Säkerhetspolisen

SÄKERHETSSKYDD

– en vägledning

PRODUKTION: Säkerhetspolisen, maj 2008. Reviderad juli 2010
GRAFISK FORMGIVNING: Jerhammar & Co Reklambyrå AB
TYPOGRAFI: Eurostile och Swift

Förord

Detta är Säkerhetspolisens vägledning till säkerhetsskydd, uppdaterad i januari 2010. Vägledningen är placerad på Säkerhetspolisens webbplats för att den ska finnas lättillgänglig för användaren och underlätta fortlöpande uppdatering.

För att skapa ett väl anpassat säkerhetsskydd krävs att en säkerhetsanalys pekar ut de skyddsvärda områdena i verksamheten. Därefter bedöms behoven av tillträdesbegränsning, informationssäkerhet och säkerhetsprövning av personal. Kontinuerlig utbildning av personalen och kontroll av den egna verksamheten är förutsättningar för att säkerhetsskyddsarbetet ska bli framgångsrikt.

Det är vår bedömning att säkerhetsanalysarbetet blir allt viktigare. I takt med att de ekonomiska ramarna blir stramare är det angeläget att de satsningar som görs på skydd verkligen träffar de allra mest skyddsvärda tillgångarna, där de tyngsta behoven finns. Att utveckla säkerhetsmedvetandet hos all personal kan i det sammanhanget ses som en god investering. Det är också vår bestämda uppfattning att det behövs klara och genomarbetade rutiner för rekrytering och uppföljning av personal, då värdet av pålitliga medarbetare inte nog kan framhållas.

Lycka till med ert arbete.

PÄR KIHLSTRÖM
Chef säkerhetsskyddsenheten, Säkerhetspolisen

Innehållsförteckning

Inledning

SYFTE, MÅLGRUPP OCH AVGRÄNSNINGAR

Syftet med denna vägledning är att den ska användas vid tillämpningen av säkerhetsskyddslagstiftningen. Den vänder sig i första hand till de myndigheter över vilka Säkerhetspolisen har ett tillsynsansvar.

Olika personalkategorier vid myndigheterna kan ha nytta av att använda denna vägledning. Läsaren kan exempelvis vara säkerhetsskyddschef, handläggare eller IT-säkerhetsansvarig. Därför kan innehåll och nivå i vägledningens kapitel skifta, beroende på vilka läsare som i huvudsak förväntas ta del av materialet.

Beträffande säkerhetsskyddad upphandling (se kapitel 7) har Säkerhetspolisen också publicerat en mer utförlig vägledning till just detta område, *Säkerhetsskyddad upphandling – en vägledning* (uppdaterad i januari 2010). Även denna vägledning är placerad på Säkerhetspolisens webbplats.

Denna vägledning till säkerhetsskydd tar inte upp eller hanterar Försvarsmaktens ansvar inom säkerhetsskyddsområdet. För detta ändamål har Försvarsmakten gett ut handboken H Säk Skydd 2007. Försvarsmakten ger också ut föreskrifter om säkerhetsskydd.

VÄGLEDNINGENS DISPOSITION OCH INNEHÅLL

Vägledningen är upplagd så att den följer kapitelindelningen i Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd; RPSFS 2010:03.

INLEDNINGEN innehåller allmän information och diskussion kring begreppet säkerhetsskydd, varför säkerhetsskydd behövs samt ansvarsförhållanden.

KAPITEL 1-11 innehåller vägledande text och förklarande diskussioner kring de områden som säkerhetsskydd omfattar. I inledningen av varje kapitel och i vissa avsnitt finns en hänvisning till de relevanta bestämmelserna i säkerhetsskyddslagstiftningen. Under vissa avsnitt återfinns också rubriken Dokumentation.

Här listas de handlingar i vilka myndigheten bör dokumentera beslut, resultat, innehåll eller rutiner för just detta område inom säkerhetsskyddet.

I en BILAGA listas alla lagar och förordningar som nämns i texten, med eventuella förkortningar.

Med begreppet MYNDIGHET avses stat, kommun och landsting. Fortsättningsvis kommer begreppet att användas med denna heltäckande innebörd utan att detta preciseras varje gång begreppet förekommer i vägledningen.

VAD ÄR SÄKERHETSSKYDD?

Med säkerhetsskydd avses:

1. Skydd mot brott som kan hota rikets säkerhet
2. Skydd av hemliga uppgifter som rör rikets säkerhet
3. Skydd mot terrorism.

Säkerhetsskydd innebär alltså att myndigheter och andra som säkerhetsskyddslagstiftningen gäller för ska vidta förebyggande åtgärder för att skydda mot brott som kan hota rikets säkerhet, såsom spionerі och sabotage.

Hemliga uppgifter som rör rikets säkerhet ska också skyddas. Eftersom offentlighets- och sekretesslagen inte ger anvisningar om hur hemliga uppgifter som rör rikets säkerhet ska hanteras, regleras detta i säkerhetsskyddslagstiftningen.

Säkerhetsskyddet omfattar också skydd mot terrorism. I vissa fall utgör terroristbrott ett hot mot rikets säkerhet, i andra fall inte. Kännetecknande för alla terroristbrott är att de innebär ett angrepp mot de demokratiska spelreglerna i samhället. Ett skydd mot terroristbrott ligger därför under alla förhållanden nära värnet om rikets säkerhet.

Verksamhet som omfattas av säkerhetsskyddslagstiftningen ska ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Skyddsvärda resurser ska regelbundet inventeras i en säkerhetsanalys, kopplade till hot, risk och sårbarhet.

Säkerhetsskyddet ska förebygga att:

1. Uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet)
2. Obehöriga får tillträde till platser där de kan få tillgång till uppgifter som avses i punkt 1 eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning)
3. Personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning).

Säkerhetsskyddet ska även i övrigt förebygga terrorism. Utbildning och kontroll är andra viktiga delar i det förebyggande säkerhetsskyddsarbetet.

Bestämmelser om säkerhetsskydd finns i säkerhetsskyddslagen, säkerhetsskyddsförordningen samt i föreskrifter och allmänna råd som meddelas av Rikspolisstyrelsen och Försvarsmakten för sina specifika ansvars- och tillsynsområden. En myndighet kan också meddela egna föreskrifter inom sitt verksamhetsområde om verkställigheten av säkerhetsskyddslagen.

SÄKERHETSHOT OCH BEHOVET AV SÄKERHETSSKYDD

Säkerhetsskydd tar tid att organisera och bygga upp. Åtgärder måste ofta planeras långt i förväg. Då åtgärderna har införts kan de vara mycket kostsamma och tidsödande att förändra eller förbättra i efterhand. Det är inte ovanligt att det krävs beslut om säkerhetsskyddslösningar som ska vara verksamma i 10 till 20 år, ibland ännu längre. Utifrån dagens konkreta och potentiella säkerhetshot (fortsättningsvis i detta avsnitt benämnt hot) kan det därför vara svårt att utforma ett väl anpassat säkerhetsskydd.

Ett avgörande problem är att det är mycket svårt att säga något om hur de hot som Sverige ställs inför kommer att se ut på lång sikt. Hotbildsförändringar kan orsakas av politiska ställningstaganden på nationell nivå och EU-nivå, och kan även vara orsakade av en oförutsägbar händelseutveckling såväl nationellt som internationellt. Dessa förändringar kan visserligen pågå under lång tid och ha en viss grad av förutsägbarhet, men ofta sker förändringar i hotbilden plötsligt och oväntat.

Det är därför viktigt att säkerhetsskyddsarbetet i första hand drivs av vilka konsekvenser som olika händelser kan få, och att fokus läggs på att identifiera och reducera de sårbarheter som kan ge upphov till de allvarligaste konsekvenserna. Det är även av betydelse att följa hotets utveckling och hålla sig informerad om den aktuella hotbilden för att värdera om vidtagna åtgärder är tillräckliga. För detta ändamål är det användbart att formulera en dimensionerande hotbeskrivning, det vill säga en allmän beskrivning av en tänkt hotaktörs förmåga och tillvägagångssätt. Denna beskrivning bör ligga till grund för en dimensionering av säkerhetsskyddet. En dimensionerande hotbeskrivning säger alltså inget om sannolikheten för hotet eller om hotaktörens övergripande motiv, utan syftar till att tydliggöra vilka hot som verksamheten ska ha förmåga att möta. På så vis kan man uppnå såväl spårbarhet som långsiktighet i säkerhetsskyddsarbetet.

ANSVAR FÖR SÄKERHETSSKYDD

5, 30 §§ säkerhetsskyddslagen
6, 39–42, 45, 49 §§ säkerhetsskyddsförordningen
1 kap. 6–7 §§, 9 kap. RPSFS 2010:03

Ansvaret för säkerhetsskyddet inom en myndighet ligger hos dess ledning. De som omfattas av säkerhetsskyddslagstiftningen är därför skyldiga att kontrollera det egna säkerhetsskyddet. Det innebär också att personalen ska få utbildning i frågor om säkerhetsskydd, och att det ska finnas en plan för intern kontrollverksamhet.

Hos dem som omfattas av säkerhetsskyddslagstiftningen ska det finnas en säkerhetsskyddschef som utövar kontroll över säkerhetsskyddet. På en myndighet ska säkerhetsskyddschefen vara direkt underställd myndighetens chef.

Med tillsyn menas utövande av kontroll över annans verksamhet. I säkerhetsskyddsförordningen anges ett antal sektorsansvariga myndigheter som ska kontrollera säkerhetsskyddet hos de bolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande. Detsamma gäller säkerhetsskyddet hos enskilda företag. Den tillsynsansvariga myndigheten har ett visst ansvar att informera de enskilda företagen om att lagen gäller för dem.

Tillsyn kan även utföras av Säkerhetspolisen och i vissa fall i samråd med den myndighet som ska svara för tillsynen över säkerhetsskyddet.

Säkerhetsskyddet hos anbudsgivare och leverantörer som har träffat säkerhetsskyddsavtal ska kontrolleras av den avtalsslutande myndigheten.

SÄKERHETSPOLISENS ROLL SOM TILLSYNSMYNDIGHET

31 § säkerhetsskyddslagen
39, 42–44, 47–48 §§ säkerhetsskyddsförordningen

Säkerhetspolisens ansvar för säkerhetsskyddet är begränsat till att utöva tillsyn och att meddela föreskrifter. Säkerhetspolisen ska kontrollera säkerhetsskyddet för Kustbevakningen, Myndigheten för samhällsskydd och beredskap samt övriga myndigheter som inte svarar under Försvarsdepartementet. Säkerhetspolisen ska dessutom kontrollera kommuner och landsting. Tillsyn görs dock inte på Justitiekanslern, Fortifikationsverket och Försvarshögskolan.

