beslut om skyddsobjekt föregås av samråd med berörda statliga myndigheter om det finns behov av det.
(Ref: 4 § SKF)

12.2.2 Bevakning och bevakningssystem

Av 5 kap. 4 § FFS-SäkS framgår att bevakning med personal eller tekniska bevakningssystem ska finnas vid alla passerställen till platser där det bedrivs säkerhetskänslig verksamhet.

Om ett tekniskt bevakningssystem avser

- utrymmen där säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklassen Konfidentiell eller högre förvaras och behandlas, eller
- platser där säkerhetskänslig verksamhet bedrivs och där en inträffad skada kan vara mer än inte obetydlig,

ska säkerhetsskyddet av de centrala delarna i det tekniska bevakningssystemet uppfylla de krav på förvaring som gäller för lägst skyddsklass 2.

Chef ska utreda vilket säkerhetsskydd som bevakningssystemet i sig kräver. En sådan utredning ska dokumenteras.
(Ref: 5 kap. 5 § FFS-SäkS)

Chef ska besluta om vilka skyddsåtgärder som ska vidtas vid larm från områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.
(Ref: 5 kap. 6 § FFS-SäkS)

12.2.3 Tillträdesbegränsning

Chef ansvarar för att rutiner för tillträde till FMV:s områden, byggnader och andra anläggningar eller objekt finns och tillämpas. Rutinerna ska dokumenteras.
(Ref: 5 kap. 2 § FFS-SäkS)

När behörig besöksmottagare medger (myndighetens tillstånd till) tillträde till FMV:s områden, byggnader och andra anläggningar eller objekt där det bedrivs verksamhet som kräver säkerhetsskydd ska denne se till att besökaren har styrkt sin identitet.

Kravet ovan ska tillämpas med beaktande av allmänhetens rätt att utan att uppge sin identitet ta del av allmänna handlingar.

Not: I 2 kap. 18 § TF framgår i vilken utsträckning den som vill ta del av allmänna handlingar får tillfrågas om sin identitet.

Vid FMV ska det för varje besökare antecknas

- dennes namn,
- personnummer, passnummer eller nummer på annan identitetshandling,
- den myndighet, organisation eller motsvarande som besökaren företräder och
- datum för besöket.

Sådana anteckningar ska bevaras i minst 10 år.

Chef ansvarar för att det vid FMV:s anläggningar finns adekvat tillträdeskontroll.

Endast behörig person medges tillträde till FMV:s anläggningar och lokaler.
(Ref: 5 kap. 3 § FFS-SäkS)

12.2.4 Skydd av anläggningar, lokaler och förvaringsutrymmen

I bilaga 2 anges de krav som gäller för skydd av ytor och förvaringsenheter. En förvaringsenhet för handlingar med säkerhetsskyddsklassificerade uppgifter ska uppfylla de krav som framgår av bilaga 2, avsnitt 3 och 4.
(Ref: 5 kap. 12 § FFS-SäkS)

12.2.5 Passerkort

Person som befinner sig inom FMV:s anläggningar och lokaler ska kunna styrka sin identitet med en av FMV godkänd ID-handling enligt bilaga 3.

Samtliga personer som tilldelas passerkort och därmed eget tillträde till FMV ska ha genomfört FMV:s tillträdesutbildning.

12.2.6 Besök vid FMV

Endast anställda vid FMV, eller den inhyrda personal som omfattas av särskilt beslut, är behöriga besöksmottagare.

Vid besök med tillträde till FMV:s anläggningar krävs att besökaren ska kunna styrka sin identitet med en av FMV godkänd ID-handling alternativt genom att en behörig besöksmottagare kan styrka identiteten.

Av besökslogg ska framgå namn, identifiering (passnummer, personnummer eller legitimationsnummer), arbetsgivare (om sådan finns), besöksmottagare samt tidpunkt för besökets början och slut.

Besöksloggen ska sparas i minst 10 år.

Lokala besöksrutiner ska dokumenteras i lokal säkerhetsskyddsinstruktion för respektive verksamhetsställe.

12.2.7 Transport

Bestämmelser avseende transportnivåer framgår av avsnitt 8.3.4.11 och bilaga 7.

13 Uppdrag från annan myndighet

13.1 Allmänt

Uppdrag från annan myndighet ska då uppdraget omfattar säkerhetskänslig verksamhet åtföljas av en säkerhetsskyddsanalys och säkerhetsskyddsplan, som utgör del av grundförutsättningarna för FMV:s säkerhetsskyddsplanering.

Not: Försvarsmakten ska upprätta och kommunicera en säkerhetsskyddsanalys för de uppdrag (beställningar) som läggs till FMV.
(Ref: Annex A.13.3 SAMO)

14 Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)

14.1 Förberedelser inför SUA-upphandling

14.1.1 Säkerhetsskyddsplanering inför SUA-upphandling

Ansvarig chef ska innan en upphandling påbörjas analysera om uppdraget rör säkerhetskänslig verksamhet.

Om upphandlingen rör säkerhetskänslig verksamhet ska ansvarig chef ta fram en plan för hur säkerhetsskyddet ska regleras i uppdraget. Vid behov ska FMV:s säkerhetsskyddsplanering revideras.

Analysen och planen ska dokumenteras.
(Ref: 8 kap. 1 § FFS-SäkS)

14.1.2 Bedömning och kontroll av leverantör

Av 8 kap. 2 § FFS-SäkS framgår att en bedömning av en leverantörs lämplighet från säkerhetsskyddssynpunkt ska göras innan ett säkerhetsskyddsavtal tecknas.

Bedömningen ska dokumenteras.

Innan FMV lämnar ut säkerhetsskyddsklassificerade uppgifter till en leverantör eller när leverantören ska delta i säkerhetskänslig verksamhet ska FMV göra en analys (se avsnitt 7.3).

Analysen ska omfatta leverantörens ledning och övriga hos leverantören som avses delta i den säkerhetskänsliga verksamheten.

Analysen ska dokumenteras.
(Ref: 8 kap. 6 § FFS-SäkS)

Om leverantören utanför FMV:s lokaler ska hantera eller förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre, eller om leverantören utanför FMV:s lokaler ska delta i säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet eller relationer till omvärlden, (SUA nivå 1) ska FMV, om det inte är uppenbart obehövligt, vidta följande åtgärder:

- Kontrollera att lokalerna och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt
- Dokumentera kontrollen
- Se till att det av säkerhetsskyddsavtalet framgår att leverantören ska upprätta en säkerhetsskyddsinstruktion som ska granskas och godkännas av FMV

(Ref: 8 kap. 8 § FFS-SäkS)

14.2 Säkerhetskyddsavtal

Av ArbO FMV framgår att Chef Jurstab är behörig att ingå ett säkerhetsskyddsavtal.
(Ref: 8 kap. 4 § FFS-SäkS)

När FMV avser att genomföra en upphandling och ingå ett avtal om varor, tjänster eller byggentreprenader ska chef se till att det i ett säkerhetsskyddsavtal anges hur kraven på säkerhetsskydd ska tillgodoses av leverantören om

- det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter, eller
- upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet.

(Ref: 2 kap. 6 § SSL)

För uppgifter i säkerhetskyddsklass Begränsat hemlig ska istället för "SUA" en särskild avtalskonstruktion användas (t.ex. ett Non-Disclosure Agreement). Efterlevnaden av ett sådant avtal kontrolleras av avtalsansvarigt VerkO/CS.

När FMV avser att genomföra en upphandling som innebär krav på säkerhetsskyddsavtal i nivå 1, där leverantören kan

- få tillgång till eller möjlighet att förvara uppgifter i säkerhetsskyddsklassen Hemlig eller högre utanför FMV:s lokaler, eller
- få tillgång till säkerhetskänsliga informationssystem utanför FMV:s lokaler och där obehörig åtkomst till systemen kan medföra allvarlig skada för Sveriges säkerhet,

ska chef innan förfarandet inleds

- genom en särskild säkerhetsbedömning identifiera och dokumentera vilka säkerhetsskydds-klassificerade uppgifter eller säkerhetskänsliga informationssystem som leverantören kan få del av och som kräver säkerhetsskydd, och
- samråda med Försvarsmakten.

(Ref: 2 kap. 6 § SSF)

En begäran om samråd ska ställas till Försvarsmakten. Till ett sådant samrådsförfarande ska de uppgifter som Försvarsmakten efterfrågar tillhandahållas.
(Ref: 8 kap. 5 § FFS-SäkS)

När FMV har ingått ett säkerhetsskyddsavtal ska detta anmälas till Säpo.
(Ref: 2 kap. 7 § SSF)

14.2.1 Löpande förvaltning av säkerhetsskyddsavtal

Chef ska se till att den särskilda säkerhetsskyddsbedömningen samt till uppdraget relaterade analyser och planer hålls uppdaterade till dess att säkerhetsskyddsavtalet upphör att gälla.
(Ref: 8 kap. 7 § FFS-SäkS)

14.2.2 Kontroll av efterlevnad av säkerhetsskyddsavtal

Säkerhetsskyddsavdelningen ska kontrollera att en leverantör följer säkerhetsskyddsavtalet. En sådan kontroll ska genomföras minst vart tredje år.

