FÖRSVARSMAKTEN
HÖGKVARTERET

FÖRSVARETS FÖRFATTNINGSSAMLING

FM LOG/TF-redaktionen
107 86 STOCKHOLM

ISSN 0347-7576

FFS 2003:7
Utkom från
trycket
2003-11-10

Försvarsmaktens föreskrifter om säkerhetsskydd;

beslutade den 20 oktober 2003.

Försvarsmakten föreskriver med stöd av 11 § andra stycket och 44 § säkerhetsskyddsförordningen (1996:633) följande.

1 kap. Allmänna bestämmelser

1 § Dessa föreskrifter gäller för Fortifikationsverket samt Försvarsmakten och övriga myndigheter som hör till Försvarsdepartementet utom Kustbevakningen, Krisberedskapsmyndigheten, Statens räddningsverk och Styrelsen för psykologiskt försvar.

2 § I dessa föreskrifter avses med hemlig uppgift, hemlig handling och säkerhetskänslig verksamhet detsamma som anges i 4 § säkerhetsskyddsförordningen (1996:633).

3 § Vad som föreskrivs om hemlig handling gäller även en handling som är av synnerlig betydelse för rikets säkerhet, kvalificerat hemlig handling, om inte annat särskilt anges.

4 § Säkerhetsskyddet indelas i dessa föreskrifter i fyra informationssäkerhetsklasser med följande beteckningar och betydelser.

Informationssäkerhetsklass	Betydelse
HEMLIG/ TOP SECRET	1. Hemliga uppgifter vars röjande kan medföra synnerligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet (kvalificerat hemliga uppgifter). 2. Hemlig handling som har åsatts beteckningen TOP SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.
HEMLIG/ SECRET	1. Hemliga uppgifter vars röjande kan medföra betydande men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.
HEMLIG/ CONFIDENTIAL	1. Hemliga uppgifter vars röjande kan medföra ett inte obetydligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen CONFIDENTIAL eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.
HEMLIG/ RESTRICTED	1. Hemliga uppgifter vars röjande kan medföra endast ringa men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen

RESTRICTED eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.

5 § Beteckningen HEMLIG/TOP SECRET i 4 § i detta kapitel anger en högre informationssäkerhetsklass än beteckningen HEMLIG/SECRET. Beteckningen HEMLIG/SECRET anger en högre informationssäkerhetsklass än beteckningen HEMLIG/CONFIDENTIAL och beteckningen HEMLIG/CONFIDENTIAL anger en högre informationssäkerhetsklass än beteckningen HEMLIG/RESTRICTED.

6 § Varje myndighet skall genomföra och dokumentera analyser avseende vilka hot, risker och sårbarheter som kan påverka myndighetens säkerhetskänsliga verksamhet och utifrån analyserna vidta lämpliga säkerhetsskyddsåtgärder.

7 § Materiel som innehåller hemliga uppgifter skall ges ett säkerhetsskydd som motsvarar vad som gäller för hemliga handlingar.

8 § Sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse skall snarast åtgärdas och anmälas till Försvarsmaktens högkvarter.

9 § För signalskyddstjänsten gäller särskilda bestämmelser i fråga om hantering av kryptonycklar och signalskyddsmateriel samt användning av kryptografiska funktioner.

2 kap. Informationssäkerhet

Hemligstämpel m.m.

1 § En allmän handling som är hemlig skall på första sidan förses med en särskild anteckning (hemligstämpel). Bestämmelser om hemligstämpling finns i 15 kap. 3 § sekretesslagen (1980:100).

Hemligstämpeln på den allmänna handlingen skall ha en rektangulär ram. Ramen skall vara enkel för hemlig handling och dubbel för kvalificerat hemlig handling.

En hemlig handling som inte är allmän skall på första sidan förses med en anteckning om att den är hemlig. Anteckningen får utformas på lämpligt sätt.

2 § En hemlig handling skall placeras i en av de informationssäkerhetsklasser som anges i 1 kap. 4 §. Handlingen skall på första sidan förses med en uppgift om i vilken informationssäkerhetsklass den har placerats.

3 § Om en hemlig handling består av flera sidor skall på varje sida finnas en hänvisning till uppgiften om informationssäkerhetsklass på första sidan.