I säkerhetsskyddslagstiftningen finns ingen uttrycklig bestämmelse som ger Säkerhetspolisen en skyldighet att lämna råd i särskilda fall, utom vad gäller Regeringskansliet, riksdagen och dess myndigheter samt Justitiekanslern. Det faller dock inom Säkerhetspolisens tillsynsansvar att i möjligaste mån biträda med råd om säkerhetsskydd.

För att säkerhetsskyddsarbete ska kunna bedrivas på ett för verksamheten ändamålsenligt och effektivt sätt, är det nödvändigt att det finns tillräckliga kunskaper om vad som behöver skyddas och vilka angrepp som kan tänkas ske. Denna information ska formuleras i en säkerhetsanalys. Här kan Säkerhetspolisen fullgöra en viktig uppgift inom sitt tillsynsområde genom att informera om den hotmiljö som myndigheternas verksamhet befinner sig i.

Vid rådgivning biträder Säkerhetspolisen med råd om säkerhetsskyddets organisation, omfattning och utformning, och innefattar exempelvis:

- Säkerhetsskyddets regelsystem
- Ansvarsförhållanden
- Metoder att genomföra säkerhetsanalys
- Administration av säkerhetsskyddet
- Metoder för genomförande av internkontroll
- Metoder för att höja säkerhetsmedvetandet
- Metoder för att göra personbedömning vid nyrekrytering.

Säkerhetspolisens tillsynsverksamhet innebär i grova drag att en överenskommelse träffas med den som tillsynen ska riktas mot om tidpunkt, inriktning och omfattning. Den kontrollerade ombeds bland annat tillhandahålla Säkerhetspolisen dokument över verksamheten, säkerhetsanalys med mera. Därefter görs tillsynsprogrammet upp i samråd, där tillfälle ges att ta upp frågeställningar som den kontrollerade känner sig osäker på eller inte behärskar.

Tillsynen börjar med en muntlig framställan genom att den kontrollerade myndigheten informerar om verksamheten och vad som bedöms som skyddsvärt. Säkerhetspolisen följer upp med en allmän information om det rättsliga bemyndigandet för tillsynens genomförande, inriktning och omfattning samt aktuell hotbild. Därefter vidtar en okulär och teknisk besiktning av de områden som har överenskommits som skyddsvärda. Tillsynen avslutas med en muntlig genomgång av de preliminära resultaten.

Vid tillsynens början och slut är det önskvärt att den verkställande ledningen finns representerad. Resultatet av tillsynen redovisas i en rapport och en uppföljning sker för att säkerställa att påtalade brister åtgärdas inom rimlig tid.

Åtgärdas inte brister som har framkommit vid en tillsyn ska tillsynsmyndigheten anmäla förhållandet till regeringen.

1 Allmänna bestämmelser

1.1 FÖR VEM GÄLLER SÄKERHETSSKYDDSLAGSTIFTNINGEN?

1–4 §§ säkerhetsskyddslagen
1–3 §§ säkerhetsskyddsförordningen
1 kap. 1–2 §§, 11 kap. RPSFS 2010:03

1.1.1 Bestämmelser om säkerhetsskydd

Bestämmelserna om säkerhetsskydd gäller vid verksamhet hos:

1. Staten, kommunerna och landstingen.
2. Aktiebolag, handelsbolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande.
3. Enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism.

Med enskilda menas alla företag över vilka det allmänna inte har ett rättsligt inflytande. Det handlar främst om verksamhet inom sådana från säkerhetssynpunkt känsliga områden som produktion och distribution av elkraft, telekommunikation och vattenförsörjning.

Bestämmelserna om säkerhetsskydd har utformats med utgångspunkten att de intressen som lagstiftningen slår vakt om ska ha samma skydd oavsett om verksamheten bedrivs av det allmänna eller av enskilda. Det har inte heller någon betydelse för säkerhetsskyddets omfattning om det allmänna driver verksamheten i traditionella myndighets- eller förvaltningsformer, eller om det sker genom egna bolag eller i annan associationsrättslig form.

För Regeringskansliet gäller endast vissa uppräknade bestämmelser (säkerhetsprövning och säkerhetsskyddad upphandling) och för kommittéer samt särskilda utredare gäller endast bestämmelserna om säkerhetsprövning.

1.1.2 Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd; RPSFS 2010:03

Säkerhetspolisen ska utöva tillsyn över säkerhetsskyddet hos vissa myndigheter. Rikspolisstyrelsen har meddelat föreskrifter och allmänna råd för säkerhetsskyddslagens tillämpning dels för sitt tillsynsområde, dels i fråga om förfarandet vid registerkontroll. RPSFS 2004:11 ersattes den 1 februari 2010 med RPSFS 2010:03.

Föreskrifterna gäller för Kustbevakningen, Myndigheten för samhällsskydd och beredskap samt övriga myndigheter som inte svarar under Försvarsdepartementet. Föreskrifterna gäller dessutom för kommuner och landsting (som är jämställda med myndigheter i föreskrifterna). Föreskrifterna gäller dock inte för Justitiekanslern, Fortifikationsverket och Försvarshögskolan.

Bestämmelserna om registerkontroll (som behandlas i kapitel 8 i föreskrifterna) gäller för samtliga myndigheter och alla andra organ – även för Regeringskansliet samt för myndigheter som avses i 39 § första punkten och bolag som avses i 19 § tredje punkten säkerhetsskyddsförordningen – som har rätt att besluta om registerkontroll.

Säkerhetspolisen får medge undantag från bestämmelserna i dessa föreskrifter.

1.1.3 Lagstiftning gällande riksdagen och dess myndigheter

För riksdagen och dess myndigheter gäller endast 11–29 §§ säkerhetsskyddslagen. Därutöver finns bestämmelser om säkerhetsskydd i lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter samt i lagen (1988:144) om säkerhetskontroll i riksdagens lokaler. För riksdagen, riksdagsförvaltningen och partikanslierna finns föreskrifter om bland annat säkerhetsskydd i Riksdagsförvaltningens föreskrift om säkerhet och fredstida krishantering; RFS 2006:2.

1.2 GRUNDLÄGGANDE BEGREPP

4 § säkerhetsskyddsförordningen
1 kap. 3–4 §§ RPSFS 2010:03

1.2.1 Begreppet rikets säkerhet

Någon legaldefinition av begreppet rikets säkerhet finns inte. Rikets säkerhet kan dock sägas avse såväl den yttre säkerheten för det nationella oberoendet som den inre säkerheten för det demokratiska statsskicket. Begreppet rikets säkerhet vållar ibland svårigheter och bekymmer i säkerhetsskyddsarbetet. Något exakt svar på vad som är rikets säkerhet finns inte, utan det är upp till varje myndighet att själva undersöka vilka uppgifter som ska hållas hemliga i förhållande till rikets säkerhet. Dessutom

ska det bedömas vilka anläggningar och system som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet och/eller till skydd mot terrorism. Viss vägledning kan man få genom att studera 18 och 19 kap. Brottsbalken och bestämmelserna om sabotage samt 6 och 7 §§ säkerhetsskyddslagen, som tar fasta på vad säkerhetsskyddet ska omfatta och förebygga.

Rikets yttre säkerhet tar i första hand sikte på totalförsvaret, som utgör den verksamhet som är nödvändig för att förbereda Sverige för krig. Totalförsvaret består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar). Under högsta beredskap är totalförsvar all den samhällsverksamhet som då ska bedrivas. I det civila försvaret ingår samhällsviktig infrastruktur som elförsörjning, vattenförsörjning, telekommunikation, hälso- och sjukvård, radio och tv med flera.

Den inre säkerheten kan vara hotad utan att totalförsvaret berörs. Angrepp mot rikets demokratiska statsskick kan förekomma från grupperingar utan förbindelse med främmande makt. Ett exempel är försök att ta över den politiska makten genom uppror, men också användning av våld, hot eller tvång mot den centrala statsledningen i syfte att påverka den nationella politikens utformning. I detta sammanhang kan det till exempel röra sig om kriminella aktiviteter inom den organiserade brottsligheten.

Ett hot mot rikets säkerhet som säkerhetsskyddsbestämmelserna ska förebygga är omstörtande verksamhet. Med det menas sådan subversiv eller underminerande verksamhet som syftar till att undergräva förtroendet för det svenska politiska systemet eller för att förbereda ett maktövertagande med illegala metoder. Denna verksamhet kan vara ett led i inhemska gruppers eller organisationers strategi, men även initierad och finansierad av främmande makt i syfte att bereda vägen för en militär intervention. Omstörtande verksamhet kan med detta synsätt avse såväl rikets yttre som inre säkerhet.

Om en verksamhet utsätts för antagonistiska handlingar så kan olika negativa konsekvenser uppstå. Dessa konsekvenser bör värderas med hjälp av följande frågeställningar:

1. Påverkas ett större antal människors liv och hälsa?
2. Påverkas ett större geografiskt område? Är denna påverkan långvarig och/eller inträffar den vid en olämplig tidpunkt?
3. Får händelsen allvarliga sociala, ekonomiska och/eller politiska konsekvenser för samhället?
4. Påverkas andra samhällsviktiga verksamheter allvarligt?
5. Finns det risk att allvarliga negativa konsekvenser uppstår i framtiden?

Om en eller flera av dessa frågeställningar besvaras jakande kan det bedömas rimligt att hela eller delar av verksamheten behöver säkerhetsskydd med hänvisning till rikets säkerhet.

Några exempel på samhällsviktiga verksamheter som kan röra eller ha betydelse för rikets säkerhet är bland annat energiförsörjning, finansiella tjänster, telekommunikationer, vattenförsörjning, transporter, livsmedelsförsörjning och arbete till skydd mot allvarlig smitta.

I offentlighets- och sekretesslagen finns bestämmelser som avser att skydda rikets säkerhet. Det är främst försvarssekretessen i 15 kap. 2 § som skyddar uppgifter vars röjande kan antas skada landets försvar eller på annat sätt vålla fara för rikets säkerhet. Andra sekretessbestämmelser av betydelse för rikets säkerhet är utrikessekretessen i 15 kap. 1 §, underrättelseverksamhet i 18 kap. 2 §, förundersökningssekretessen i 18 kap. 1 §, sekretess för kvalificerade skyddsidentiteter i 18 kap. 5 §, sekretessen för säkerhets- eller bevakningsåtgärd i 18 kap. 8 §, sekretessen för chiffer och kod i 18 kap. 9 § och sekretess för myndigheters risk- och sårbarhetsanalyser i 18 kap. 13 §.

1.2.2 Begreppet terrorism

Det finns ingen entydig definition av vad terrorism är. Lagen om terroristbrott baseras på EU:s rambeslut om bekämpande av terrorism. Enligt denna lag är terrorism en gärning som allvarligt kan skada en stat eller mellanfolklig organisation om gärningen syftar till att:

1. Injaga allvarlig fruktan hos en befolkning eller befolkningsgrupp,
2. Tvinga offentliga organ eller en mellanstatlig organisation att vidta eller avstå från att vidta en åtgärd, eller
3. Destabilisera eller förstöra grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturer.