Om säkerhetsskyddsavtalet avser Kvalificerat hemliga uppgifter eller säkerhetskänslig verksamhet som är av synnerlig betydelse för Sverige säkerhet, ska kontrollen genomföras varje år.

Kontrollen ska dokumenteras.
(Ref: 9 kap. 2 § FFS-SäkS)

14.2.3 Uppsägning av säkerhetskyddsavtal

När ett uppdrag som omfattats av ett säkerhetsskyddsavtal upphör, ska den som är ansvarig för uppdraget skyndsamt meddela Säkerhetsskyddsavdelningen om att uppdraget har upphört, så att aktuellt säkerhets-skyddsavtal eventuellt kan sägas upp.

När ett säkerhetsskyddsavtal upphör att gälla ska Säkerhetsskyddsavdelningen anmäla detta till Säpo.
(Ref: 2 kap. 7 § SSF)

15 Överlåtande av säkerhetskänslig verksamhet

En anmälan avseende planerat överlåtande av säkerhetskänslig verksamhet till en enskild verksamhetsutövare ska ställas till Försvarsmakten. Anmälan ska göras snarast, dock senast 6 månader innan den säkerhetskänsliga verksamheten ska överlåtas. Anmälan ska omfatta en beskrivning av den verksamhet som FMV avser att överlåta, när överlåtelsen planeras att genomföras och på vilket sätt överlåtelsen är avsedd att genomföras.
(Ref: 8 kap. 9 § FFS-SäkS)

Ansvarig chef ska vidare upplysa den enskilde verksamhetsutövaren om att SSL gäller för verksamheten. En sådan upplysning ska innehålla en påminnelse om de skyldigheter som enligt SSL gäller för den som är ansvarig för en säkerhetskänslig verksamhet.
(Ref: 2 kap. 9 § SSF)

Beslut om överlåtande av säkerhetskänslig verksamhet till enskild verksamhetsutövare fattas av lägst Chef VerkO/CS.

16 Internationell säkerhetsskyddssamverkan och säkerhetsintyg

Om det i en överenskommelse (som avses i 10 kap. 1 eller 2 §§ regeringsformen som rör ett visst internationellt samarbete) förekommer bestämmelser om säkerhetsskydd som avviker från krav enligt FFS-SäkS ska bestämmelserna i avtalet ha företräde.
(Ref: 11 kap. 1 § FFS-SäkS)

Ett säkerhetsintyg får utfärdas för personer som har sin hemvist i Sverige och leverantörer med säte i Sverige när en annan stat eller en mellanfolklig organisation har ansökt om ett sådant intyg, om

- behov av ett sådant intyg finns vid internationell samverkan om säkerhetskänslig verksamhet enligt SSL, eller
- intyget, utöver vad som följer av första punkten, kan underlätta för en person eller för en leverantör att delta i en verksamhet som en annan stat eller en mellanfolklig organisation bedömer vara i behov av säkerhetsskydd.

Ett intyg enligt ovan får utfärdas endast om deltagandet avser verksamhet i eller för en stat eller en mellanfolklig organisation som omfattas av ett internationellt åtagande om säkerhetsskydd.

Maximal giltighetstid för ett säkerhetsintyg enligt ovan är två år från beslutsdatum.
(Ref: 4 kap. 1 § SSL)

17 Utbildning

Utöver krav i detta kapitel finns krav på utbildning i andra delar av denna TjF.

Chef ska se till att den som anställs eller på annat sätt ska delta i säkerhetskänslig verksamhet får utbildning i säkerhetsskydd. Sådan utbildning ska genomföras innan personen får delta i säkerhetskänslig verksamhet. Behovet av utbildning ska följas upp under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.
(Ref: 7 kap. 1 § FFS-SäkS)

Chef ska tillse att anställda, inhyrd personal, uppdragstagare och andra som deltar i den säkerhetskänsliga verksamheten fortlöpande utbildas och övas i säkerhetsskydd.

Omfattningen och innehållet ska utgå från FMV:s säkerhetsskyddsplan och dokumenteras i en utbildningsplan. Utbildningsplanen beslutas enligt delegeringsordning.

Efter genomförd utbildning skall chef rapportera till HR, som upprätthåller en för FMV samlad förteckning över vilka anställda och andra som har genomgått utbildning i säkerhetsskydd, samt vilken utbildning som genomförts och när.
(Ref: 7 kap. 2 § FFS-SäkS)

18 Kontroll

Chef ska årligen och vid behov kontrollera att regler för säkerhetsskyddet enligt denna TjF följs och att säkerhetsskyddet är anpassat till aktuell säkerhetsskyddsplanering.

Kontrollen ska dokumenteras.
(Ref: 9 kap. 1 § FFS-SäkS)

Chef ska ha en plan för kontroll av den egna verksamhetens säkerhetsskydd. Planen ska uppdateras vid behov och i planen ska det anges vem som är ansvarig för att kontroll och uppföljning genomförs.
(Ref: 9 kap. 3 § FFS-SäkS)

För varje VerkO/CS ska finnas en beslutad plan för internkontroller.

Minst årligen eller vid behov ska VerkO/CS genomföra internkontroll rörande säkerhetsskyddet inklusive signalskyddet inom eget ansvarsområde.

Internkontroll ska dokumenteras och sparas i minst 10 år.

Chef VerkO/CS ansvarar för att årligen till Säkerhetsskyddsavdelningen redovisa en sammanfattning av resultatet av genomförda internkontroller.

När Försvarsmakten genomför tillsyn ska Försvarsmakten få tillgång till sådan dokumentation som krävs för att kunna utöva tillsyn över säkerhetsskyddet.
(Ref: 9 kap. 4 § FFS-SäkS)

19 Incidenthantering, rapportering och anmälan

19.1 Incidenthantering

Säkerhetsskyddsavdelningen ansvarar för att det finns dokumenterade rutiner för hantering av incidenter, avvikelser, fel eller brister relaterade till säkerhetsskyddet.

Chef ansvarar för att gällande rutiner tillämpas för att upptäcka, bedöma och hantera

- incidenter och avvikelser som rör säkerhetskänslig verksamhet samt
- sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse.

(Ref: 1 kap. 3 § FFS-SäkS)

Sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse för Sveriges säkerhet eller relationer till omvärlden ska snarast åtgärdas.

Det åligger all personal att skyndsamt anmäla befarade eller konstaterade brister i säkerhetsskyddet (incidenter).

Chef ska se till att anmälda incidenter som avser sådant som är av vikt för säkerhetsskyddet hanteras skyndsamt. Vid behov ska rapportering även göras till högre chef.

Anmälda incidenter utreds av Säkerhetsskyddskoordinatorn vid det VerkO/CS där incidenten ägt rum eller där incidören är placerad.

19.1.1 Sekretessförlust

Vid en befarad eller konstaterad förlust av sekretess ansvarar berörd chef för att:

- ärendet snarast rapporteras till Säkerhetsskyddsavdelningen och till berörd Säkerhetsskydds-koordinator
- ärendet snarast utreds
- nödvändiga åtgärder vidtas så att skadan reduceras
- en skadebedömning genomförs

19.1.2 Röjande av säkerhetsskyddsklassificerad uppgift

Vid ett befarat eller konstaterat röjande av säkerhetsskyddsklassificerade uppgifter ansvarar berörd chef för att:

- ärendet snarast rapporteras till Säkerhetsskyddsavdelningen och till berörd Säkerhetsskyddskoordinator
- ärendet snarast utreds
- nödvändiga åtgärder vidtas så att skadan reduceras
- en skadebedömning genomförs

19.2 Rapportering och anmälan

19.2.1 Anmälan vid säkerhetshotande händelser/verksamhet

Indikationer på eller konstaterade säkerhetshotande händelser (incidenter) eller allvarlig säkerhetshotande verksamhet ska anmälas till berörd Säkerhetsskyddskoordinator och till Säkerhetsskyddsavdelningen, för eventuell vidare anmälan till Försvarsmakten.

Vid tveksamhet om huruvida en säkerhetshotande verksamhet är allvarlig, ska FMV samverka med Försvarsmakten i bedömningen.
(Ref: 10 kap. 1 § FFS-SäkS)

Säkerhetskyddsavdelningen ska skyndsamt anmäla till Säpo och Försvarsmakten om

- en säkerhetsskyddsklassificerad uppgift kan ha röjts,
- det inträffat en IT-incident i ett informationssystem som FMV är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller
- FMV får kännedom eller misstanke om någon annan för myndigheten allvarlig säkerhetshotande verksamhet.

(Ref: 2 kap. 10 § SSF)

I de fall FMV tillhandahåller tjänster åt en annan verksamhetsutövare ska FMV i samband med anmälan informera och vid behov samråda med de uppdragsgivare som berörs av incidenten.
(Ref: 2 kap. 11 § SSF)

19.2.2 Anmälan av fel, brister och sårbarheter

Av 10 kap. 2 § FFS-SäkS framgår att sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse för Sveriges säkerhet eller relationer till omvärlden ska snarast anmälas till Försvarsmakten.
(Ref: 10 kap. 2 § FFS-SäkS)

Av 10 kap. 3 § FFS-SäkS framgår att av en anmälan ska det framgå typ av händelse, tidpunkt och plats för det inträffade, vilka sårbarheter och brister som har identifierats samt vilken säkerhetskänslig verksamhet som har berörts.
(Ref: 10 kap. 3 § FFS-SäkS)

19.2.3 Rapportering av säkerhetshotande och särskilt säkerhetskänslig verksamhet

Förhållande som tyder på säkerhetshotande verksamhet och incidenter ska snarast rapporteras till Säkerhetsskyddsavdelningen och berörd säkerhetsskyddskoordinator informeras.