4 § Om en handling som är försedd med hemligstämpel inte längre bedöms vara hemlig skall beslut om detta antecknas på handlingen. Anteckningen skall innehålla myndighetens namn, datum för beslutet samt vem som har fattat beslutet. Därefter skall hemligstämpeln överkorsas och anteckning om beslutet göras i det register där handlingen är diarieförd.

Om en handling, som har försetts med den hemligstämpel som gäller för en kvalificerat hemlig handling, inte längre bedöms som kvalificerat hemlig skall samråd ske med den som har upprättat handlingen innan åtgärder vidtas enligt första stycket. Anteckning om samrådet skall göras på handlingen.

Om en handling som är försedd med anteckning som avses i 1 § tredje stycket i detta kapitel inte längre bedöms vara hemlig, skall anteckningen överkorsas. På handlingen skall vidare anges vem som har beslutat överkorsningen.

5 § Om en hemlig handling placeras i en annan informationssäkerhetsklass än vad som anges på handlingen skall detta antecknas på handlingen. Anteckningen skall innehålla den nya informationssäkerhetsklassen, myndighetens namn, datum för beslutet samt vem som har fattat beslutet.

Om en handling inte längre skall vara placerad i en informationssäkerhetsklass skall anteckningen om informationssäkerhetsklass överkorsas.

Behörighet att ta del av hemliga uppgifter

6 § Varje myndighet skall besluta vem som är behörig att ta befattning med hemliga handlingar som är placerade i någon av informationssäkerhetsklasserna HEMLIG/CONFIDENTIAL, HEMLIG/SECRET respektive HEMLIG/TOP SECRET eller som på annat sätt får ta del av en hemlig uppgift. Ett sådant beslut skall dokumenteras.

Arbetsrutiner med hemlig handling

7 § Är en allmän handling som är hemlig placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall det på sändlistan till handlingen eller i det register där handlingen är diarieförd anges hur många exemplar av handlingen som har framställts och vilka som är mottagare av respektive exemplar.

8 § Vid framställning av en allmän handling som är hemlig och som är placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall på första sidan antecknas handlingens beteckning, exemplarnummer, antal sidor samt bilagor, om sådana följer med. Sidorna skall numreras i följd.

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

9 § Varje myndighet skall besluta vilka rutiner som skall tillämpas i samband med kopiering av eller utdrag ur en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre. Beslutet skall dokumenteras.

Kopia av eller utdrag ur en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET får göras endast efter medgivande av myndighetens chef eller den han bestämmer.

10 § Har en kopia av eller ett utdrag ur en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre gjorts, skall uppgift om detta liksom uppgift om till vem kopian eller utdraget har lämnats antecknas i register eller liggare.

Om det inte framgår av ett utdrag ur en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre till vilken handling utdraget hör, skall det på utdraget antecknas från vilken handling utdraget har gjorts.

Kvittering

11 § När en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET tas emot skall mottagandet kvitteras med namnteckning och namnförtydligande. Kvittensen skall bevaras hos myndigheten i minst 10 år.

När en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET tas emot skall mottagandet kvitteras med namnteckning och namnförtydligande på ett särskilt kvitto med kopia. När en sådan handling återlämnas skall detta antecknas på kvittokopian, som skall bevaras hos myndigheten i minst 25 år.

Vad som föreskrivs i första och andra styckena gäller dock inte när arkiv- eller expeditionspersonal tar emot en sådan hemlig handling för registrering, kopiering, arkivering eller förstöring, om inte den som lämnar över handlingen begär det.

12 § Varje myndighet skall besluta hur kvittering skall göras om uppgifter i en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET lämnas muntligt eller genom visning.

Förvaring

13 § Ett förvaringsutrymme för hemliga handlingar skall uppfylla de krav som gäller för skyddsnivå 1, 2, 3 eller 4. I *bilaga* till dessa föreskrifter anges de krav som gäller för respektive skyddsnivå.

14 § En hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/RESTRICTED skall förvaras inlåst eller i en lokal som endast den som är behörig att ta del av handlingen har tillträde till. Förvaringsutrymmet skall uppfylla de krav som gäller för skyddsnivå 1.

15 § En hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET skall förvaras i ett förvaringsutrymme som uppfyller de krav som gäller för skyddsnivå 3.

16 § En hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET skall förvaras i ett förvaringsutrymme som uppfyller de krav som gäller för skyddsnivå 4.