Skyddsvärt i detta sammanhang är verksamhet som är kritiskt viktig för värnandet om ett öppet och säkert samhälle samt samhällsviktiga infrastruktursystem.

Det som är skyddsvärt mot terrorism och det som är skyddsvärt avseende rikets säkerhet kan ibland sammanfalla.

1.2.3 Övriga grundläggande begrepp

Ett antal begrepp är centrala i säkerhetsskyddsföreskrifterna, och har sitt ursprung i olika författningar. Det är därför viktigt att de definieras på rätt sätt och används med rätt innebörd av alla. Exempelvis kommer begreppet handling från tryckfrihetsförordningen, och flera andra definitioner kommer från säkerhetsskyddsförordningen. Begreppen som anges i 1 kap. 3–4 §§ RPSFS 2010:03 är ständigt återkommande och definieras som följer (se även avsnitt 2.4):

HANDLING: Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med teknisk hjälp (2 kap. 3 § tryckfrihetsförordningen).

HEMLIG UPPGIFT: Uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet (4 § säkerhetsskyddsförordningen).

HEMLIG HANDLING: Handling som innehåller hemlig uppgift (4 § säkerhetsskyddsförordningen).

KVALIFICERAT HEMLIG HANDLING: Handling som är av synnerlig betydelse för rikets säkerhet (1 kap. 3 § RPSFS 2010:03).

1.3 SÄKERHETSANALYS

5 § säkerhetsskyddslagen
5 § säkerhetsskyddsförordningen
1 kap. 5–7 §§ RPSFS 2010:03

1.3.1 Vad är säkerhetsanalys?

Myndigheter och andra som säkerhetsskyddsförordningen gäller för ska undersöka vilken verksamhet som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Det kan till exempel gälla att identifiera den mest skyddsvärda informationen, de mest skyddsvärda IT-systemen, de mest skyddsvärda anläggningarna och de mest känsliga befattningarna. Detta ska göras i en säkerhetsanalys.
En säkerhetsanalys utgör grunden för ett väl anpassat säkerhetsskydd. En säkerhetsanalys är dels en undersökning som syftar till att kartlägga vad som är skyddsvärt i en verksamhet, dels en handling som dokumenterar de resonemang som leder fram till vad som är skyddsvärt. Undersökningen ska också relatera det skyddsvärda till de hot som verksamheten kan utsättas för och de säkerhetssårbarheter som verksamheten kan vara behäftad med. Säkerhetssårbarheter (fortsättningsvis i detta avsnitt benämnt sårbarhet) är sådana sårbarheter som kan utnyttjas av en antagonist.

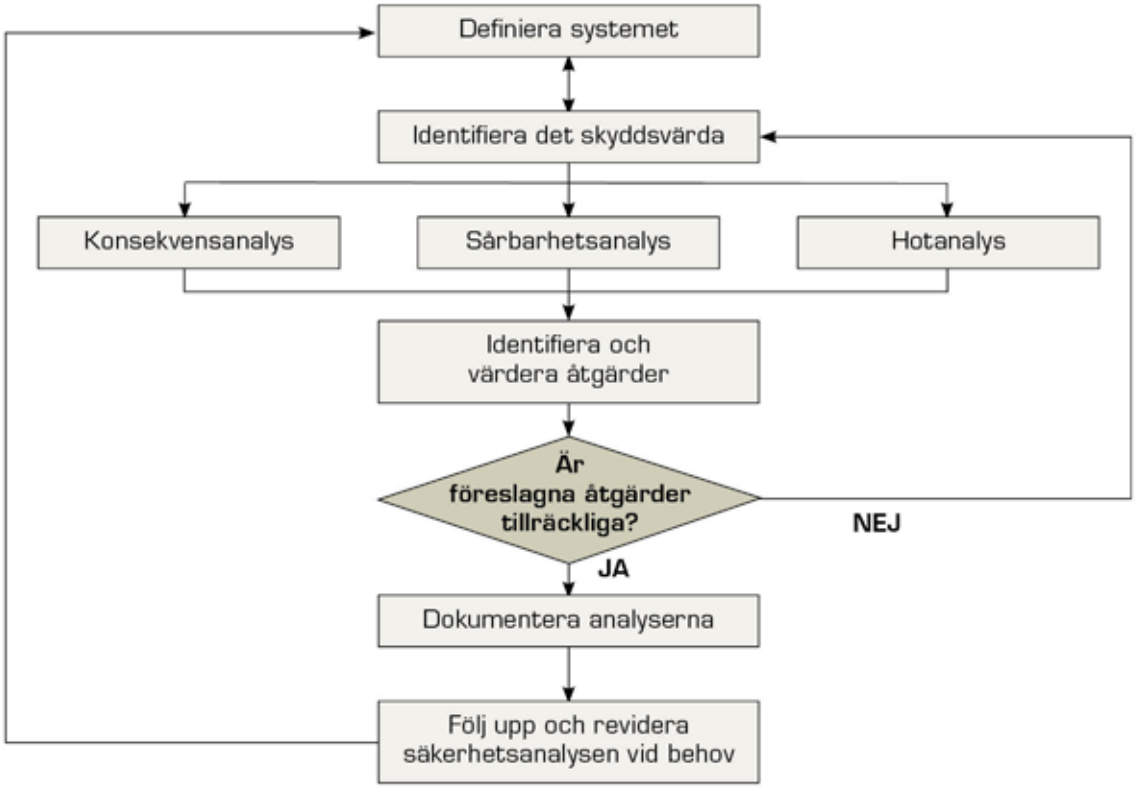
I förlängningen syftar säkerhetsanalysen till att ta fram ett beslutsunderlag för säkerhetsskyddsåtgärder samt att skapa spårbarhet för detta underlag. Säkerhetsskyddsåtgärder kan potentiellt sett vara relativt kostsamma och riskerar att ge en negativ påverkan på en verksamhets effektivitet. Det är därför viktigt att de som ska besluta om säkerhetsskyddsåtgärderna förstår motiven till de åtgärder som krävs utifrån identifierade behov. Likaså är det viktigt att den som måste beakta skyddsaspekterna i sitt arbete förstår de bakomliggande orsakerna. Annars finns risken att medarbetare försöker kringgå skyddsåtgärderna i syfte att höja effektiviteten i arbetet.

1.3.2 Processen för framtagande av en säkerhetsanalys

Arbetet med att ta fram en säkerhetsanalys är en process som kan delas in i fem olika steg. Stegen innebär att:
- Definiera systemet eller verksamheten som ska analyseras samt identifiera det skyddsvärda
- Värdera konsekvenser (konsekvensanalys)
- Identifiera sårbarheter (sårbarhetsanalys)
- Kategorisera och beskriva relevanta hotaktiviteter som kan ge allvarliga konsekvenser (hotanalys)
- Identifiera och värdera säkerhetsskyddsåtgärder som reducerar sårbarheter och medför att systemet eller verksamheten läggs på en väl anpassad skyddsnivå.

De olika stegen behöver inte utföras i någon speciell ordning utan kan delvis utföras parallellt och korsbefrukta varandra. Det kan dock vara lämpligt att initialt lägga tyngdpunkten på analys av konsekvenser och att vänta med att diskutera åtgärder. I figur 1 beskrivs ett ramverk för säkerhetsanalys* där de olika stegen relateras till varandra.

* Detta ramverk är influerat av det standardramverk som används för riskanalys av tekniska system. IEC, 1995, Dependability management - Part 3: Application guide — Section 9: Risk analysis of technological systems. International Electrotechnical Commission (IEC), Geneva.



Figur 1. Ramverk för säkerhetsanalys

Processen börjar med att SYSTEMET DEFINIERAS. Detta steg syftar till att tydliggöra och avgränsa vilken verksamhet det är som ska analyseras. Vad är verksamhetens övergripande mål och ansvar? Vilka generella processer består verksamheten av? Hur ser beroenden till andra verksamheter ut? Därefter kan verksamheten analyseras mer i detalj för att IDENTIFIERA DET SKYDDSVÄRDA, till exempel beträffande lokaler, anläggningar, befattningar, system, rutiner och information.

Det är viktigt att inte snäva in analysen av verksamheten alltför mycket i början, och exempelvis endast beakta sådant som tidigare har bedömts som skyddsvärt. Risken är då att nytillkommen verksamhet eller verksamhet som har fått ökad betydelse inte identifieras som skyddsvärd. Det är också viktigt att dokumentera den argumentation som leder till att något identifieras som skyddsvärt. Ofta är det minst lika viktigt att även dokumentera vad som inte är skyddsvärt.

KONSEKVENSANALYSEN kan med fördel utgå från de frågeställningar som ges i inledningskapitlets avsnitt 1.2.1 och 1.2.2 om begreppen rikets säkerhet och terrorism. Det viktiga är att identifiera de konsekvenser som får stor betydelse inte bara för den egna verksamheten utan också för hela samhället.

SÅRBARHETSANALYSEN kan innefatta allt från bedömningar av olika säkerhetspolicyer och besiktningar av befintliga fysiska säkerhetsåtgärder till penetrationstester av IT-system. Här gäller det att identifiera brister som kan utnyttjas av en tänkt hotaktör och som kan medföra mycket allvarliga konsekvenser.

Vid identifieringen av de hotaktiviteter som kan riktas mot verksamheten – HOTANALYSEN – krävs kreativitet för att formulera vilka tänkbara taktiska mål som aktörer skulle kunna finna i den verksamhet som ska analyseras. Man bör ha i minnet att antagonister försöker att slå så effektivt som möjligt, det vill säga utsätter sig för minsta möjliga risk och följer inga regler för att uppnå största möjliga effekt.

Till skillnad från många kvantitativa riskanalysmodeller beräknas i en säkerhetsanalys ingen

sannolikhet för att ett hot ska realiseras. När det gäller antagonistiska hot är detta i det närmaste omöjligt att göra med någon som helst noggrannhet eller precision. När man ska värdera hot är det därför viktigt att undvika utsagor av sannolikhetskaraktär. Mer användbart är att göra relativa bedömningar där man rangordnar möjliga hot mot en viss verksamhet efter hur troliga man bedömer dem vara i relation till varandra.

Hotanalysen bör syfta till att ta fram en dimensionerande hotbeskrivning (se inledningskapitlets avsnitt Säkerhetshot och behovet av säkerhetsskydd) för verksamheten. Den dimensionerande hotbeskrivningen utgörs av de bedömda egenskaper som en angripare kan tänkas ha samt de förutsättningar som gäller vid det hypotetiska angreppstillfället. Beskrivningen bör vara utformad så att det finns en viss marginal i förhållande till den aktuella hotbilden. Det innebär att det bör finnas utrymme för förändringar i hotbilden utan att verksamheten för den skull måste påbörja ett omfattande arbete med att identifiera och införa nya skyddsåtgärder för att möta hoten.