Planering och genomförande av särskilt säkerhetskänslig verksamhet ska löpande rapporteras till ansvarig Säkerhetsskyddskoordinator för vidare rapportering till Säkerhetsskyddsavdelningen, för ev. vidare anmälan till Försvarsmakten.

20 Beredning av denna TjF

2019 års revision av denna tjänsteföreskrift har genomförts under ledning av FMV Jurstab Säk.

Arbetsgrupp har utgjorts av Johan Bendz och Kenneth Olofsson, Jurstab Säk, samt Lars Velander, Ledstab Syst.

Referensgrupp har utgjorts av Erik Welleman, Thomas Palfelt och Jesper Rikala, Jurstab Säk, samt Johan Strandman, Jurstab Jur.

Tjänsteföreskriften har tillställts samtliga VerkO/CS för granskning i två omgångar (februari och maj 2019).

21 Tillämpning

Bestämmelserna i denna tjänsteföreskrift gäller för FMV personal. Bestämmelserna kan dessutom i avtal åberopas att i tillämpliga delar gälla för uppdragstagare eller andra som medverkar i FMV verksamhet.

Tillkommande bestämmelser kan förekomma inom vissa områden/verksamheter.

Denna tjänsteföreskrift träder i kraft 2020-01-01.

21.1 Avsteg

Chef Jurstab får besluta om avsteg från bestämmelserna i denna tjänsteföreskrift, om det finns särskilda skäl.

21.2 Övergångsbestämmelser

FMV tillåter fram till och med 2020-03-31 användning av de tidigare använda informationssäkerhetsklasserna i stödsystem som ännu ej anpassats till kraven i denna TjF.
(Ref: Not 3 FFS-SäkS)

21.3 Upphävande av tidigare beslut

Denna tjänsteföreskrift upphäver och ersätter tidigare utgåva (15FMV11468-2:1).

22 Beslut

I den slutliga beslutsberedningen har Chef Jurstab Säk Erik Welleman, informationssäkerhetschef Thomas Palfelt, juristen Johan Strandman och säkerhetsskyddshandläggaren Johan Bendz deltagit, den senare som föredragande.

Anders Sjöborg

Chef Jurstab

Tjänsteföreskrift avseende säkerhetsskydd och sekretess (2020)

Bilaga 1

<1 underbilaga: Bilaga 1-1 - Beslut om lokal delegeringsordning>

Instruktion och beslutsmall för lokal delegeringsordning

1 Allmänt

Underbilaga 1-1 utgör beslutsmall för en för VerkO/CS lokal delegeringsordning avseende beslutsbefogenheter för säkerhetsskydd och sekretess. Beslutsmallen innehåller även beslut som inte behöver delegeras.

2 Bakgrund

Av TjF framgår att:

> Chef VerkO/CS ska besluta om en delegeringsordning avseende beslutsbefogenheter enligt denna TjF, som är anpassad till egen verksamhet och organisation. För GD/ÖD hanteras beslutsbefogenheter i särskild ordning.
>
> I de flesta fall, där beslutsbefogenheter regleras i denna TjF, begränsas delegeringen enligt följande principer/modell:
>
> - För hantering av uppgifter i säkerhetskyddsklass Kvalificerat hemlig är behörig beslutsfattare lägst Chef Avdelning.
> - För hantering av uppgifter i säkerhetskyddsklass Konfidentiell eller Hemlig regleras behörig beslutsfattare av VerkO/CS delegeringsordning.
> - För hantering av uppgifter i säkerhetskyddsklass Begränsat hemlig fattas beslut av enskilda handläggare.
> - För hantering av uppgifter som enbart omfattas av sekretess fattas beslut av enskilda handläggare.
> - För hantering av handlingar, lagringsmedier eller materiel gäller motsvarande ordning.

3 Tillämpning

Mallen kan lämpligen utnyttjas så att Chef VerkO/CS utformar Beslut om lokal delegeringsordning genom att komplettera sidan 1 med aktuella uppgifter, samt att för varje beslutstyp på sidorna 2-4 med kryss i lämplig kolumn ange den lägsta nivå som beslut av den aktuella typen delegeras till.

Beslutsmallen i Word-format kan hämtas på Insidan under Säkerhetsskydd och i FMV VHL.

Den ifyllda blanketten utgör dokumentation av beslutet i fråga och diarieförs i lämpligt säkerhetsskyddsrelaterat ärende inom VerkO/CS. Kopia på beslutet/blanketten tillställs Säkerhetsskyddsavdelningen för kännedom och som underlag för kommande kontroll.

Bilaga 1-1 till FMV TjF Säkerhetsskydd och sekretess (2020) (19FMV6705-1:1)

Ej sekretess

BESLUT

Datum	Diarienummer	Ärendetyp
ange	ange	ange
	Dokumentnummer	Sida
	ange	1(5)
Giltig t.o.m.	Upphäver	
ange	ange	

Beslutande

ange

Föredragande

ange

Beslut om lokal delegeringsordning

Detta beslut reglerar delegering av beslutsbefogenheter inom säkerhetsskyddsfunktionen för <OrgE>.

Blanketten på sidan 2-5 redovisar, för varje beslutstyp i FMV TjF Säkerhetsskydd och sekretess (2020) (19FMV6705-1:1), den lägsta beslutsnivån till vilken beslutsbefogenheter får delegeras inom <OrgE>.

Beslut i detta ärende har fattats av chefen för <OrgE>, NN.
I beredningen av detta beslut har NN, NN och säkerhetsskyddskoordinator NN medverkat, den senare som föredragande.

FÖRSVARETS MATERIELVERK

Sändlista

NN

Säkerhetsskyddsavdelningen
Arkiv

Kap/Avs	Rubrik		C1	C2	C3	C4	Handläggare
4	**Ansvar och beslutsbefogenheter**						
4.2	**Ansvar för säkerhetsskyddet**						
4.2.1	**Chefers ansvar**						
		Chef ansvarar för att lokal säkerhetsskyddsinstruktion och/eller lokal signalskyddsinstruktion beslutas , när behov föreligger.					
4.3	**Beslutsbefogenheter**						
4.3.2	**Delegeringsordning**						
		Chef VerkO/CS ska besluta om en delegeringsordning avseende beslutsbefogenheter enligt denna TjF, som är anpassad till egen verksamhet och organisation. För organisationsenheten GD/ÖD hanteras beslutsbefogenheter i särskild ordning.					
5	**Säkerhetsskyddsorganisation**						
5.1	**Allmänt**						
		Chef VerkO/CS ska besluta om vilken säkerhetsskydds-organisation som behövs för att upprätthålla ett erforderligt säkerhetsskydd inom eget ansvarsområde.					
6	**Säkerhetsskyddsplanering**						
6.1	**Allmänt**						
		Chef VerkO/CS ansvarar för att säkerhetsskyddsplanering för den egna verksamheten finns beslutad.					
		För varje uppdrag/projekt ska en dokumenterad och beslutad säkerhetsskyddsplanering finnas.					
6.3	**Säkerhetsskyddsplan**						
		Av säkerhetsskyddsplanen ska det framgå: .... Planen ska beslutas av verksamhetsansvarig chef.					
7	**Personalsäkerhet**						
7.3	**Identifiering av säkerhetskänsliga befattningar**						
7.3.1	**Analys av befattning**						
		Chef ska analysera vilka säkerhetskänsliga befattningar som finns inom verksamheten... Analysen ska vara beslutad av chef.					
7.5	**Tillsättande av person till säkerhetskänslig befattning**						
7.5.2	**Beslut om tillsättande av person till säkerhetskänslig befattning**						
		Personalansvarig chef ska fatta beslut om tillsättande av person till säkerhetskänslig befattning (oavsett om denna är placerad i säkerhetsklass eller ej) enligt delegeringsordning med följande begränsningar: - för säkerhetsklass 1 - Lägst Chef VerkO/CS - vid avrådan från Säkerhetsskyddsavdelningen ska beslut tas av högre chef efter samråd med Säkerhetsskyddschefen.					
		- för säkerhetsklass 1					
		- för övriga					
8	**Informationssäkerhet**						
8.2	**Uppgifter som omfattas av sekretess**						
8.2.3	**Utlämning av uppgifter som omfattas av sekretess**						
		Utlämning av uppgifter som omfattas av sekretess får göras efter beslut av ansvarig handläggare eller chef.					
8.2.5	**Hantering av handling med uppgifter som omfattas av sekretess**						
8.2.5.1	**Hävande av sekretess (ändring av tidigare bedömning)**						
		I det fall sekretessbedömningen för en uppgift ändras ska beslut om hävande av sekretess fattas av ansvarig handläggare eller chef ...					
8.2.5.4	**Medförande av handling med sekretessbelagda uppgifter**						
		Inhyrd personal får medföra handling med uppgifter som omfattas av sekretess utanför FMV först efter beslut av ansvarig handläggare eller chef.					
8.3	**Uppgifter som omfattas av krav på säkerhetsskydd**						
8.3.1	**Säkerhetsskyddsklassificering**						
		Beslut om säkerhetsskyddsklassificering fattas enligt delegeringsordning.					