17 § Varje myndighet får fatta beslut som avviker från föreskrifterna i 14-16 §§ i detta kapitel under förutsättning att motsvarande skyddsnivå kan upprätthållas. Ett sådant beslut skall dokumenteras.

18 § Om en myndighet har beslutat att anställda under kortare tid får lämna hemliga handlingar framme i ett låst arbetsrum, skall huvudnycklar och reservnycklar förvaras så att inte någon obehörig kan komma åt dem.

19 § I det register där en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre är diarieförd skall anges vem som förvarar handlingen eller om handlingen har förkommit eller gallrats.

Medförande av hemliga handlingar utanför myndighetens lokaler

20 § Varje myndighet skall besluta i vilken omfattning hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre får medföras från myndighetens lokaler. Ett sådant beslut skall dokumenteras.

Hemliga handlingar som medförs från myndigheten skall hållas under omedelbar uppsikt eller förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av handlingarna inom myndighetens lokaler.

Inventering

21 § Inventering av allmänna handlingar som är hemliga och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET liksom inventering av hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET skall protokollföras.

Förstöring av hemlig handling

22 § Förstöring av hemliga handlingar eller av materiel som innehåller hemliga uppgifter skall ske så att åtkomst och återskapande av uppgifterna omöjliggörs.

Förstöring av sådana hemliga handlingar och sådan materiel som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall dokumenteras utom såvitt avser karbonpapper, karbonband och färgband.

23 § För gallring av hemliga handlingar gäller särskilda bestämmelser som meddelas av Riksarkivet.

Åtgärder vid distribution av hemlig handling

24 § Varje myndighet skall besluta hur försändelser med hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall sändas från och tas emot av myndigheten. Myndigheten skall se till att erforderliga skyddsåtgärder vidtas under distributionen.

En försändelse med hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall sändas med en distributör som har godkänts av myndigheten.

25 § I 11 § första stycket säkerhetsskyddsförordningen (1996:633) finns föreskrifter om försändelser med hemliga handlingar till utlandet.

Hemliga handlingar som sänds utomlands skall förses med anteckning om uppgifternas ursprungsland.

Varje myndighet får i avtal med ett annat land eller mellanfolklig organisation komma överens om att distribuera hemliga handlingar på annat sätt än vad som föreskrivs i 11 § första stycket säkerhetsskyddsförordningen (1996:633).

3 kap. Tillträdesbegränsning

Tillträde och bevakning

1 § Varje myndighet skall besluta om tillträdesrätt till myndighetens objekt, lokaler och områden. Beslutet skall dokumenteras.

2 § Den myndighet som medger en person tillträde till myndighetens objekt, lokaler eller områden där det bedrivs verksamhet som kräver säkerhetsskydd skall se till att personen genom besökstillstånd eller på annat sätt har fått myndighetens tillstånd till tillträde och att personen har styrkt sin identitet. Vid myndigheten skall för varje besökare antecknas dennes namn, den myndighet eller organisation (motsv.) som besökaren företräder och dagen för besöket. Sådana anteckningar skall bevaras i minst 10 år.

Första stycket skall dock tillämpas med beaktande av allmänhetens rätt att utan att uppge identitet ta del av allmänna handlingar.

3 § Bevakning med personal eller med teknisk utrustning eller med båda skall finnas vid alla passerställen till platser där det bedrivs verksamhet som kräver säkerhetsskydd.

Nycklar, kort och koder

4 § Nycklar, kort och koder till utrymmen där hemliga uppgifter finns eller där säkerhetskänslig verksamhet bedrivs skall förvaras så att inte någon obehörig kan komma åt dem.

5 § En kod skall bestämmas och ställas in av den som har tilldelats ett förvaringsutrymme.

6 § En nyckel, ett kort eller en kod får innehas endast av den som har ansvaret för förvaringsutrymmet, om inte myndigheten har beslutat annat. Ett sådant beslut skall dokumenteras.

7 § Det skall finnas en förteckning över samtliga nycklar, kort och koder till förvaringsutrymmen som rymmer hemliga handlingar. Av förteckningen skall framgå till vem och när en nyckel, ett kort eller en kod har lämnats samt var reservnyckel, reservkort eller reservkod förvaras.