Vilka ÅTGÄRDER som det finns behov av att genomföra beror på vilka sårbarheter som har identifierats. Att värdera vilka åtgärder som är mest lämpliga styrs av flera faktorer. Skyddsåtgärder som förhindrar de allvarligaste konsekvenserna är naturligtvis högt prioriterade. Likaså bör man beakta vilka som är de troligaste tillvägagångssätten för en hotaktör samt vilket skydd som redan finns på plats. Åtgärderna får inte begränsa verksamhetens huvudsyfte i alltför stor utsträckning, då de i så fall riskerar att bli kontraproduktiva. Sist men inte minst spelar naturligtvis kostnaden för olika åtgärder en betydande roll. Alla åtgärder behöver dock inte införas omedelbart utan kan skjutas på framtiden. Det kan vara användbart att formulera kriterier som indikerar när en viss åtgärd bör införas.

Arbetet bygger till stor del på subjektiva expertbedömningar. Det är därför viktigt att i alla steg DOKUMENTERA de resonemang och bedömningar som görs för att skapa spårbarhet i de beslut som sedan fattas med avseende på säkerhetsskydd.

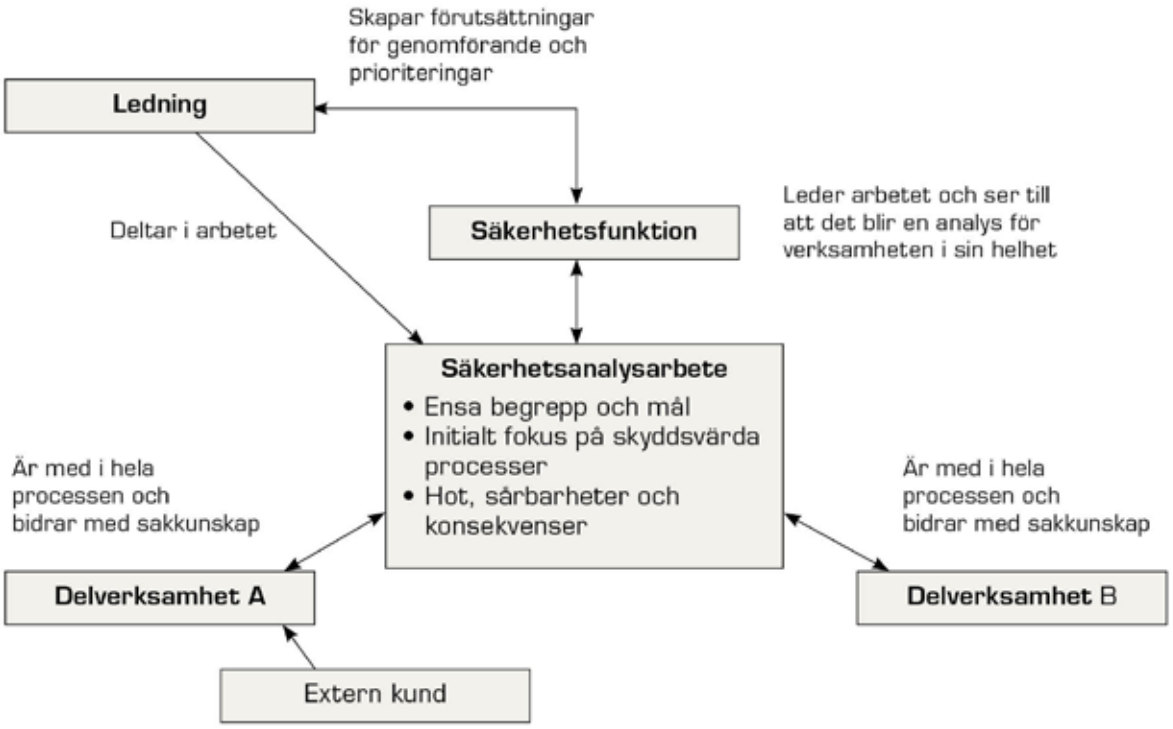
När verksamheten förändras och detta potentiellt sett kan påverka säkerhetsskyddet ska man följa upp säkerhetsanalysen och eventuellt revidera analysen, varvid man får gå igenom hela säkerhetsanalysprocessen igen.

1.3.3 Organisationen för framtagande av en säkerhetsanalys

Arbetsprocessen för att ta fram en säkerhetsanalys (se figur 2) kan ta sig många olika former. Det är viktigt att ledningen stödjer och skapar förutsättningar för säkerhetsanalysarbetet. När det gäller stora och komplexa verksamheter kan det vara lämpligt att utse en grupp med ansvar för hela säkerhetsanalysen – en säkerhetsfunktion. Denna grupp bör besättas så att det finns kunskap om helheten i verksamheten. Likaså bör det i gruppen finnas kunskaper om hur konsekvens-, sårbarhets- och hotanalyser kan genomföras. Funktionen bör i säkerhetsanalysarbetet ta stöd av sakkunniga från olika delverksamheter.

En viktig poäng med att ha en övergripande funktion som leder säkerhetsanalysarbetet är att man skapar förutsättningar för att inte missa sårbarheter mellan olika delverksamheter.

De flesta verksamheter har olika typer av krav på sig att genomföra risk- och sårbarhetsanalyser och har därför befintliga processer för framtagandet av dessa. Säkerhetsanalysarbetet bör relatera till och nyttja material från detta analysarbete. Det är dock viktigt att påpeka att en säkerhetsanalys ensidigt fokuserar på antagonistiska hot och på de delar av verksamheten där de allvarligaste konsekvenserna kan uppstå på grund av spionage eller sabotage.



Figur 2. Organisation för genomförande av säkerhetsanalys

2 Allmänt om informationssäkerhet

7, 9 §§ säkerhetsskyddslagen
4, 9–13 §§ säkerhetsskyddsförordningen
1 kap. 3–4, 6 §§, 2 kap. RPSFS 2010:03

2.1 BEGREPPET INFORMATIONS-SÄKERHET

Det finns flera definitioner av begreppet informationssäkerhet. En av dem beskriver informationssäkerhet som säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet. Även ytterligare egenskaper, såsom exempelvis spårbarhet, kan tillföras begreppet.

I begreppet informationssäkerhet ryms såväl säkerhet relaterad till hanteringen av fysiska handlingar som säkerhet relaterad till IT (se figur 3). För att nå upp till lämplig skyddsnivå för IT-system krävs ofta en kombination av olika skyddsåtgärder. IT-säkerhet avser främst skyddsåtgärder av teknisk karaktär, till exempel olika former av behörighetskontrollsystem. IT-säkerhet inkluderar både datasäkerhet (säkerhet i samband med behandling och/eller lagring av data) och kommunikationssäkerhet (säkerhet vid överföring av data). För att höja den generella säkerhetsnivån behöver ofta IT-säkerhetsskyddsåtgärder kompletteras med exempelvis fysiska och administrativa säkerhetsåtgärder.

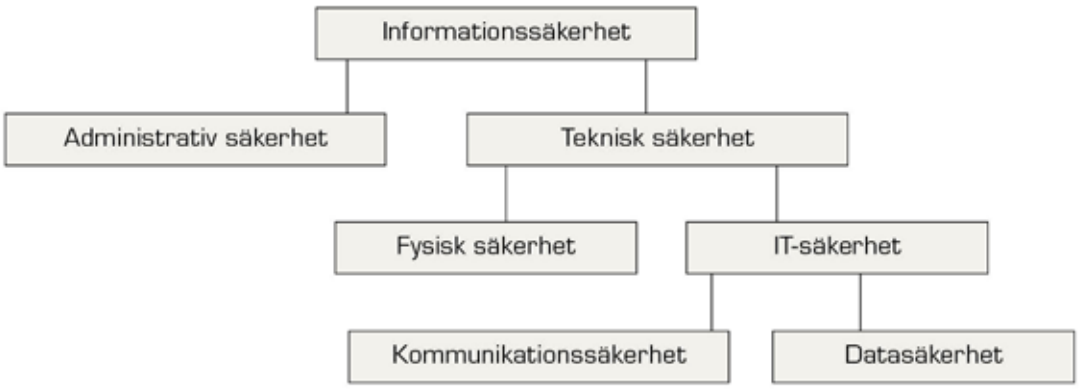
2.2 BESTÄMMELSER OCH HJÄLPMEDEL

Förutom de grundläggande säkerhetsskyddsbestämmelserna – säkerhetsskyddslagen, säkerhetsskyddsförordningen samt RPSFS 2010:03 – finns inom informationssäkerhetsområdet även Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2009:10). Enligt dessa ska en myndighet i sitt arbete med säkert elektroniskt informationsutbyte tillämpa ett ledningssystem för informationssäkerhet, LIS. Det ska ske i former enligt etablerade svenska standarder, för närvarande:

- SS-ISO/IEC 27001:2006, fastställd 2006-01-19
- SS-ISO/IEC 27002:2005, fastställd 2005-08-12.

Vid sidan av bestämmelser som ställer krav på informationssäkerhetsarbetet finns också ett flertal hjälpmedel i form av metoder, standarder och verktyg. Exempel på detta är Common Criteria (ISO/IEC 15408), standard och metod för utvärdering av säkerheten i IT-produkter och system, samt BITS (basnivå för IT-säkerhet). Dessa ger en bra överblick över vad som ska åtgärdas men säger inte nödvändigtvis hur det ska göras.

För att få vägledning i hur ett säkerhetsarbete ska planeras och genomföras bör någon form av metodik tillämpas. Flera olika metoder för riskhantering finns att tillgå. En av dessa är den så kallade fria metodiken OCTAVE (www.cert.org/octave).



Figur 3. Sambandet mellan informationssäkerhetsbegreppets olika delar (se Terminologi för informationssäkerhet, SIS HB 550, 2007).

2.3 HANDLINGSSEKRETESS OCH TYSTNADSPLIKT I DET ALLMÄNNAS VERKSAMHET

Offentlighetsprincipen är ett grundläggande inslag i svensk rättskipning och offentlig förvaltning. Den innebär att allmänheten och massmedierna ska ha så stor insyn i det allmännas verksamhet som möjligt. Exempel på detta är allmänna handlingars offentlighet, yttrande- och meddelarfrihet samt offentlighet vid domstolsförhandlingar och vid beslutande församlingars sammanträden. I vissa fall är dock behovet av att skydda uppgifter större än rätten till insyn för den enskilde. I offentlighets- och sekretesslagen finns bestämmelser som närmare anger i vilken utsträckning undantag gäller från principen om allmänna handlingars offentlighet.

Sekretess enligt offentlighets- och sekretesslagen gäller för en uppgift som sådan. Det innebär att det saknar betydelse om uppgiften förekommer i en handling, framgår av ett annat föremål eller inte är dokumenterad. Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom att en allmän handling lämnas ut eller sker på annat sätt. Denna tystnadsplikt kvarstår även efter det att anställningen, uppdraget eller dylikt har upphört.