Kap/Avs	Rubrik		C1	C2	C3	C4	Handläggare
8.3.1.3	**Ändring av säkerhetskyddsklass (inkl. hävande)**						
		Om klassificeringen av uppgifterna i en registrerad handling ändras till annan säkerhetsskyddsklass än vad som anges på handlingen, inklusive hävande av tidigare klassificering, ska detta beslutas enligt delegeringsordning med följande begränsning: - för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef VerkO/CS.					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig					
		- för övriga uppgifter					
8.3.2	**Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter**						
		Beslut om behörighet att ta del av säkerhetsskyddsklassificerade uppgifter fattas enligt delegeringsordning med följande begränsning: - för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning.					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig					
		- för övriga uppgifter					
		Aktuella behörighetslistor för respektive säkerhetsskyddsklassen Kvalificerat hemlig och för säkerhetsskyddsklasserna Hemlig och Konfidentiell ska upprättas och fastställas av personalansvarig chef....					
8.3.3	**Delgivning av säkerhetsskyddsklassificerade uppgifter**						
8.3.3.1	**Delgivning av säkerhetsskyddsklassificerade uppgifter inom FMV**						
		Delgivning av säkerhetsskyddsklassificerade uppgifter till FMV personal får					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig					
		- för övriga uppgifter					
8.3.3.2	**Utrymmen för muntlig delgivning av säkerhetsskyddsklassificerade uppgifter**						
		Chef Jurstab ska fatta beslut om kraven på de kategorier av utrymmen som är godkända för regelbunden muntlig delgivning av säkerhetsskyddsklassificerade uppgifter som är placerade i säkerhetsskyddsklass Konfidentiell eller högre.	C Jurstab				
8.3.3.3	**Delgivning av säkerhetsskyddsklassificerade uppgifter utanför FMV inom Sverige**						
		Delgivning av säkerhetsskyddsklassificerade uppgifter till svensk myndighet får ske först efter beslut enligt delegeringsordning med följande begränsningar: - för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning.					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig					
		- för övriga uppgifter					
		Delgivning av säkerhetsskyddsklassificerade uppgifter till svenskt företag får ske först efter beslut enligt delegeringsordning delegeringsordning med följande begränsningar: - för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning.					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig					
		- för övriga uppgifter					
8.3.3.4	**Delgivning av säkerhetsskyddsklassificerade uppgifter till utlandet**						
		För delgivning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass Hemlig, Konfidentiell eller Begränsat hemlig till utländsk part krävs (i tillämpliga delar) att: ... - beslut om delgivning har fattats enligt delegeringsordning, ...					
8.3.4	**Hantering av handling med säkerhetsskyddsklassificerade uppgifter**						
8.3.4.3	**Gemensam användning**						
		Beslut om gemensam användning av handlingar/lagrings-medier/materiel					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig					
		- för övriga uppgifter					
8.3.4.4	**Kopiering, utdrag**						
		Beslut om kopiering/utdrag ur handling fattas enligt delegeringsordning med följande begränsning: - för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning - för uppgifter i övriga säkerhetsskyddsklasser krävs inget beslut.					

Kap/Avs	Rubrik		C1	C2	C3	C4	Handläggare
8.3.4.5	**Förvaring**						
8.3.4.5.1	**Samförvaring**						
		Beslut om samfövaring av handlingar/lagringsmedier/materiel fattas enligt delegeringsordning med följande begränsning: - för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning. - för uppgifter i säkerhetsskyddsklass Begränsat hemlig krävs inget beslut.					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig					
		- för uppgifter i säkerhetsskyddsklass Hemlig eller Konfidentiell					
8.3.4.6	**Nycklar, kort och koder**						
		En nyckel, ett kort eller en kod får innehas endast av den som har ansvaret för utrymmet, om inte ansvarig chef har beslutat annat.					
		I det fall den som ansvarar för förvaringsutrymmet inte är närvarande får användande av reservnyckel/-kort/-kod till förvaringsutrymme där handling/lagringsmedium/materiel med uppgifter i säkerhetsskyddsklass Begränsat hemlig eller högre förvaras endast ske efter beslut av berörd chef.					
8.3.4.10	**Medförande**						
8.3.4.10.2	**Inom Sverige**						
		Beslut om medförande av handling/lagringsmedium/ materiel utanför FMV:s lokaler fattas enligt delegeringsordning med följande begränsning: - för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef Avdelning. - för uppgifter i säkerhetsskyddsklass Begränsat hemlig krävs beslut endast för inhyrd personal.					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig					
		- för uppgifter i säkerhetsskyddsklass Hemlig eller Konfidentiell					
		- för uppgifter i säkerhetsskyddsklass Begränsat hemlig, när medförande ska göras av inhyrd personal.					
8.3.4.10.3	**Utanför Sverige**						
		Beslut om medförande utanför Sverige av handling/ lagringsmedium/materiel, vilken ska återföras till FMV, fattas enligt delegeringsordning med följande begränsning: - för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef VerkO/CS i samråd med säkerhetsskyddschef eller av denne utsedd, alternativt högre chef - för FMV-anställds medförande av uppgifter i säkerhetsskyddsklass Begränsat hemlig krävs inget beslut - För inhyrd personals medförande, oavsett säkerhetsskyddsklass, krävs beslut.					
		- för uppgifter i säkerhetsskyddsklass Kvalificerat hemlig - lägst Chef VerkO/CS i samråd med säkerhetsskyddschef eller av denne utsedd, alternativt högre chef					
		- för uppgifter i säkerhetsskyddsklass Hemlig eller Konfidentiell					
		- för uppgifter i säkerhetsskyddsklass Begränsat hemlig, när medförande ska göras av inhyrd personal.					
8.3.4.11	**Transport**						
8.3.4.11.1	**Allmänt**						
		Chef ska besluta hur transport av handlingar/lagrings-medium/materiel med säkerhetsskyddsklassificerade uppgifter ska genomföras.					
8.3.4.11.2	**Transportsäkerhetsanalys**						
		Den chef som avser genomföra transport av handlingar/lagringsmedier/materiel med säkerhetsskyddsklassificerade uppgifter ska göra en transportsäkerhetsanalys och besluta transportnivån i enlighet med bilaga 7 till denna TjF före varje sådan transport.					

Kap/Avs	Rubrik		C1	C2	C3	C4	Handläggare
9	**Informationssäkerhet i och kring informationssystem (IT-säkerhet)**						
9.4	**Säkerhetskrav för informationssystem som har betydelse för säkerhetskänslig verksamhet**						
9.4.1	**Säkerhetsfunktioner i och säkerhetsskyddsåtgärder för informationssystem**						
9.4.1.9	**Röjande signaler (RÖS)**						
		CIO ska besluta om säkerhetskrav för skydd mot röjande signaler (RÖS).	CIO				
9.4.5	**Rutiner**						
		I de fall FMV avser att använda ett informationssystem i säkerhetskänslig verksamhet ska systemansvarig chef besluta vilka rutiner, resurser och kompetenser för drift, förvaltning, underhåll, övervakning och hantering av incidenter som är nödvändiga ur säkerhetsskyddssynpunkt under hela systemets livscykel.					
9.4.7	**Förberedande åtgärder inför driftsättning av informationssystem**						
9.4.7.2	**Ackreditering**						
		Not: Ackrediteringsbeslut rörande respektive FMV:s IT-tjänster fattas av CIO...	CIO				
10	**Lagringsmedier och säkerhetskänslig materiel**						
10.2.2	**Lagringsmedier för säkerhetsskyddsklassificerade uppgifter**						
10.2.2.7	**Medförande av lagringsmedier**						
		Chef ska besluta i vilken omfattning lagringsmedier med uppgifter i säkerhetsskyddsklassen Konfidentiell eller högre får medföras från FMV:s lokaler eller områden.					
12	**Fysisk säkerhet**						
12.2	**Verksamhetsställen, byggnader, anläggningar, områden**						
12.2.1	**Skyddsobjekt**						
		Chef ansvarig för säkerhetskänslig verksamhet ska i samråd med Säkerhetsskyddsavdelningen besluta om ansökan om skyddsobjekt enligt skyddslagen (2010:305) för berörd anläggning eller berört område där verksamhet bedrivs.					
12.2.2	**Bevakning och bevakningssystem**						
		Chef ska besluta om vilka skyddsåtgärder som ska vidtas vid larm från områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.					
15	**Överlåtande av säkerhetskänslig verksamhet**						
		Beslut om överlåtande av säkerhetskänslig verksamhet till enskild verksamhetsutövare fattas av lägst Chef VerkO/CS.					
17	**Utbildning**						
		... Utbildningsplanen beslutas enligt delegeringsordning. ...					
18	**Kontroll**						
		För varje VerkO/CS ska finnas en beslutad plan för internkontroller.					
21	**Tillämpning**						
21.1	**Avsteg**						
		C Jurstab får besluta om avsteg från bestämmelserna i denna tjänsteföreskrift, om det finns särskilda skäl.	C Jurstab				

Tjänsteföreskrift avseende säkerhetsskydd och sekretess (2020)

Bilaga 2-7

Bilaga 2

Krav för ytor och förvaringsenheter

1 Allmänt

Denna bilaga beskriver krav för ytor och förvaringsenheter där säkerhetskänslig verksamhet bedrivs och där säkerhetsskyddsklassificerade uppgifter förekommer.