8 § 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, skall förhållandet omedelbart anmälas till myndighetens säkerhetsskyddschef eller till den han bestämmer.

Skyddsnivåer för vissa utrymmen

9 § Utrymmen som innehåller växlar, korskopplingar och servrar samt datorhallar skall uppfylla de krav som gäller för skyddsnivå 2, 3 eller 4. I *bilaga* till dessa föreskrifter anges de krav som gäller för respektive skyddsnivå.

10 § Om det i sådana utrymmen som anges i 9 § i detta kapitel behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/RESTRICTED skall utrymmena uppfylla de krav som gäller för skyddsnivå 2.

Om det i sådana utrymmen behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET skall utrymmena uppfylla de krav som gäller för skyddsnivå 3.

Om det i sådana utrymmen behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/TOP SECRET skall utrymmena uppfylla de krav som gäller för skyddsnivå 4.

11 § Utrymmen som anges i 9 § i detta kapitel skall vara försedda med system för inpasseringskontroll.

12 § Varje myndighet får fatta beslut som avviker från föreskrifterna i 10 § i detta kapitel under förutsättning att motsvarande säkerhetsskyddsnivå kan upprätthållas. Ett sådant beslut skall dokumenteras.

4 kap. Säkerhetsprövning

1 § Varje myndighet skall analysera vilka anställningar vid myndigheten som skall placeras i säkerhetsklass och vilket annat deltagande i myndighetens verksamhet som kan komma att placeras i säkerhetsklass. Resultatet av analysen skall dokumenteras. Av dokumentationen skall även framgå vem som skall bli föremål för registerkontroll till skydd mot terrorism.

2 § Varje myndighet skall fortlöpande pröva pålitligheten från säkerhetssynpunkt särskilt i fråga om de personer som har anställning eller deltar i verksamhet som är placerad i säkerhetsklass eller som är registerkontrollerade till skydd mot terrorism. Vid denna prövning skall särskild vikt läggas vid de personliga förhållandena.

5 kap. Utbildning

1 § Vid varje myndighet skall det finnas en plan för utbildning i säkerhetsskydd.

2 § Varje myndighet skall föra en förteckning över de anställda som har genomgått utbildning i säkerhetsskydd.

6 kap. Kontroll

1 § Vid varje myndighet skall det finnas en plan för intern kontrollverksamhet. Myndigheten skall föra protokoll över varje kontroll. Protokollen skall förvaras samlade hos myndigheten.

7 kap. Hantering av hemliga uppgifter i IT-system

Definitioner

1 § I detta kapitel avses med

1. *lagringsmedium:* permanent minnesmedium som används för att kunna lagra och läsa uppgifter,
2. *IT-system:* system med teknik som hanterar och utbyter information med omgivningen,
3. *behörighetskontroll:* administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att kontrollera en användares identitet, styra en användares behörighet att använda IT-systemet och dess resurser samt registrera användaren,

4. *säkerhetsfunktion:* en eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet skall skyddas,

5. *säkerhetsloggning:* manuell eller automatisk registrering, eller både manuell och automatisk registrering, av händelser som är av betydelse för säkerheten i eller kring ett IT-system,

6. *röjande signaler:* inte önskvärda elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs,

7. *intrångsskydd*: administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att skydda IT-system mot obehörig åtkomst från ett elektroniskt kommunikationsnät,

8. *intrångsdetektering:* administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att detektera intrång, eller försök till intrång eller förberedelse till intrång,

9. *skadlig kod:* otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett IT-system, och

10. *ackreditering:* ett sådant godkännande av ett IT-system från säkerhetssynpunkt som avses i 12 § tredje stycket säkerhetsskyddsförordningen (1996:633).

Hantering av hemliga uppgifter och lagringsmedium

2 § En hemlig uppgift i ett IT-system skall ha ett säkerhetsskydd som motsvarar det säkerhetsskydd som gäller för den informationssäkerhetsklass som uppgiften har placerats i.

3 § Ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter skall ha ett säkerhetsskydd som motsvarar det säkerhetsskydd som gäller för den informationssäkerhetsklass som lagringsmediet har placerats i.

4 § Ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter får endast hanteras i ett IT-system som uppfyller de krav som gäller för

hantering av uppgifter i den högsta informationssäkerhetsklass som någon av uppgifterna på lagringsmediet kan komma att placeras i eller har placerats i.