Den som röjer uppgifter i strid med bestämmelser i lag eller förordning kan göra sig skyldig till brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken. Är brottet mot tystnadsplikten straffbart enligt någon annan straffbestämmelse tillämpas denna i första hand. Exempelvis kan den som bryter mot bestämmelserna i 15 kap. offentlighets- och sekretesslagen i vissa fall i stället dömas för brott mot riket säkerhet, till exempel spionerі.

Det finns undantag från tystnadsplikten, den så kallade meddelarfriheten, som är en grundlagsskyddad rättighet. Det innebär att det kan vara tillåtet att röja en uppgift för exempelvis publicering i massmedia som det i andra fall är förbjudet att avslöja. Meddelarfriheten innebär inte någon skyldighet att lämna uppgifter till massmedierna, utan bara en möjlighet att göra det. Meddelarfriheten begränsas dock på vissa områden där intresset av sekretesskydd väger tyngre än behovet av insyn.

Det är därför inte tillåtet att:

- Lämna ut uppgifter för publicering genom vilket uppgiftslämnaren gör sig skyldig till ett allvarligt brott mot rikets säkerhet
- Med avsikt lämna ut allmän handling som är hemlig för publicering
- Avsiktligen bryta mot de tystnadsplikter där rätten att meddela och offentliggöra uppgifter har inskränkts av offentlighets- och sekretesslagen.

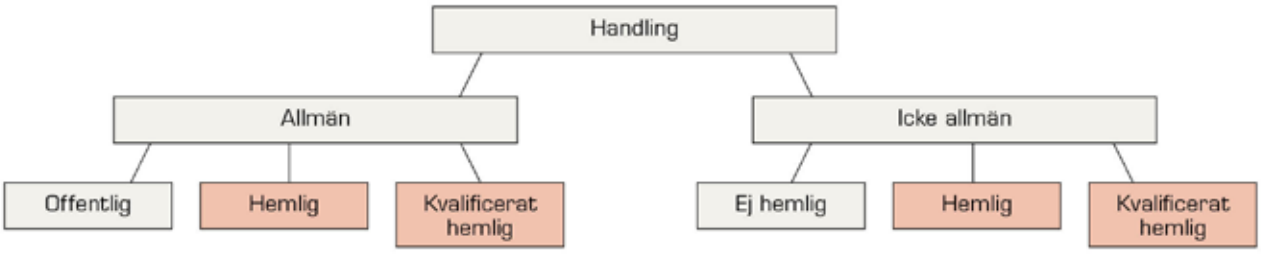
När det gäller hemliga uppgifter som rör rikets säkerhet är därför meddelarfriheten starkt begränsad.

Om någon utnyttjar sin rätt till meddelarfrihet råder det ett efterforskningsförbud för myndigheter eller andra allmänna organ att efterforska vem källan är. Det så kallade anonymitetsskyddet innebär att journalister med flera inte får avslöja sin källa om denna vill vara anonym.

2.4 ALLMÄN HANDLING

En handling som förvaras hos en myndighet efter att den antingen har inkommit till myndigheten eller upprättats där är – utom i vissa i tryckfrihetsförordningen angivna undantagsfall – en allmän handling. Med upprättad menas i detta sammanhang att handlingen har expedierats eller i övrigt är att anse som färdigställd. En allmän handling är offentlig, om inte innehållet ska hemlighållas med stöd av offentlighets- och sekretesslagen.

Utanför begreppet allmän handling faller hos en myndighet tillkomna minnesanteckningar, under förutsättning att de efter slutbehandling av det ärende som de angår inte har tagits omhand för ar-



Figur 4. Olika typer av handlingar. Handlingar i de färgade rutorna som rör rikets säkerhet ska säkerhetsskyddas.

kivering. Med minnesanteckningar avses promemorior och andra uppteckningar eller upptagningar som har tillkommit endast som hjälpmedel vid ett ärendes föredragning eller beredning, och som inte har tillfört ärendet nytt sakmaterial.

Inte heller icke justerade protokoll, beslut eller skrivelser innefattas i begreppet allmän handling. Denna typ av handlingar, som kallas interna handlingar eller arbetshandlingar, blir inte allmänna handlingar förrän de har expedierats eller tagits omhand för arkivering.

2.5 REGISTRERING OCH UTLÄMNANDE AV ALLMÄNNA HANDLINGAR

5 kap. 1–4 §§, 6 kap. offentlighets- och sekretesslagen
1, 3 §§ offentlighets- och sekretessförordningen
3 kap. 4, 9, 14, 16, 24 §§ RPSFS 2010:03

Kravet på registrering av hemliga handlingar i offentliga register är motiverat av allmänhetens möjlighet till insyn i myndighetens bestånd av allmänna handlingar. Enligt huvudregeln ska en hemlig handling som är allmän registreras i ett register som är tillgängligt för allmänheten. Vid registrering av en hemlig handling får emellertid vissa uppgifter utelämnas.

En allmän hemlig handling kan dessutom registreras i ett hemligt register hos myndigheten. I ett hemligt register har allmänheten ingen insyn, varför registreringen kan göras fullständig. Vidare kan man där göra alla för handläggningen nödvändiga noteringar.

Förfarandet med ett hemligt register som komplement till ett offentligt register kan rekommenderas, eftersom myndigheten genom registret får en samlad och god överblick över myndighetens samtliga hemliga handlingar, såväl allmänna som inte allmänna. Detta underlättar den inventering av hemliga handlingar som myndigheten är skyldig att göra. Vidare är myndigheten skyldig att ha någon form av diarium eller register som visar var myndighetens samtliga hemliga handlingar förvaras.

Om en myndighet förvarar många kvalificerat hemliga handlingar är det lämpligt att dessa registreras i ett särskilt register.

Av tryckfrihetsförordningen och offentlighets- och sekretesslagen framgår det att en begäran att få ta del av en allmän handling görs hos den myndighet som förvarar handlingen. Huvudregeln är att det också är denna myndighet som prövar frågan om utlämnande av en allmän handling till en enskild. I ett sådant fall kan myndigheten fritt ta ställning till utlämnandefrågan. I vissa fall – på grund av föreskrift i sekretessbestämmelse i lag eller förordning – prövar en annan myndighet frågan om utlämnande av allmän handling till en enskild. Ett exempel på ett sådant fall är att en begäran om att få ta del av handlingar som är av synnerlig betydelse för rikets säkerhet endast får prövas av vissa departementschefer. Om en handling till exempel avser kvalificerat hemliga uppgifter som angår polisens verksamhet för att hindra eller uppdaga brott som rör rikets säkerhet, är det chefen för Justitiedepartementet som prövar utlämnandefrågan. Ytterligare information finns i avsnitt 2.3 om handlingssekretess och tystnadsplikt i det allmännas verksamhet.

2.6 MYNDIGHETENS HEMLIGA HANDLINGAR OCH ARBETSMATERIEL

2 kap. 4–6 §§ RPSFS 2010:03

Informationssäkerheten beträffande hemliga handlingar kan oftast byggas upp på ett likartat sätt på de flesta myndigheter. Denna typ av skydd behandlas därför jämförelsevis utförligt i kapitel 3–4. Åtgärder för att skydda föremål måste däremot ofta bestämmas från fall till fall.

Hemliga uppgifter kan framgå av ett visst förhållande, en anläggning eller föremål av olika slag.

Med FÖRHÅLLANDE avses resurser och verksamhet av vilka det framgår planläggning, belägenhet, beredskap, intresseinriktning, effekt eller dylikt.

Med ANLÄGGNING avses i regel ett markområde, byggnad, rum eller annat utrymme som är iordningställt för en viss funktion eller verksamhet. Begreppet innefattar även nödvändiga installationer såsom tele-, korskopplings- och serverrum, skyddsrum, förrådslokaler eller befästningar.

Med FÖREMÅL avses en handling eller materiel. Med handling menas en framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. Materiel är andra föremål, exempelvis konstruktion, maskin, utrustning och andra lagringsmedier.

Materiel som innehåller hemliga uppgifter ska så långt det är möjligt hanteras på samma sätt som hemliga handlingar.

När det gäller icke allmänna handlingar finns det ingen skyldighet att lämna ut dem till utomstående även om innehållet inte är sekretessbelagt. I den mån innehållet är hemligt med stöd av offentlighets- och sekretesslagen samt rör rikets säkerhet (hemliga uppgifter) ska de dock säkerhetsskyddas, vilket är av betydelse för den interna hanteringen. Det är nämligen inte handlingens status av att vara allmän eller inte som avgör dess skyddsvärde. Alla hemliga uppgifter är lika skyddsvärda oavsett i vilken form av handling de är dokumenterade. Menet eller skadan vid ett eventuellt röjande av de hemliga uppgifterna kan vara lika stort oberoende av om uppgifterna finns i en allmän hemlig handling eller en icke allmän hemlig handling.

En hemlig handling kan därför vara en allmän handling, en intern handling, en minnesanteckning eller ett koncept som innehåller hemliga uppgifter. Även lagringsmedier och annan liknande arbetsmateriel är att jämställa med hemliga handlingar, om de innehåller hemliga uppgifter (hemlig arbetsmateriel). Se figur 4.

Hemliga uppgifter i IT-system och lagringsmedier som innehåller eller har innehållit hemliga uppgifter ska hanteras på samma sätt som hemliga handlingar. Med lagringsmedium avses såväl digitala lagringsmedier som andra lagringsmedier, dock inte handlingar i skrift eller bild.

Med digitala lagringsmedier avses lagringsmedier som är avsedda för annat än tillfällig lagring i arbetsminne av digital information, till exempel hårddiskar, disketter och USB-minnen.

Med andra lagringsmedier avses till exempel analoga videoband, analoga ljudband och mikrofilm.

Ett lagringsmedium ska ha ett säkerhetsskydd som motsvarar den högsta säkerhetsskyddsnivå som krävs för såväl de enskilda uppgifterna som den totala mängden hemliga uppgifter på lagringsmediet. Ytterligare information om informationssäkerhet i IT-system finns i kapitel 4.

Annan materiel som innehåller hemliga uppgifter ska hanteras på samma sätt som hemliga handlingar i skrift eller bild. Om detta inte är möjligt ska andra åtgärder vidtas så att säkerhetsskyddet blir jämförbart med det som finns för hemliga handlingar i skrift eller bild.

2.7 BEHÖRIGHET ATT TA DEL AV HEMLIGA UPPGIFTER SAMT UNDERTECKNANDE AV SEKRETESSFÖRBINDELSE

7–8 §§ säkerhetsskyddsförordningen
2 kap. 1 § RPSFS 2010:03

Endast den som är behörig att ta del av hemliga uppgifter får göra det, om inte något annat följer av särskilda bestämmelser i lag.

Behörig är den som uppfyller följande tre krav:

1. Bedöms som pålitlig* från säkerhetssynpunkt
2. Har tillräckliga kunskaper om säkerhetsskydd
3. Behöver uppgifterna för sitt arbete i den verksamhet där de hemliga uppgifterna förekommer.