1.1 Termer, definitioner och exempel

- **Yta** - synonymer till termen yta i denna bilaga är miljö, område, lokal eller utrymme.
- **Förvaring** - med förvaring av säkerhetsskyddsklassificerad uppgift avses alla de sätt på vilken sådan uppgift förvaras då den inte står under ständig uppsikt av behörig person.
- **Förvaringsenheter** - exempel på förvaringsenheter är värdeförvaringsenhet, stöldskyddsskåp, säkerhetsskåp.

1.2 Standarder

- SSF 200 är Svenska Stöldskyddsföreningens norm *Regler för inbrottsskydd – Byggnader och lokaler.*
- SSF 130 är Svenska Stöldskyddsföreningens norm *Regler för projektering och installation av inbrotts- och överfallslarmanläggning.*
- SSF 3492 är Svenska Stöldskyddsföreningens *Regler för säkerhetsskåp – Provning och utvärdering av inbrottsskydd.*
- SS-EN14450 är Svensk Standard/Europanorm *Värdeförvaringsenheter – Krav, klassificering och provning av inbrottsmotstånd – stöldskyddsskåp.*
- SS-EN 1143-1 är Svensk Standard/Europanorm Värdeförvaringsenheter - *Krav, klassificering och provning av inbrottsmotstånd - Del 1: Värdeskåp, uttagsautomater, valvdörrar och valv.*
- SS 25268:2007 är Svensk Standard *Byggakustik - Ljudklassning av utrymmen i byggnader - Vårdlokaler, undervisningslokaler, dag- och fritidshem, kontor och hotell.*

2 Skydd mot obehörig observation eller avlyssning

2.1 Allmänt

FMV skall skydda säkerhetsskyddsklassificerade uppgifter mot obehörig åtkomst (röjande) genom observation (insyn) eller avlyssning.

- Glasytor skall förses med skydd mot insyn, anpassade efter hotbilden. Gardiner eller persienner kan i många fall ge ett tillräckligt skydd.
- Utrustningar med inspelnings- eller kommunikationsförmåga, till exempel surfplattor, mobiltelefoner eller datorer, skall lämnas utanför rum där delgivning av säkerhetsskydds-klassificerade uppgifter sker.

FMV skall vidta erforderliga åtgärder för att minska risken för obehörig avlyssning, till exempel genom att ha kontroll över och runt om lokalen. Risken för att avlyssningsutrustning kan maskeras som i kontorsmiljö vanligen förekommande utrustning skall beaktas.

2.2 Krav på utrymmen för regelbunden muntlig delgivning

Försvarsmakten ställer i FFS-SäkS krav på beslut avseende utrymmen godkända för regelbunden muntlig delgivning av uppgifter i säkerhetsskyddsklass Konfidentiell eller högre. Se TjF, avsnitt 8.3.3.2.

FMV har valt att indela utrymmen för regelbunden muntlig delgivning i kategorier, för att graderat hantera den exponering av säkerhetsklassificerade uppgifter som olika delgivningssituationer innebär.

Kategorierna är:

- Kategori A – särskilt utpekade tjänsterum, chefsrum eller mötesrum.
- Kategori B – särskilt avdelade och hanterade mötesrum, i TrV initialt samordnade med för CMS H/S reserverade mötesrum.
- Kategori C – särskilt avdelade och hanterade mötesrum.

2.2.1 Kategori A

Regelbunden muntlig delgivning av uppgifter upp till och med [säkerhetsskyddsklass Kvalificerat hemlig i mindre omfattning och vid enstaka tillfällen] får endast ske i utrymmen av kategori A eller högre.

Krav på utrymme vid ny- eller ombyggnad

- Innerväggar till utrymmen skall gå ända upp till bjälklag/tak och dimensioneras för att minst innehålla ljudkrav R'w = 35 dB enligt SS 25268:2007.
- Överhörning via ventilationsdon, kabelkanaler och liknande dimensioneras för minst 10 dB högre [ökad dämpning] än ljudkrav på vägg.
- Dörrar och dörrpartier ska minst innehålla ljudkrav R'w = 35 dB.

Krav på passagekontroll

- Tillträde till utrymmet (rummet) eller dess omedelbara omgivning (korridoren) ska vara reglerat med system för passagekontroll, manuellt eller tekniskt.
- Utrymmet ska hållas låst när det inte används av behöriga användare.

Tillåten permanent utrustning
I samband med regelbunden muntlig delgivning får i utrymmet får endast finnas följande permanent installerade, av FMV tillhandahållen och godkänd utrustning:

- Dator SFAP med periferiutrustning
  - Dockningsstation
  - Bildskärm
  - Tangentbord
  - Pekdon
  - Lokal skrivare
  - Headset
- Väggmonterad bildskärm (Signage) eller fast monterad videoprojektor
- Dator SFAP-H (tidigare SFAP-X) med periferiutrustning
- Dator H-LAN med periferiutrustning
- Klientutrustning CMS H/S med periferiutrustning
- Videokonferensutrustning
- Mobiltelefon Robot
- Annan kryptotelefon eller videokonferensutrustning
- Fast telefon (linje, DECT)

Tillåten tillfällig utrustning
I samband med regelbunden muntlig delgivning får endast följande av FMV tillhandahållen och godkänd utrustning tillfälligt medföras och användas i utrymmet:

- Mobil bildskärm (Signage) eller videoprojektor
- Dator SFAP-H (tidigare SFAP-X) med periferiutrustning
- Dator H-LAN med periferiutrustning
- Klientutrustning CMS H/S med periferiutrustning
- Av FMV godkänd annan kryptotelefon eller videokonferensutrustning

Krav för användning

- FMV Checklista för regelbunden muntlig delgivning ska tillämpas

Observera att

- SFAP inte får användas för att hantera säkerhetsskyddsklassificerade uppgifter och ska vara avstängd.
- Av FMV tillhandahållna mobiltelefoner (iPhone och Robot) inte får finnas i utrymmet.
- Ingen annan teknisk utrustning med inspelnings-, lagrings- eller kommunikationsförmåga får finnas i utrymmet.

2.2.2 Kategori B

Regelbunden muntlig delgivning av uppgifter upp till och med [säkerhetsskyddsklass Kvalificerat hemlig i större omfattning **eller** ofta förekommande] får endast ske i utrymmen av kategori B eller högre.

Krav på yta vid ny- eller ombyggnad

- Innerväggar till utrymmen skall gå ända upp till bjälklag/tak och dimensioneras för att innehålla ljudkrav R'w = 47 dB.
- Överhörning via ventilationsdon, kabelkanaler och liknande dimensioneras för minst 10 dB högre [ökad dämpning] än ljudkrav på vägg.
- Dörrar och dörrpartier ska minst innehålla ljudkrav R'w = 47 dB.

Krav på passagekontroll

- Tillträde till utrymmet (rummet) ska vara reglerat med system för passagekontroll, manuellt eller tekniskt.
- Utrymmet ska hållas låst när det inte används av behöriga användare.

Tillåten permanent utrustning

I samband med regelbunden muntlig delgivning får i utrymmet endast finnas följande permanent installerade, av FMV tillhandahållen och godkänd utrustning:

- Dator SFAP-H (tidigare SFAP-X) med periferiutrustning
- Dator H-LAN med periferiutrustning
- Klientutrustning CMS H/S med periferiutrustning

Tillåten tillfällig utrustning

I samband med regelbunden muntlig delgivning får endast följande av FMV tillhandahållen och godkänd utrustning tillfälligt medföras och användas i utrymmet:

- Dator SFAP-H (tidigare SFAP-X) med periferiutrustning
- Dator H-LAN med periferiutrustning
- Klientutrustning CMS H/S med periferiutrustning
- Av FMV godkänd annan kryptotelefon eller videokonferensutrustning

Krav för användning

- FMV Checklista för regelbunden muntlig delgivning ska tillämpas

Observera att

- Mobiltelefon Robot är begränsad till uppgifter i högst säkerhetsskyddsklass Begränsat hemlig
- Av FMV tillhandahållna mobiltelefoner (iPhone och Robot) inte får finnas i utrymmet.
- Ingen annan teknisk utrustning med inspelnings-, lagrings- eller kommunikationsförmåga får finnas i utrymmet.

2.2.3 Kategori C

Regelbunden muntlig delgivning av uppgifter [i säkerhetsskyddsklass Kvalificerat hemlig, i större omfattning **och** ofta förekommande] får endast ske i utrymmen av kategori C eller högre.

Krav på utrymmen i kategori C meddelas i särskild ordning.

3 Mekaniskt skydd

3.1 Krav på ytor och förvaringsenheter där säkerhetsskyddsklassificerade uppgifter förvaras

De civila skyddsklasserna är vedertagna föreskrifter med stor tillgång på produkter och material och som leverantörer av byggtjänster är vana att följa. Godkänd förvaring innebär att krav på antingen yta eller förvaringsenhet är uppfyllda.