5 § Ett lagringsmedium som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/SECRET eller HEMLIG/TOP SECRET får inte återanvändas i ett IT-system som är avsett för behandling av hemliga uppgifter som är placerade i en lägre informationssäkerhetsklass.

6 § Ett lagringsmedium som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/RESTRICTED eller HEMLIG/CONFIDENTIAL får återanvändas om myndigheten har vidtagit åtgärder för att säkerställa att inga hemliga uppgifter längre kan utläsas ur lagringsmediet. Sådana åtgärder skall dokumenteras.

Utveckling, anskaffning, användning och avveckling

7 § Varje myndighet som överväger att införa eller använda ett IT-system som skall användas av flera personer skall noga analysera vilket säkerhetsskydd systemet kräver och vilka åtgärder som måste vidtas för att säkerhetsskyddet skall få avsedd effekt. En sådan analys skall även göras innan en myndighet upplåter ett IT-system till en annan myndighet, ett annat land eller en mellanfolklig organisation.

Analyser som avses i första stycket skall dokumenteras.

8 § Varje myndighet som beslutar att anskaffa eller förändra ett IT-system skall, för att kunna fastställa erforderligt säkerhetsskydd för systemet, göra en sekretessbedömning av såväl de enskilda uppgifterna som den totala informationsmängden som avses hanteras i IT-systemet.

9 § Varje myndighet skall dokumentera det säkerhetsskydd som finns i fråga om ett IT-system, från dess utveckling till dess avveckling. Dokumentationen skall hållas aktuell.

Behörighetskontroll

10 § Varje IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer skall vara försett med en av myndigheten godkänd säkerhetsfunktion för behörighetskontroll. En sådan säkerhetsfunktion skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

Säkerhetsloggning

11 § Varje IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer skall vara försett med en av myndigheten godkänd säkerhetsfunktion för säkerhetsloggning. En sådan säkerhetsfunktion skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

12 § Varje myndighet skall besluta vilket säkerhetsskydd som är erforderligt vad avser förvaring av säkerhetskopierade säkerhetsloggar.

Röjande signaler och obehörig avlyssning

13 § Varje IT-system som är avsett för behandling av hemliga uppgifter skall vara försett med av myndigheten godkända säkerhetsfunktioner för skydd mot röjande signaler och obehörig avlyssning. Sådana säkerhetsfunktioner skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

IT-system som är avsedda för behandling av uppgifter som har placerats i högst informationssäkerhetsklassen HEMLIG/RESTRICTED behöver dock inte förses med en säkerhetsfunktion för skydd mot röjande signaler.

Intrångsskydd och intrångsdetektering

14 § Varje IT-system som är avsett för behandling av hemliga uppgifter skall vara försett med av myndigheten godkända säkerhetsfunktioner som skyddar mot intrång och som möjliggör intrångsdetektering. Sådana säkerhetsfunktioner skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

IT-system som är avsedda för behandling av uppgifter som har placerats i högst informationssäkerhetsklassen HEMLIG/RESTRICTED behöver dock inte förses med en säkerhetsfunktion som möjliggör intrångsdetektering.

Skadlig kod

15 § Varje IT-system som är avsett för behandling av hemliga uppgifter skall vara försett med en av myndigheten godkänd säkerhetsfunktion som skyddar mot skadlig kod. En sådan säkerhetsfunktion skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

Ackreditering

16 § Varje myndighet skall inför en ackreditering granska säkerheten i och kring ett IT-system och därvid särskilt beakta hur IT-systemet är avsett att samverka med andra IT-system. En sådan säkerhetsgranskning skall dokumenteras.

17 § Beslut om ackreditering skall dokumenteras.

8 kap. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal

1 § Med företag förstås i detta kapitel aktiebolag, handelsbolag, föreningar och andra juridiska personer samt enskilda firmor med vilka en myndighet avser att träffa avtal som avses i 8 § säkerhetsskyddslagen (1996:627).

2 § Varje myndighet skall innan en upphandling påbörjas pröva om uppdraget helt eller delvis skall säkerhetsskyddas.

3 § Innan en myndighet lämnar ut hemliga uppgifter till ett företag skall myndigheten göra en bedömning av vilka personer i företaget som skall placeras i säkerhetsklass. Bedömningen skall omfatta företagets styrelse, ledning och övriga anställda.