Varje myndighet bör internt närmare informera om sina föreskrifter om hantering av hemliga handlingar. Ytterligare information om utbildning finns i kapitel 9.

Om hemliga uppgifter ska delges muntligen med en större grupp behöriga personer är det viktigt att detta sker i en lokal som är lämplig från säkerhetsskyddssynpunkt. I detta avseende bör man bland annat beakta risken för att någon form av hemlig avlyssning kan förekomma.

När det gäller kvalificerat hemliga uppgifter ska myndighetens chef eller motsvarande organ, eller den som sådan chef eller sådant organ bestämmer, besluta vem som är behörig att ta del av uppgifter av detta slag.

Den som tillåts att ta del av hemliga uppgifter ska också upplysas om omfattningen och innebörden av sekretessen. Denna upplysning kan ske genom att myndigheten upprättar en sekretessförbindelse, som undertecknas av den som har fått denna upplysning. En sekretessförbindelse är en bekräftelse på att den anställde eller den person som anlitas har blivit påmind om vad som gäller avseende tystnadsplikt, samt att han eller hon ska rätta sig efter offentlighets- och sekretessbestämmelserna. I en eventuell rättegång eller ett disciplinärt förfarande utgör en sekretessförbindelse ett bevis på att personen i fråga har eller borde ha förstått att han eller hon bröt mot sin tystnadsplikt.

* Denna bedömning grundas på den säkerhetsprövning som ska genomföras i varje enskilt fall. Ytterligare information om säkerhetsprövning finns i kapitel 6.

En utebliven upplysning är inte någon grund för ansvarsfrihet. Tystnadsplikten gäller på grund av lag och inte på grund av upplysningen.

2.8 ARBETE MED HEMLIGA UPPGIFTER

Arbetet med hemliga uppgifter måste bedrivas på ett sådant sätt att obehöriga inte kan få del av uppgifterna. För att hindra obehörig insyn kan avskärmning, övertäckning eller dylikt krävas i vissa situationer. Vid arbete med hemliga uppgifter i IT-baserade utrustningar måste problematiken med röjande signaler (RÖS) beaktas. Ytterligare information om röjande signaler finns i avsnitt 4.2.7.

Personer som för sin anställning eller för sitt uppdrag inte behöver tillgång till hemliga uppgifter bör inte ha sitt varaktiga arbete förlagt till lokaler där sådana uppgifter hanteras, utan att personerna bedömts som pålitliga från säkerhetssynpunkt och har tillräckliga kunskaper om säkerhetsskydd.

För personer som anlitats att utföra till exempel reparations- och underhållsarbeten i lokaler där hemliga uppgifter förvaras gäller särskilda regler. Ytterligare information om säkerhetsskyddad upphandling finns i kapitel 7.

2.9 MARKERING OCH KLASSIFICERING AV HEMLIGA HANDLINGAR

2 kap. 2, 16 §§ tryckfrihetsförordningen
5 kap. 5 § offentlighets- och sekretesslagen
3 kap. 1–4 §§, 4 kap. 27–29 §§ RPSFS 2010:03

2.9.1 Sekretessmarkering

Den grundläggande bestämmelsen för att få göra en anteckning om att en allmän handling inte får lämnas ut finns i tryckfrihetsförordningen.

En allmän handling får enligt offentlighets- och sekretesslagen förses med en särskild anteckning – sekretessmarkering – om det kan antas att en uppgift i handlingen inte får lämnas ut på grund av en bestämmelse om sekretess.

Det finns inte längre något krav på att endast ordet hemlig får användas vid markering av att det kan gälla sekretess för vissa uppgifter i en handling. Bestämmelsen är teknikneutral. Anteckningen ska ange tillämplig sekretessbestämmelse, datum för anteckningen samt den myndighet som har låtit göra den.

Utlämnande till en enskild av en uppgift i en allmän handling som är av synnerlig betydelse för rikets säkerhet enligt offentlighets- och sekretessförordningen kan i vissa fall prövas endast av en viss myndighet. Om så är fallet ska en sekretessmarkering göras så snart som möjligt. Av anteckningen ska det framgå vilken myndighet som ska pröva frågan om utlämnande.

2.9.2 Hemligbeteckning och klassificering

En hemlig handling ska markeras genom en särskild anteckning som anger vilket skydd informationen i handlingen kräver. Detta gäller både allmänna handlingar och icke allmänna handlingar.

Informationsklassificering innebär en indelning av information i en hemlig handling utifrån kriterier avseende konfidentialitet, tillgänglighet, riktighet med mera. Till exempel föreskriver Försvarsmakten att hemliga handlingar ska indelas i fyra olika informationssäkerhetsklasser (se FFS 2010:01). Bestämmelser om andra myndigheters informationsklassificering finns i MSBFS 2009:10.

Genom att klassificera hemliga handlingar och hemligbeteckna dessa anges i vilken säkerhetsskyddsnivå handlingen ska hanteras. Vid osäkerhet om konsekvenserna av att uppgifterna röjs, ändras eller förstörs bör en hemlig handling hanteras enligt reglerna i den högsta säkerhetsskyddsnivån.

En allmän hemlig handling ska förses med en hemligbeteckna dessa anges i vilken säkerhetsskyddsnivå handlingen ska hanteras. Ramen ska vara enkel för hemlig handling och dubbel för kvalificerat hemlig handling. Den rektangulära ramen bör vara röd. Se figur 5.

Figur 5. Exempel på hur hemligbeteckningar kan utformas på en hemlig handling.

SÄKERHETSPOLISEN HEMLIG SE SIDAN 1	Dokument		Sida
	RAPPORT		18 (58)
Upprättad av	Datum	Diarienr	
	2009-12-06		

Figur 6. Exempel på hänvisning till hemligbeteckning på första sidan.

En hemlig handling som inte är allmän ska förses med en anteckning om att den är hemlig. Sådan anteckning kan utformas på samma sätt som för en allmän handling.

Om en hemlig handling – oavsett om den är allmän eller inte – består av flera sidor, ska hänvisning göras på varje sida till hemligbeteckningen (se figur 6).

I det fall en hemlig handling som är försedd med hemligbeteckning inte längre bedöms vara hemlig, ska en anteckning om detta göras på handlingen. Denna anteckning ska innehålla uppgift om:

- Myndighetens namn
- Datum för anteckningen
- Vem som beslutat i saken.

Hemligbeteckningen ska överkorsas och i förekommande fall ska en anteckning om åtgärden ske i myndighetens diarium. Samråd bör ske med den som har upprättat handlingen.

I fråga om kvalificerat hemliga handlingar gäller dessutom följande: när en handling som har betraktats som kvalificerat hemlig inte längre bedöms vara det ska – innan bedömningen föranleder någon åtgärd – samråd ske med den som har upprättat handlingen. Anteckningen om samrådet ska göras på handlingen. Om en kvalificerat hemlig handling övergår till att vara hemlig ska man tillämpa det förfarande som gäller för en hemlig handling som inte längre bedöms vara hemlig (se ovan).

Vid arkivering av hemliga handlingar bör man pröva om uppgifterna fortfarande omfattas av sekretess och rör rikets säkerhet samt vilken säkerhetsskyddsnivå som är aktuell.

Det kan vara på sin plats att här påminna om bestämmelsen i 2 kap. 7 § RPSFS 2010:03 om att hemlig materiel som innehåller hemliga uppgifter så långt som möjligt ska hanteras på samma sätt som hemliga handlingar. Hemlig materiel samt pärmar, kortlådor eller dylikt med hemligt innehåll, bör om det behövs märkas för att upplysa om att innehållet är hemligt samt vilken säkerhetsskyddsnivå som gäller.

2.10 INTERNATIONELL SAMVERKAN

10 kap. RPSFS 2010:03

Handlingar som upprättas i Sverige men är avsedda att sändas till en annan stat, utländsk myndighet eller mellanfolklig organisation bör – utöver en eventuell svensk markering – ges relevant utländsk beteckning såsom TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED eller motsvarande. Utländsk beteckning bör även ges andra handlingar som upprättas i Sverige, om Sverige eller en myndighet i Sverige internationellt åtagit sig att så ska ske. Motsvarande bör gälla för annat lagringsmedium och materiel. Vid markering med utländsk beteckning bör respektive definition i tillämplig internationell överenskommelse beaktas. Utländsk beteckning bör utformas i enlighet med vad som föreskrivs i tillämplig internationell överenskommelse eller, i det fall sådana föreskrifter saknas, på annat lämpligt sätt.

I internationellt samarbete förekommer också beteckningen LIMITE avseende handlingar som inte är att anse som hemliga men som endast bör sändas till behöriga mottagare. Handlingen är med andra ord inte avsedd att offentliggöras. Det kan därför

ibland vara motiverat med ett visst säkerhetsskydd för dessa handlingar.

En hemlig handling i skrift eller bild som sänds utomlands ska förses med anteckning om uppgifternas ursprungsland.

2.11 SIGNALSKYDD

13 § säkerhetsskyddsförordningen
2 kap. 2–3 §§ RPSFS 2010:03

Innan hemliga uppgifter sänds i ett datanät utanför myndighetens kontroll ska myndigheten förvissa sig om att det finns en fullgod informationssäkerhet för uppgifterna. Hemliga uppgifter får krypteras endast med kryptosystem som är godkända av Försvarsmakten (Högkvarteret). Sändningen ska ske enligt de regler som gäller för den aktuella säkerhetsskyddsnivån. För signalskyddstjänsten gäller därutöver särskilda bestämmelser när det gäller kryptonycklar och signalskyddsmateriel samt användningen av kryptografiska funktioner.

Med signalskyddssystem avses här främst:

- Krypto-PC (MGR)
- Kryptotelefon (MGL)
- Kryfax (MGM)
- Krypterat GSM-telefonsystem (MGWI)
- Krypterat mobilt GSM-system (MGCI).

Utöver instruktionsböcker för respektive system finns grundläggande regler om signalskyddstjänsten i handboken för signalskyddstjänsten, H TST Grunder (2007). Särskilda regler för signalskyddstjänsten återfinns till exempel i förordning om krisberedskap och höjd beredskap, i FFS 2005:2 samt i Myndigheten för samhällsskydd och beredskaps föreskrifter om civila myndigheters kryptoberedskap; MSBFS 2009:11.

Från den 1 januari 2009 ansvarar Försvarets radioanstalt (FRA) för och samordnar signalskyddstjänsten i det civila försvaret. Däremot ska Försvarsmakten leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information, vilket framgår av 3 § förordningen med instruktion för Försvarsmakten.

3 Informationssäkerhet för hemliga handlingar i skrift eller bild

3.1 ARBETSRUTINER FÖR HEMLIGA HANDLINGAR I SKRIFT ELLER BILD

3.1.1 Framställning

3 kap. 5–6, 24 §§ RPSFS 2010:03

När en allmän hemlig handling i skrift eller bild framställs ska handlingen förses med uppgifter enligt följande.