Säkerhetsskyddsklass	**Krav på ytor**	**Krav på förvaringsenheter**
Begränsat hemlig	Skyddsklass 1 enl. SSF 200	Låst tjänsterum, låst plåtskåp eller låst träkonstruktion. Exempel på förvaringsenheter för uppgifter framgår av Vägledning.
Konfidentiell och Hemlig	Omslutningsyta i betong med armering max c/c 250 mm och armeringsjärn om minst 10 mm diameter. Certifierad dörr i klass 3 enl. SSF 1078 alt. certifierad dörr enl. SS-EN-1627, RC 4. Fönster lägst P8B enl. SS-EN 356 eller galler certifierade enl. SSF 012, i lägst gallerklass 3.	Säkerhetsskåp enligt SSF 3492 *eller* värdeförvaringsenhet enligt SS-EN 1143-1 lägst grade 0. Förvaringsenheten skall vara försedd med kodlås.
Kvalificerat hemlig	Krav enligt separat beslut, meddelas vid behov av Säkerhetsskyddsavdelningen.	Krav enligt separat beslut, meddelas vid behov av Säkerhetsskyddsavdelningen.

I lokal säkerhetsskyddsinstruktion kan andra krav på mekaniskt skydd framgå, förutsatt att en säkerhets-skyddsanalys motiverar detta. Exempel ges i Vägledning.

3.1.1 Övrigt

Säkra rum eller container-lösningar kan användas för förvaring av säkerhetsskyddsklassificerad uppgift i säkerhetsskyddsklass Konfidentiell eller Hemlig, och får då ersätta användning av säkerhetsskåp enligt SSF 3492. I detta fall skall rummet/containern uppfylla SS-EN 1143-1, lägst grade 0, och placeras i yta som uppfyller skyddsklass 2 enligt SSF 200. Om rummet/containern är en del av omslutningsytan, eller utgör en fristående byggnad, skall det uppfylla SS-EN 1143-1, lägst grade 4. Rum/container skall förses med öppningsskydd i form av invändigt monterade förspända magnetkontakter och invändigt monterade seismiska detektorer i erforderlig omfattning. Rummet/containern skall utgöra separat larmområde.

3.2 Förvaring av säkerhetsskyddsklassificerade uppgifter då säkerhetsskåp eller värdeförvaringsenheter inte kan användas.

Större förvaringslösningar, till exempel rum eller byggnader kan användas för förvaring av hemlig uppgift i säkerhetsskyddsklass Konfidentiell och Hemlig och får då ersätta användning av säkerhetsskåp enligt SSF 3492. I detta fall skall konstruktionen uppfylla SS-EN 1143-1, lägst grade 0, och placeras i yta som uppfyller skyddsklass 2 enligt SSF 200. Om konstruktionen är en del av en omslutningsyta skall den uppfylla SS-EN 1143-1, lägst grade 4. Om konstruktionen utgör en fristående byggnad/motsvarande, skall den uppfylla SS-EN 1143-1, lägst grade 4. Om konstruktionen utgör en fristående byggnad/motsvarande och om den skall

innehålla säkerhetsskyddsklassificerad uppgift i säkerhetsskyddsklass Kvalificerat hemlig, ska krav inhämtas rån Säkerhetsskyddsavdelningen.

Förvaringslösningar enligt detta avsnitt skall ha larmskydd i enlighet med kapitel 4 nedan.

4 Larmskydd

4.1 Larmskydd för ytor där säkerhetsskyddsklassificerade uppgifter förvaras

Säkerhetsskyddsklass	**Krav på larmskydd**
Begränsat hemlig	Larmklass 1 enligt SSF 130. Larmöverföring i larmklass 3 enligt SSF 130.
Konfidentiell och Hemlig	Öppningsskydd i form av förspända magnetkontakter och seismiska detektorer i erforderlig omfattning. Ytan skall utgöra separat larmområde. Larmöverföring i larmklass 3 enligt SSF 130.
Kvalificerat hemlig	Krav enligt separat beslut, meddelas vid behov av Säkerhetsskyddsavdelningen.

I lokal säkerhetsskyddsinstruktion kan andra krav på larmskydd framgå, förutsatt att en säkerhetsskydds-analys motiverar detta. Exempel ges i Vägledning.

4.2 Larmskydd för förvaringsenheter där säkerhetsskyddsklassificerade uppgifter förvaras

Säkerhetsskyddsklass	**Krav på larmskydd**
Begränsat hemlig	Larm som detekterar intrång i förvaringsenheten, t.ex. rörelsedetektor. Larmöverföring i larmklass 3 enligt SSF 130.
Konfidentiell och Hemlig	Öppningsskydd i form av invändigt monterade förspända magnetkontakter och invändigt monterade seismiska detektorer i erforderlig omfattning. Förvaringsenheten skall utgöra separat larmområde. Larmöverföring i larmklass 3 enligt SSF 130.
Kvalificerat hemlig	Krav enligt separat beslut, meddelas vid behov av Säkerhetsskyddsavdelningen.

I lokal säkerhetsskyddsinstruktion kan andra krav på larmskydd framgå, förutsatt att en säkerhetsskydds-analys motiverar detta. Exempel ges i Vägledning.

5 Översättningstabell mellan skyddsnivå och skyddsklass

5.1 Bakgrund

Försvarsmakten ställer krav på fysiskt skydd enligt så kallade skyddsnivåer. Dessa återfinns bland annat i Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2019:2). Dessutom finns Försvarsmaktens syn på fysisk säkerhet i Försvarsmaktens Handbok Säkerhetstjänst Fysisk säkerhet (H Säk Fysisk säkerhet) från 2015.

FMV tillämpar de skyddsklasser som fastställts i Svenska Stöldskyddsföreningens föreskriftsserier. Skyddsklasserna ligger bland annat till grund för försäkringsfrågor. Skyddsklasserna är allmänt accepterade och etablerade. Detta förfaringssätt gör det enklare för såväl FMV som försvarsindustrin att uppfylla relevanta säkerhetsskyddskrav. FMV reglerar kraven på fysiskt skydd internt genom myndighetens Tjänsteföreskrift för säkerhetsskydd och sekretess och externt gentemot industrin genom Industrisäkerhetsskyddsmanualen (ISM).

Eftersom skyddsnivåer och skyddsklasser inte är sinsemellan direkt översättningsbara, har det sedan lång tid funnits behov av en tolkning av gällande regelverk så att erforderligt fysiskt skydd kan uppnås.

Försvarsmaktens skyddsnivåer ska alltså ej användas för kravställning för fysisk säkerhet vid FMV. Endast Svenska Stöldskyddsföreningens föreskriftsserier gäller, se översättningstabellen nedan.

5.2 Översättningstabell

FMV har tagit fram en översättningstabell med tillhörande förklaringar. Syftet är att säkerställa att Försvarsmaktens krav på fysiskt skydd tillgodoses med hjälp av civila regelverk. Detta underlättar vid ny- och ombyggnad av lokaler, eftersom de civila skyddsklasserna är vedertagna föreskrifter med stor tillgång på produkter och material och som leverantörer av byggtjänster är vana att följa.

Försvars-maktens skyddsnivåer	**FMV:s krav på yta**	**FMV:s krav på förvaringsenhet**	**FMV:s krav på larm**
1	Får ej användas vid FMV eller av leverantörer för hantering och förvaring av säkerhetsskyddsklassificerad uppgift oavsett säkerhetsskyddsklass.		
2	Krav enligt Begränsat hemlig i tabell avsnitt 3.1.	Stöldskyddsskåp enligt EN 14450 lägst klass S2 *eller* säkerhetsskåp enligt SSF 3492	Se kapitel 4
3	Krav enligt Konfidentiell och Hemlig i tabell avsnitt 3.1. [1]	Krav enligt Konfidentiell och Hemlig i tabell avsnitt 3.1.	Se kapitel 4
4	Krav enligt separat beslut, meddelas vid behov av Säkerhetsskyddsavdelningen.	Krav enligt separat beslut, meddelas vid behov av Säkerhetsskydds-avdelningen.	Se kapitel 4

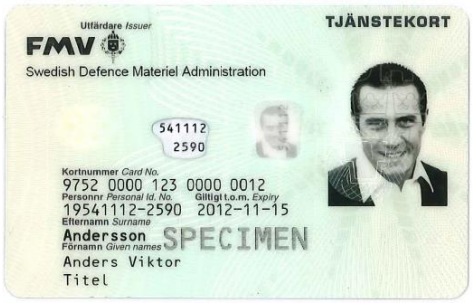
[1] Skyddsklass 2 uppfyller kraven motsvarande skyddsnivå 3 om omslutningsytan utförs i betong enligt fordringarna för SSF200 med armering max c/c 250 mm och armeringsjärn om minst 10 mm diameter. Övriga utföranden enligt skyddsklass 2 är ej godkända. Vidare krävs för skyddsnivå 3 att dörrar är certifierade i lägst klass 4 enligt SS-EN 1627.