4 § Om företaget skall hantera eller förvara hemliga uppgifter i egna lokaler skall myndigheten, om detta inte genom egen eller annan myndighets dokumentation är uppenbart obehövligt, genom ett besök kontrollera att företagets lokaler och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt.

5 § Om företaget skall hantera eller förvara hemliga uppgifter utanför myndighetens lokaler, skall det av säkerhetsskyddsavtalet framgå att företaget skall upprätta en säkerhetsskyddsinstruktion som skall granskas och godkännas av myndigheten.

6 § När företaget har fullgjort ett uppdrag som krävt säkerhetsskydd skall myndigheten säga upp säkerhetsskyddsavtalet. Myndigheten skall säkerställa att vad som har avtalats om tystnadsplikt och sekretess i övrigt skall bestå.

7 § Varje myndighet skall utan dröjsmål underrätta Säkerhetspolisen om säkerhetsskyddsavtal som har träffats och om säkerhetsskyddsavtal som har upphört att gälla.

En sådan underrättelse skall lämnas på en blankett som har fastställts av Säkerhetspolisen.

9 kap. Internationell verksamhet

1 § I Försvarsmaktens föreskrifter (FFS 2001:6) om säkerhetsskydd vid visst försvarsmaterielsamarbete finns bestämmelser om säkerhetsskydd för sådan in-

formation som i ramavtalet den 27 juli 2000 mellan Frankrike, Italien, Spanien, Storbritannien, Sverige och Tyskland om åtgärder för att underlätta omstrukturering och drift av den europeiska försvarsindustrin benämns sekretessbelagd information.

2 § Om det i ett avtal för visst internationellt samarbete förekommer bestämmelser om säkerhetsskydd som avviker från föreskrifterna i denna författning skall bestämmelserna i avtalet ha företräde.

10 kap. Undantag

1 § Försvarsmakten får medge undantag från föreskrifterna i denna författning.

Överbefälhavaren eller den han bestämmer fattar beslut i ärenden om undantag.

Ikraftträdande- och övergångsbestämmelser

1. Denna författning träder i kraft den 1 januari 2004.

2. Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 1999:10) om säkerhetsskydd.

3. Föreskrifterna i 3 kap. 9-12 §§ i den nya författningen skall inte börja tillämpas förrän den 1 januari 2007.

4. Föreskrifterna i 2 kap. 2 och 3 §§ i den nya författningen gäller inte handlingar som har tillkommit före ikraftträdandet av den nya författningen *(äldre handlingar)*. Föreskrifterna får dock tillämpas i fråga om äldre handlingar.

Vad som föreskrivs i första stycket första meningen gäller dock inte kopior av eller utdrag ur äldre handlingar, om kopiorna eller utdragen har framställts efter ikraftträdandet av den nya författningen.

5. Äldre handlingar som inte har placerats i en informationssäkerhetsklass enligt den nya författningen skall hanteras enligt följande. Har en handling försetts med en särskild anteckning (hemligstämpel) om att den är

a) KVALIFICERAT HEMLIG, skall den anses vara placerad i informationssäkerhetsklassen HEMLIG/TOP SECRET, eller

b) HEMLIG, skall den anses vara placerad i informationssäkerhetsklassen HEMLIG/SECRET.

6. Har myndigheten före ikraftträdandet av den nya författningen beslutat

a) vem som är behörig att ta befattning med hemliga respektive kvalificerat hemliga handlingar, skall beslutet anses som ett beslut enligt 2 kap. 6 § i den nya författningen,

b) hur kvittering skall göras i fråga om kvalificerat hemliga uppgifter som har lämnats muntligt eller genom visning, skall beslutet anses som ett beslut enligt 2 kap. 12 § i den nya författningen,

c) i vilken omfattning hemliga respektive kvalificerat hemliga handlingar får medföras från myndighetens lokaler, skall beslutet anses som ett beslut enligt 2 kap. 20 § i den nya författningen,

d) hur försändelser med hemliga respektive kvalificerat hemliga handlingar skall sändas från och tas emot av myndigheten, skall beslutet anses som ett beslut enligt 2 kap. 24 § första stycket i den nya författningen, eller

e) godkänna en distributör av hemliga respektive kvalificerat hemliga handlingar, skall godkännandet anses som ett godkännande enligt 2 kap. 24 § andra stycket i den nya författningen.