På första sidan ska anges:
- Handlingens beteckning
- Exemplarnummer
- Sidantal
- Antalet bilagor (om bilagor följer med den hemliga handlingen).

Sidorna i den hemliga handlingen ska numreras i löpande följd. På bilagor och blad i bok med lösbladssystem ska det också anges till vilken handling bilagan respektive bladet hör. Det ska framgå av en sändlista eller en särskild förteckning hur många exemplar av den allmänna hemliga handlingen som har framställts och vilka som är mottagare av dessa. Ett missiv eller en ärendemening bör inte innehålla någon hemlig uppgift.

En utgångspunkt vid framställningen av hemliga handlingar bör vara att hemliga och offentliga uppgifter in i det längsta tas in i skilda handlingar. Det är också viktigt att tänka på att inte framställa en hemlig handling i större antal exemplar än vad som är nödvändigt.

En myndighet har möjlighet att i särskilda föreskrifter medge undantag från dessa bestämmelser för hemliga handlingar vars innebörd vid ett röjande endast kan antas medföra ringa men för rikets säkerhet.

3.1.2 Kopiering och utdrag

3 kap. 7–8, 24 §§ RPSFS 2010:03

Den som framställer en kopia eller ett utdrag av en allmän hemlig handling ska se till att en anteckning om detta görs, antingen på handlingen eller i en särskild förteckning. Där ska det också antecknas till vem som kopian eller utdraget har lämnats. På ett utdrag ur en allmän hemlig handling ska det även antecknas från vilken handling utdraget har gjorts. Kopian eller utdraget ska numreras enligt avsnitt 3.1.1.

Den huvudsakliga anledningen till detta förfarande vid kopiering och utdrag är att det i efterhand ska gå att spåra vem som har tagit del av hemliga uppgifter. Så kallade svartkopior får alltså inte förekomma.

Kopiering och utdrag ur en hemlig handling bör endast göras i myndighetens lokaler och enligt en rutin som försvårar obehörig kopiering. Kopiatorn bör därför inte ha något lagringsmedium (exempelvis i form av en hårddisk) om myndigheten inte har kontroll över kopiatorerna.

Rutiner för kopiering eller utdrag ur en icke allmän hemlig handling bör anges i myndighetens särskilda föreskrifter.

Kopia av eller utdrag ur en kvalificerat hemlig handling får endast göras efter tillstånd av myndighetens chef eller motsvarande organ. Behörighet att ge ett sådant tillstånd får överlåtas till en annan person inom myndigheten.

En myndighet har möjlighet att i särskilda föreskrifter medge undantag från dessa bestämmelser för hemliga handlingar vars innebörd vid ett

röjande endast kan antas medföra ringa men för rikets säkerhet.

3.2 KVITTERING

3 kap. 9–10, 24 §§ RPSFS 2010:03

Den som tar emot en allmän hemlig handling ska kvittera mottagandet i register eller liggare, eller på särskilt kvitto. Kvittering ska ske genom namnteckning och namnförtydligande. Kvittensen ska bevaras hos myndigheten i minst 10 år.

En icke allmän hemlig handling ska först på begäran kvitteras av mottagaren på samma sätt som för en allmän hemlig handling.

Kvittensregeln gäller inte för den personal som har till uppgift att registrera, arkivera, kopiera eller förstöra hemliga handlingar om inte kvittens begärs av den som lämnar handlingen.

Den angivna ordningen med kvittering får ses som en skyddsåtgärd dels för att skydda den anställde, dels som ett skydd för myndighetens hemliga handlingar.

Det är viktigt att kvittering görs på det ovan beskrivna sättet. Det får alltså inte förekomma att kvittering sker på den hemliga handling som kvitteringen avser. En sådan ordning skulle nämligen innebära att man saknar kännedom om var handlingen finns under den tid som handlingen är utlånad. Om handlingen senare skulle förstöras så utplånas dessutom möjligheterna att i efterhand utreda vem som har haft tillgång till handlingen.

Anledningen till att kvittering ska ske genom att mottagaren skriver sin namnteckning med namnförtydligande är att det aldrig ska råda någon tvekan om vem som har kvitterat en hemlig handling.

Hemliga uppgifter som delges någon muntligt eller genom visning är naturligtvis lika skyddsvärda som dokumenterade hemliga uppgifter. I det fall hemliga uppgifter delges någon muntligen eller genom visning bör det göras en kvittering eller anteckning om detta.

Det bör uppmärksammas att kvittot kan bli en allmän handling men däremot inte själva handlingen. Inom en och samma myndighet kan behöriga tjänstemän emellan hantera en icke allmän hemlig handling och förvara den inom myndigheten utan att kvittering behöver ske.

På myndigheter bör det finnas särskilda föreskrifter som anger hur ett återlämnande av en kvitterad hemlig handling ska hanteras.

En myndighet har möjlighet att i särskilda föreskrifter medge undantag från dessa bestämmelser för hemliga handlingar vars innebörd vid ett röjande endast kan antas medföra ringa men för rikets säkerhet.

En kvalificerat hemlig handling ska kvitteras med namnteckning och namnförtydligande på ett särskilt kvitto, som ska upprättas i minst två exemplar. Kvittot ska förvaras hos myndigheten i 25 år. Detta gäller även vid ett återlämnande. Lämnas uppgifter i en kvalificerat hemlig handling muntligen eller genom visning ska det göras en kvittering eller anteckning om detta. En myndighet ska fastställa rutiner för hur en sådan kvittering eller anteckning ska ske.

Dokumentation
Rutin kring kvittering av kvalificerat hemlig handling

3.3 FÖRVARING

3 kap. 11–14, 24 §§ RPSFS 2010:03

3.3.1 Allmänt om förvaringsutrymmen

Det är lämpligt att den som ansvarar för hemliga handlingar förfogar över ett eget förvaringsutrymme för dessa dokument. Vid val av förvaringsutrymme måste hänsyn tas till den allmänna skyddsnivån, platsen för förvaringsutrymmet samt vilket skydd som tillträdesbegränsningen ger i den lokal där förvaringsutrymmet ska placeras. I en del fall måste förvaringsutrymmet förses med larmanordning. Även bevakning kan komma ifråga, vilket bör framgå av myndighetens säkerhetsanalys.

Skrymmande hemliga föremål, som på grund av sitt omfång inte kan förvaras i ett fabrikstillverkat säkerhetsskåp med lägsta säkerhetsnivå, måste skyddas på annat lämpligt sätt. Detta kan ske genom att förvaringsutrymmet för sådan materiel byggs om så att det motsvarar samma förvaringskrav som för hemlig handling. Vid en ombyggnad kan det vara viktigt att beakta Riksarkivets bestämmelser för arkiv. Ett annat alternativ kan vara övertäckning eller sektionering av den lokal i vilken

föremålet förvaras och hålls under omedelbar uppsikt. Det är då viktigt att lokalen har ett godtagbart skydd från säkerhetsskyddssynpunkt.

Förvaringen av hemliga handlingar och hemlig materiel kan delas in i varaktig och tillfällig förvaring. Med tillfällig förvaring menas sådan förvaring som förekommer exempelvis vid ett kortare arbetsuppehåll och där undantag i vissa fall kan göras från det krav som annars gäller för förvaringen (se avsnitt 3.3.2).

3.3.2 Förvaringskrav

Myndigheten ska förvara hemliga handlingar på ett sådant sätt att en obehörig inte kan komma åt handlingarna. Sigill, assuranstejp, plomberingstänger och präglingsanordningar för sigillsvets ska förvaras på samma sätt som hemliga handlingar. Motsvarande ordning gäller också för datamedier, färgband och färgkassetter om de har använts vid arbete med hemliga uppgifter. Ytterligare information om hantering av hemliga uppgifter i IT-miljö finns i kapitel 4.

Hemliga handlingar ska därför förvaras i ett förvaringsutrymme med en lägsta skyddsnivå motsvarande säkerhetsskåp SS 3492.

Ett förvaringsutrymme i klass SS 3493 uppfyller kraven på SS 3492 samt brandsäkerhetskraven enligt normen NT Fire 017.

Förvaras ett flertal kvalificerat hemliga handlingar på en myndighet rekommenderas att man använder förvaringsutrymmen i lägst klass SS 3150 med den europeiska beteckningen EN 1143-1 grade 3. För att ytterligare förstärka skyddet kan bevakning tillkomma. Det är alldeles nödvändigt att myndighetens egen säkerhetsanalys ger upplysning om vilka skyddsbehov som föreligger.

Myndigheten ska ha ett diarium eller något annat register som visar var en allmän hemlig handling förvaras och om en sådan handling har förkommit eller gallrats.

Myndigheten får meddela särskilda föreskrifter som reglerar hur tillfällig respektive varaktig förvaring av hemliga handlingar ska ske hos myndigheten. Föreskrifter om tillfällig förvaring kan bland annat medge undantag vid kortare arbetsuppehåll om den hemliga handlingen i stället förvaras i ett låst rum, under förutsättning att rummet är låst med ett lås som ger den ansvarige exklusivt tillträde till rummet. Exempelvis kan en tjänsteman vid ett arbetsuppehåll tillåtas förvara en hemlig handling på sitt tjänsterum, om rummet är låst och ingen annan än tjänstemannen kan få tillträde till rummet under den tid som handlingen förvaras där. Myndighetens föreskrifter kan även klarlägga ansvarsförhållanden för personer som av praktiska skäl måste använda samma förvaringsutrymme. I sistnämnda fall måste det regleras vem som har ansvaret för nyckeln eller koden, villkor för överlämnande av nyckeln eller delgivning av koden, handlingarnas ordnande i förvaringsutrymmet, kvitteringssystem, arbetsställen och närvaroliggare.

En myndighet har möjlighet att i särskilda föreskrifter medge undantag från kravet på förvaringsregister och lägsta skyddsnivå SS 3492 för förvaring av hemliga handlingar vars innebörd vid ett röjande endast kan antas medföra ringa men för rikets säkerhet.

En kvalificerat hemlig handling ska förvaras av myndighetens chef eller motsvarande organ. Förvaringen får emellertid överlåtas till annan inom myndigheten. Det är lämpligt att hålla kvalificerat hemliga handlingar åtskilda från andra handlingar, till exempel i ett låst innerfack i säkerhetsskåpet. För kvalificerat hemliga handlingar kan det vara lämpligt att förse säkerhetsskåpen med larm. Det är inte möjligt att göra undantag från förvaringskraven när det gäller kvalificerat hemliga handlingar.