Bilaga 3

Godkända id-handlingar

Vid FMV är nedan redovisade id-handlingar godkända:

- Pass (OBS provisoriskt pass är inte giltigt som id-handling)
- Nationellt id-kort utfärdat av land inom Schengen.
- Svenskt körkort
- Svenskt SIS-märkt id-kort
- Id-kort utfärdat av en svensk statlig myndighet, ex.v. Polisen eller Skatteverket



Bilaga 4

Godkända signalskydds- och kryptosystem

1 Allmänt

Signalskyddssystem som ingår i ett av FMV ackrediterat och godkänt IT-system behöver inget särskilt godkännande utan är godkänt att använda för att skydda sekretessbelagda uppgifter enligt aktuell ackreditering.

2 För säkerhetsskyddsklassifcierade uppgifter

Tabellen nedan redovisar de i FMV tillämpade säkerhetsskyddsklasserna samt de signalskyddsgrader, för av Försvarsmakten granskade och godkända signalskyddssystem, som lägst krävs för skydd av dessa uppgifter.

Säkerhetsskyddsklass för uppgifter	**Lägsta signalskyddsgrad**
Kvalificerat hemlig (KH).	TOP SECRET (SG TS)
Hemlig (H).	SECRET (SG S)
Konfidentiell (K).	CONFIDENTIAL (SG C)
Begränsat hemlig (BH).	RESTRICTED (SG R)

3 För uppgifter som omfattas av sekretess

Uppgifter som omfattas av sekretess, och som inte är säkerhetsskyddsklassificerade, får skyddas med nedan redovisade kryptosystem, under förutsättning att hanteringen sker i enlighet med respektive hanterings-instruktion.

- KSU-krypton
  - KURIR – filkrypto för datafiler
  - FÄRIST MOBILE – skyddat tal och text
- Microsoft BitLocker – hårddiskkrypto som är godkänt för SFAP
- Corsair Flash Padlock med aktiverad krypteringsfunktion
- Personaliserad SafeBoot – minne med fingeravtrycksläsare

I enskilda fall kan även annat kryptosystem godkännas.

Uppgifter som omfattas av sekretess kan även skyddas med signalskyddssystem enligt avsnitt 2 ovan.

Bilaga 5

Godkända förstöringsmetoder

1 Allmänt

FMV har beslutat att renodla och förenkla regelverket för förstöring av pappershandlingar, lagringsmedier och andra bärare av uppgifter som omfattas av sekretess, oavsett om dessa även är indelade i säkerhetsskyddsklass.

FMV tillämpar den tyska standarden DIN 66399 *Büro- und Datentechnik - Vernichten von Datenträgern* från 2012 (Förstöring av databärare). DIN 66399 består av tre huvudsakliga delar:

- Del 1 redogör för principer och definitioner
- Del 2 reglerar formella krav på förstörare (destruktörer)
- Del 3 reglerar processen för förstöring

2 Skyddsklasser

Standarden anger tre olika skyddsklasser, beroende på informationens känslighet. För FMV gäller i alla sammanhang den högsta klassen (3).

3 Databärare

Den tyska standarden DIN 66399 delar in de olika databärarna i sex typer:

Typ	**Omfattning**
P	Pappersbaserade produkter (*papper, foton, trycksaker*)
F	Filmbaserade produkter inklusive mikrofilm, mikrofiche, diabilder (*film, mikrofilm, folie*)
O	Optiska lagringsmedier, t. ex CD och DVD (*CD, DVD*)
T	Magnetiska datamedia, t. ex. disketter, ID-kort, magnetband och kassettband (*disketter, id-handlingar, magnetband, kassettband*)
H	Hårddiskar
E	Elektroniska datamedia, t. ex. USB-minnen, kort, SSD, mobiltelefoner (*USB-stickor, minneskort, halvledardisk, mobil eller smartphone*)

4 Förstöringsklasser

Den tyska standarden DIN 66399 anger sju olika förstöringsklasser, beroende på viken typ av media som skall förstöras.

För FMV gäller följande:

Medium	**Destruktionsklass enligt DIN 66399**	**Anmärkning**
Pappersbaserade produkter (P)	P-6	
Filmbaserade produkter (F)	F-6	
Optiska lagringsmedier (O)	O-6	
Magnetiska datamedia (T)	T-6	Destruktion skall föregås av avmagnetisering med degausser, minst *Single Pass Pulse*
Hårddiskar (H)	H-6	Destruktion skall föregås av avmagnetisering med degausser, minst *Single Pass Pulse*
Elektroniska datamedia (E)	E-5	

5 Övrigt

- Bränning får i yttersta nödfall användas som alternativ förstöringsmetod för destruktionsklasserna P, F, O och T.
- Vid destruktion av medier med säkerhetsskyddsklassificerade uppgifter ska restprodukten i möjligaste mån blandas med annat destruktionsmaterial av samma typ.

6 Tillämpning

FMV kommer successivt att byta ut befintlig utrustning för förstöring. I samband med upphandling av ny utrustning kommer krav enligt denna bilaga att tillämpas.

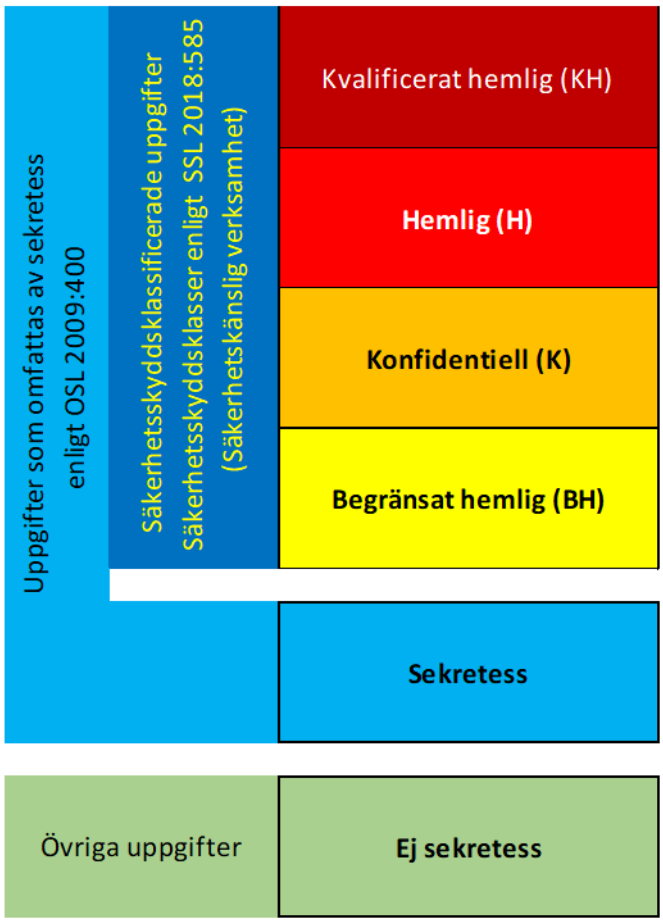
Bilaga 6

Anteckningar om sekretess respektive säkerhetsskyddsklass

Denna bilaga reglerar märkning av handlingar/lagringsmedier/materiel.

1 Informationsklassificering

FMV MODELL FÖR MÄRKNING AV UPPGIFTERS KONFIDENTIALITET



2 Anteckning på handling

I FMV hanteras såväl allmänna handlingar som övriga handlingar (arbetshandlingar etc.) enligt dessa principer.

Ett separat utdrag av denna bilaga i Word-format finns tillgänglig på Insidan och i VHL. I denna finns förekommande anteckningar tillgängliga som redigeringsbara grafiska objekt, att kopieras in i olika dokument. OBS att anteckningar avseende sekretess får förekomma i såväl SFAP som andra miljöer, medan anteckningar om säkerhetsskyddsklass inte får förekomma i SFAP, utan endast i andra miljöer (bl.a. SFAP-H, SFAP-X, H-LAN, CMS H/S).

2.1 Anteckning om sekretess

Om flera lagrum enligt OSL är aktuella ska dessa anges i var sin anteckning.

2.1.1 Första sidan

På första sidan i handlingen ska en anteckning om sekretess (sekretessmarkering) göras. Denna ska ha en rektangulär ram och om möjligt vara röd. Av anteckningen ska följande framgå:

1. tillämplig sekretessbestämmelse enligt OSL (referens till lagrum: X kap. Y §),
2. datum då anteckningen gjordes,
3. att det är FMV som har gjort anteckningen.

SEKRETESS
Enligt **X** kap. **Y** § offentlighets- och sekretesslagen (2009;400)

ÅÅÅÅ-MM-DD

Försvarets materielverk
Swedish Defence Materiel Administration

2.1.1.1 Synnerlig betydelse för rikets säkerhet

Ramen ska vara dubbel för en handling med uppgifter som är av ”synnerlig betydelse för rikets säkerhet” enligt OSL.

Utöver det som ingår enligt ovan ska det av anteckningen även framgå vilken myndighet som ska pröva frågan om utlämnande.