Har myndigheten fattat ett eller flera beslut som avses i första stycket beträffande hemliga handlingar gäller respektive beslut även handlingar som enligt den nya författningen har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL.

7. Har ett beslut om ackreditering fattats före ikraftträdandet av den nya författningen gäller inte föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen.

Skall ett IT-system, på grund av förändringar som kan påverka säkerheten i det, på nytt ackrediteras enligt vad som följer av 12 § tredje stycket säkerhets-

skyddsförordningen (1996:633) skall dock föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen tillämpas.

8. Har ett underlag för ackreditering tagits fram före ikraftträdandet av den nya författningen gäller inte föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen i fråga om detta underlag.

Johan Hederstedt

Stefan Ryding-Berg

Bilaga

Utrymmens indelning i skyddsnivåer

Skyddsnivå 1	Byggnad eller lokal med certifierad dörr i klass 1 enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 81 73 45 eller standarddörrar i trä eller plåt. Väggar, golv och tak skall bestå av trämaterial, gipsskivor eller korrugerad plåt. Flyttbara förvaringsutrymmen med omslutningsytor av tunn plåt eller träkonstruktion.
Skyddsnivå 2	Byggnad eller lokal med certifierad dörr i lägst klass 2 enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 81 73 45, branddörr i plåt, arkivdörr eller D-dörr. Väggar, golv och tak skall bestå av betong med 75 mm, sten med 120 mm eller lättbetong med 150 mm tjocklek eller en stark träkonstruktion. Fönster enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 22 44 25 i lägst klass B 3 eller galler certifierade enligt Sveriges Försäkringsförbunds normer för galler i gallerklass 3. Omslutningsytorna får bestå av annat material med motsvarande motståndskraft. Flyttbara förvaringsutrymmen såsom vapenkista med beteckning 1-3 eller sprängämneskista.
Skyddsnivå 3	Byggnad eller lokal med certifierad dörr i klass 3 eller 4 enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 81 73 45, splitterskyddad dörr av stål, förstärkt D-dörr (D+), stötvågsdörr och lucka eller gastät ståldörr och lucka med minst 30 mm tjocklek.

Väggar, golv och tak skall bestå av armerad betong med en tjocklek av minst 100 mm. Armeringen får inte medge genomkrypning. Armeringen skall vara minst 10 mm i diameter och avståndet från centrum till centrum mellan armeringsstålen får vara högst 250 mm. Fönster enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 22 44 25 i lägst klass B 3 eller galler certifierade enligt Sveriges Försäkringsförbunds normer för galler i gallerklass 3. Omslutningsytorna får bestå av annat material med motsvarande motståndskraft.

Ammunitionsbox som är fast monterad i truppserviceförråd samt flyttbara förvaringsutrymmen såsom värdeskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 3150 och med lägre än 100 skyddsvärdespoäng, säkerhetsskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 3492, Svensk Standard (SS-EN) 1143-1, grade 0-II, kassaskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 3493, vapenkista med beteckning 1 B, 2 B, 3 B eller 1 TP, vapenkassun som inte är förankrad på bottenplatta eller motsvarande underlag eller tillträdesskyddad container.

Skyddsnivå 4

Byggnad eller lokal med valvdörr, vapenkassundörr, AD-dörr, VDS-dörr, TD-dörr eller VDB-dörr. Väggar, golv och tak skall bestå av betong med dubbel, förskjuten armering med en tjocklek av minst 180 mm. Armeringen får inte medge genomkrypning. Armeringen skall vara minst 12 mm i diameter och avståndet från centrum till centrum mellan armeringsstålen får vara högst 180 mm. Förskjutning av armering krävs inte vid högst 130 mm avstånd från centrum till centrum mellan armeringsstålen.

Väggar, golv, tak och dörrar får bestå av annat material med motsvarande motståndskraft. Byggnad eller lokal får inte ha fönster.

Flyttbara förvaringsutrymmen såsom värdeskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 3150 med minst 100 skyddsvärdespoäng, svensk Standard (SS-EN) 1143-1 lägst grade III, säkerhetsbox med beteckning 301 eller 302 samt vapenkassun som är förankrad på bottenplatta eller motsvarande underlag.