SEKRETESS
Synnerlig betydelse för rikets säkerhet

Enligt **X** kap. **Y** § offentlighets- och sekretesslagen (2009;400)

ÅÅÅÅ-MM-DD

Frågan om denna handlings utlämnande ska prövas av chefen för

☐ Justitiedepartementet (15 kap.2 § eller 18 kap. 1-3 §§ OSL avs. Polisen)

☐ Utrikesdepartementet (15 kap. 1 §)

☐ Försvarsdepartementet (15 kap. 2 § utöver Justitiedepartementet)

Försvarets materielverk
Swedish Defence Materiel Administration

Frågan om handlings utlämnande enligt ovan regleras i X kap. Y § OSF.

2.1.2 Övriga sidor

På övriga sidor i handlingen (andra till sista sidan) ska en förenklad anteckning finnas, som hänvisar till anteckningen på första sidan.

2.1.2.1 Synnerlig betydelse för rikets säkerhet

SEKRETESS
Synnerlig betydelse för rikets säkerhet
Se sid. 1

2.1.3 Bilagor

Bilagor ska hanteras på samma sätt som huvudhandling.

2.1.4 Missiv

Av missivet ska framgå, för varje bilaga, huruvida denna omfattas av sekretess eller ej. Dessutom ska missivet märkas med anteckning om förekommande sekretess.

Det förekommer att missiv i sig inte omfattas av sekretess, men att bilagor gör det. Det ska i så fall framgå att missivet i sig inte omfattas av sekretess.

2.2 Anteckning om säkerhetsskyddsklass

2.2.1 Första sidan

En anteckning om säkerhetskyddsklass på en handling ska redovisa den högsta säkerhetsskyddsklass som förekommer för uppgifterna i handlingen. Ramen ska vara rektangulär och om möjligt vara röd. Ramen ska vara dubbel för anteckning avseende uppgifter i säkerhetsskyddsklass Kvalificerat hemlig.

KVALIFICERAT HEMLIG
Enligt säkerhetsskyddslagen (2018:585)

HEMLIG
Enligt säkerhetsskyddslagen (2018:585)

KONFIDENTIELL
Enligt säkerhetsskyddslagen (2018:585)

BEGRÄNSAT HEMLIG
Enligt säkerhetsskyddslagen (2018:585)

2.2.2 Övriga sidor

På övriga sidor i handlingen (andra till sista sidan) ska en anteckning finnas, som

- hänvisar till anteckningen på första sidan, eller som
- anger den högsta säkerhetsskyddsklass som uppgifterna på den enskilda (aktuella) sidan är placerade i.

KVALIFICERAT HEMLIG
Se sid. 1

HEMLIG
Se sid. 1

KONFIDENTIELL
Se sid. 1

BEGRÄNSAT HEMLIG
Se sid. 1

För enskild sida (där den högst klassificerade uppgiften på sidan är lägre än klassificeringen för handlingen som helhet).

HEMLIG
Enligt säkerhetsskyddslagen (2018:585)
Avser endast denna sida

KONFIDENTIELL
Enligt säkerhetsskyddslagen (2018:585)
Avser endast denna sida

BEGRÄNSAT HEMLIG
Enligt säkerhetsskyddslagen (2018:585)
Avser endast denna sida

2.2.3 Bilagor

Bilagor ska hanteras på samma sätt som huvudhandling.

2.2.4 Missiv

Av missivet ska framgå, för varje bilaga, den högsta säkerhetsskyddsklassen för de uppgifter som förekommer i bilagan. Dessutom ska missivet märkas med den högsta säkerhetsskyddsklassen för de uppgifter som förekommer.

Det förekommer att missiv i sig inte innehåller säkerhetsskyddsklassificerade uppgifter, men att bilagor gör det. Det ska i så fall framgå att missivet i sig inte innehåller säkerhetsskyddsklassificerade uppgifter.

3 Materiel och lagringsmedier med eller avsedd för hantering av sekretessbelagda eller säkerhetsskyddsklassificerade uppgifter

Lagringsmedium/materiel ska om möjligt märkas i tillämplig omfattning enligt samma principer som för handling (avsnitt 1).

Lagringsmedium/materiel, där uppgifterna är krypterade med av Säkerhetsskyddsavdelningen för ändamålet godkänd kryptering, behöver inte märkas.

Registrering ska ske enligt avsnitt 10.2.2.3 i TjF.

Bilaga 7

Skyddad transport - Transportnivåer

1 Allmänt

Med skyddad transport avses i denna TjF en sådan transport av säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig/skyddsvärd materiel (såsom t.ex. skjutvapen eller ammunition) där ett särskilt skydd erfordras enligt den säkerhetsanalys som skall göras innan varje enskilt transporttillfälle.

Följande faktorer skall beaktas vid framtagning av säkerhetsanalys och val av transportnivå:

- mängd och omfattning av den transporterade informationen
- materielslag
- materielens betydelse för Sveriges säkerhet
- materielens värde
- materielens organisatoriska betydelse för myndigheten
- möjlighet att återanskaffa skadad, stulen eller försvunnen materiel och
- för den hotbild som bedöms för materielen

Krav på vilka transportnivåer som krävs för att skydda handlingar eller övrig säkerhetskänslig/ skyddsvärd materiel kan ibland finnas i centrala beslut eller för materielen särskilt framtagna förteckningar eller bestämmelser. Chefen för verksamhetsområdet som avsänder godset är ansvarig för att transportsäkerhetsanalys samt plan upprättas innan transport. Analys och plan ska dokumenteras.

I beskrivningen av de olika transportnivåerna används begrepp såsom *ringa mängd, mindre mängd, större mängd* och *mycket stora mängder* för att ange mängden handlingar med säkerhetsskyddsklassificerade uppgifter eller mängden säkerhetskänslig/skyddsvärd materiel. Exemplen nedan visar hur man kan göra bedömningar avseende vilken transportnivå som bör väljas, beroende på vilken säkerhetsskyddsklassificering berörda uppgifter eller vilket skyddsvärde den aktuella materielen har.

Vid skyddade transporter ska företag med säkerhetsskyddsavtal användas. Vid transport i nivå 4 ska företag som är auktoriserat värdetransportföretag användas.

En skyddad transport som genomförs som järnvägs-, flyg-, eller sjötransport kan, av praktiska skäl, inte alltid ske på samma sätt som om transporten genomförs som marktransport. Åtgärder skall dock vidtas så att transporten genomförs på ett sådant sätt att skyddsnivån, från säkerhetssynpunkt, motsvarar aktuell transportnivå.

Krav på transportsäkerhetsanalys och fastställande av transportnivå gäller inte i fråga om personligen utkvitterade hemliga handlingar som någon medför i sin tjänsteutövning.

4 Transportnivåer

4.1 Tillämpning av transportnivåer

Transportnivå 1	Gäller för transport av - handlingar med uppgifter i säkerhetsskyddsklassen Begränsat hemlig, samt för - en ringa mängd säkerhetskänslig/skyddsvärd materiel.
Transportnivå 2	Gäller för transport av - en mindre mängd handlingar med uppgifter i säkerhetsskyddsklassen Konfidentiell eller Hemlig, samt för - en mindre mängd säkerhetskänslig/skyddsvärd materiel.
Transportnivå 3	Gäller för transport av - en mindre mängd hemliga handlingar som är placerade i säkerhetsskyddsklassen Kvalificerat hemlig, eller - en större mängd hemliga handlingar som är placerade i säkerhetsskyddsklassen Konfidentiell eller Hemlig, samt för - en större mängd säkerhetskänslig/skyddsvärd materiel.
Transportnivå 4	Gäller för transport av - en större mängd hemliga handlingar som är placerade i säkerhetsskyddsklassen Kvalificerat hemlig, eller - mycket stora mängder hemliga handlingar som är placerade i säkerhetsskyddsklassen Konfidentiell eller Hemlig, samt för - mycket stora mängder säkerhetskänslig/skyddsvärd materiel.

4.2 Krav för respektive transportnivå

4.2.1 Allmänt

4.2.1.1 Personsäkerhetslarm - definition

Ett handburet eller fordonsmonterat larm som vid manuell aktivering skickar larm och positionsangivelse till en extern larmmottagningscentral. Vid utlöst larm ska larmmottagningscentralen ha möjlighet att spåra transporten och kunna avlyssna ljud.

4.2.1.2 Anmälan

Anmälan ska göras för transporter i transportnivå 3 och 4. Se TjF avsnitt 8.3.4.11.4.

4.2.2 Transportnivå 1

Transporten ska

- utföras med fordon vars transportutrymme ska vara låst och skyddat mot insyn.
    - Om möjligt ska det skyddsvärda godset förvaras i låst och plomberat transportemballage.

4.2.3 Transportnivå 2

Transporten ska

- uppfylla krav enligt Transportnivå 1 ovan, samt vara
- försett med personsäkerhetslarm, eller vara
- åtföljt av följebil.

4.2.4 Transportnivå 3

Transporten ska

- uppfylla krav enligt Transportnivå 2 ovan, med tillägget att
- transportutrymmet ska utgöras av en låst förvaringsenhet enligt SSF 3492 (eller ett annat transportutrymme av motsvarande standard, t.ex. standardcontainer enligt ISO 668:2013 låst med hänglås av lägst klass 4 enligt SSF 3522), samt
- köras utan avbrott från start till mål, eller
- parkeras inom bevakat område vid avbrott i körningen.

4.2.5 Transportnivå 4

Krav enligt separat beslut, meddelas vid behov av Säkerhetsskyddsavdelningen.