3.4 MEDFÖRANDE AV HEMLIGA HANDLINGAR UTANFÖR MYNDIGHETENS LOKALER

11 § säkerhetsskyddsförordningen
3 kap. 15, 23 §§ RPSFS 2010:03

Hemliga handlingar som tas med från ordinarie arbetsplats i myndighetens lokaler ska hållas under omedelbar uppsikt eller förvaras enligt den säkerhetsskyddsnivå som gäller hos myndigheten. Kvalificerat hemliga handlingar får överhuvudtaget inte tas med från arbetsplatsen utan tillstånd av myndighetens chef eller motsvarande organ. Behörigheten att ge sådant tillstånd får överlåtas till en annan person inom myndigheten. Ovanstående gäller även vid tjänsteresa utomlands. Se även avsnitt 3.7, sista stycket.

Förvaringsmöjligheterna är av naturliga skäl ofta begränsade vid resor. Därför bör endast absolut nödvändiga handlingar medföras. En bärbar dator, portfölj eller en väska som innehåller en hemlig handling får inte lämnas obevakad i till exempel bil, tågkupé eller annat transportmedel. Inte heller

får portföljen eller väskan överlämnas till effektförvaring på exempelvis järnvägsstation, flygplats eller hotell, eller låsas in i förvaringsbox.

Om en hemlig handling hanteras på ett vårdslöst sätt och en hemlig uppgift röjs, kan straffansvar enligt 19 kap. 9 § brottsbalken för vårdslöshet med hemlig uppgift komma i fråga.

3.5 INVENTERING

9–10, 44 §§ säkerhetsskyddsförordningen
3 kap. 16, 22, 24 §§ RPSFS 2010:03

Kvalificerat hemliga handlingar ska inventeras minst en gång per år. Andra hemliga handlingar ska inventeras i den omfattning som myndigheten själv har bestämt i sina särskilda föreskrifter. Protokoll ska föras över inventeringen av allmänna hemliga handlingar.

Vid myndighetens ställningstagande till hur ofta denna inventering ska ske, bör myndigheten beakta att preskriptionstiden för brottet vårdslöshet med hemlig uppgift är två år. Om myndigheten inventerar sina hemliga handlingar alltför sällan kan det få till följd att angivna straffstadgande förlorar i betydelse. Det är därför lämpligt att myndigheten inventerar alla sina hemliga handlingar minst en gång per år.

Om en hemlig uppgift kan ha röjts ska detta skyndsamt anmälas till Säkerhetspolisen, om röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa.

En myndighet har möjlighet att i särskilda föreskrifter medge undantag från kravet på protokoll över inventeringen när det gäller hemliga handlingar vars innebörd vid ett röjande endast kan antas medföra ringa men för rikets säkerhet.

3.6 FÖRSTÖRING AV HEMLIGA HANDLINGAR I SKRIFT ELLER BILD

3 kap. 18, 24 §§ RPSFS 2010:03

Hemliga handlingar eller materiel som innehåller hemliga uppgifter ska förstöras på ett sådant sätt att åtkomst och återskapande av uppgifterna omöjliggörs. Förstöringen ska dokumenteras.

Förstöring bör ske maskinellt eller genom bränning. Det kan vara svårt och tidsödande att erhålla fullständig förbränning, bland annat eftersom egen ansvarig personal måste delta under hela förbränningsprocessen och utföra kontroller. För maskinell förstöring används främst så kallade dokumentförstörare. Dessa är ofta av golvmodell med spånavskärare. En dokumentförstörare vars spånavskärare ger spån med 15 mm längd och max 1,2 mm bredd, alternativt 2 x 2 mm eller mindre, kan förordas beträffande pappersdokument. Vid förstöring av en handling med komprimerad text, till exempel mikrofiche, är bränning att föredra.

Utöver dokumentförstörare finns så kallade specialdestruktörer och centraldestruktörer. Specialdestruktörer används för förstöring av disketter, bandkassetter och liknande föremål. Centraldestruktörer är större maskiner som ofta har roterande knivar och kan vara lämpliga att använda då man ska förstöra stora mängder handlingar samtidigt. Egen personell övervakning bör finnas med under hela förstöringsprocessen.

Det finns destruktionsanläggningar i Sverige som förstör handlingar och annat som innehåller hemliga uppgifter. Dessa kan utnyttjas, men egen ansvarig personal måste i så fall vara med under hela destrueringen och utföra kontroller.

Vid förstöring av signalskyddsnycklar ska FFS 2005:2 följas.

En myndighet har möjlighet att i särskilda föreskrifter medge undantag från dessa bestämmelser för hemliga handlingar vars innebörd vid ett röjande endast kan antas medföra ringa men för rikets säkerhet.

Dokumentation
Förstöringsrapport

3.7 ARBETSRUTINER VID DISTRIBUTION AV HEMLIGA HANDLINGAR

11 § säkerhetsskyddsförordningen
3 kap. 19–24 §§ RPSFS 2010:03

I allmänhet måste hemliga handlingar distribueras på ett sådant sätt att obehöriga hindras att få del av uppgifterna. Som framgår nedan får hemliga handlingar inte sändas som vanliga postförsändelser, det vill säga som ett sedvanligt brev eller paket.

När en försändelse med en hemlig handling sänds inom Sverige ska den sändas som värdepost, rekommenderad post eller motsvarande och med en av myndigheten godkänd distributör.

Då en hemlig handling sänds bör givetvis emballaget vara så beskaffat att det är omöjligt att ta del av uppgifterna i handlingen utan att bryta emballaget. Det måste även gå att se om någon har brutit emballaget. Förslagsvis kan man använda ett så kallat säkerhetskuvert av polyeten. Dessa är lätta att försluta på ett säkert sätt och är dessutom individuellt numrerade. Säkerhetskuvert, utprovade av Säkerhetspolisen, kan beställas hos Försvarets bok- och blankettförråd,* nr M 7102-122740 för VÄRDE samt nr M 7102-122730 för REK. Av försändelsens omslag, adresskort, postbok eller dylikt bör det av naturliga skäl inte framgå att det är fråga om en hemlig handling. En hemlig handling som sänds till en annan myndighet för exempelvis yttrande eller annat liknande förfarande kan förses med en anteckning om att den ska återställas inom en viss tid. Hemlig arbetsmateriel som får förstöras av mottagaren bör förses med en anteckning om detta.

Den som hämtar en försändelse hos en distributör ska kontrollera att försändelsen stämmer överens med kvittenslistan och att försändelsen är oskadad. Vid skada ska den som hämtar försändelsen begära att distributören gör en anteckning om skadans beskaffenhet. Därutöver ska samma person anmäla skadan till avsändaren.

Den som mottar försändelsen ska kontrollera att den är oskadad och att innehållet överensstämmer med uppgifterna i huvudhandlingen, missivet eller sändlistan. I det fall försändelsen är skadad eller uppgifterna inte stämmer överens, ska avsändaren underrättas om detta. Görs ingen anmärkning ska eventuella sigillavtryck förstöras.

Om det uppkommer en misstanke om att en obehörig har tagit eller försökt ta del av innehållet i en försändelse med hemliga uppgifter, kan samma förfarande som när en hemlig uppgift kan ha röjts bli tillämpligt (se avsnitt 3.5).

Myndigheten bör i sina särskilda föreskrifter reglera frågan om hur hemliga handlingar ska sändas och tas emot inom myndigheten.

En myndighet har möjlighet att i särskilda föreskrifter medge undantag från bestämmelser om hur försändelser som hämtas och tas emot ska kontrolleras när det gäller hemliga handlingar vars innebörd vid ett röjande endast kan antas medföra ringa men för rikets säkerhet.

Om hemliga handlingar sänds till utlandet ska Utrikesdepartementets kurirförbindelse anlitas. Skälet till detta är att kurirförbindelsen anses erbjuda ett högre mått av säkerhetsskydd för handlingarna än någon annan transportförbindelse. Säkerhetspolisen har emellertid möjlighet för sitt tillsynsområde att besluta om undantag från kravet att anlita Utrikesdepartementets kurirförbindelse. I RPSFS 2010:03 medges att en myndighet får besluta att personal som är behörig att ta del av hemliga uppgifter får ta med försändelser i skrift eller bild till utlandet.

3.8 UNDANTAG

3 kap. 24 § RPSFS 2010:03

Undantagsbestämmelserna i 3 kap. 24 § RPSFS 2010:03 har införts för att underlätta hanteringen av hemliga handlingar i skrift eller bild vars röjande endast kan antas medföra ringa men för rikets säkerhet. Endast myndigheter med särskilda säkerhetsföreskrifter kan föreskriva om vilka av undantagen som gäller för den egna myndigheten. Mottagare av en handling vars röjande endast kan anses medföra ringa men ska naturligtvis göra en egen bedömning av vilken säkerhetsskyddsnivå som handlingen ska hanteras i på den egna myndigheten.

För att dra nytta av undantagen måste myndigheten redan vid upprättandet av en handling göra en så kallad förtida menbedömning, det vill säga bedöma eventuella skadeverkningar om innehållet i handlingen röjs. I de särskilda föreskrifterna bör det finnas rutiner för hemligbeteckning.

Handlingar vars röjande endast kan antas medföra ringa men för rikets säkerhet kan utöver hemligbeteckningen även förses med en anteckning om ringa men, exempelvis RM på förstasidan i anslutning till hemligbeteckningen.

* Tfn 0589-810 20, fax 0589-810 21 eller e-post fbf@saabgroup.com (2009-09-21).

4 Informationssäkerhet för hemliga uppgifter i IT-system

9 § säkerhetsskyddslagen
9–13 §§ säkerhetsskyddsförordningen
4 kap. RPSFS 2010:03

Utformningen av säkerhetsskyddslagstiftningen medför i dagsläget att det inte ställs samma krav på säkerhetsskydd för system som hanterar hemliga uppgifter i IT-miljö som på ett IT-system som behöver skyddas mot terrorism. Vilken slags information som hanteras i ett IT-system är alltså avgörande för skyddsbehovet i systemet. Den skada som informationen kan orsaka om den kommer i orätta händer bör beaktas när det gäller att bestämma skyddsvärdet för systemet. Samhällets allt större beroende av IT-system gör det nödvändigt att bedöma vilka åtgärder som behövs för att säkerställa hög säkerhet, inklusive tillgänglighet och riktighet, hos samhällskritiska och samhällsviktiga system.

Syftet med detta kapitel är främst att belysa vilka krav som säkerhetsskyddslagstiftningen ställer på myndigheterna när det gäller inrättande och utnyttjande av IT-system.* Bestämmelserna om informationssäkerhet för hemliga uppgifter behandlar inte utformningen av tekniska lösningar i IT-system. Detta avsnitt kommer därför i första hand att presentera kraven på informationssäkerhet och i andra hand resonera kring tekniska lösningar.

Utvecklingen i samhället har gått mot att dokument och annan viktig information som tidigare har lagrats i pappersform nu hanteras i IT-system. IT-system möjliggör också alltmer utvecklade tjänster som samhället i ökande utsträckning förväntar sig ska fungera. Det är därför viktigt att skydda informationen och tillgängligheten i systemen mot obehörig åtkomst eller påverkan.

* Med IT-system avses system som använder sig av informationsteknologi. Detta inkluderar även exempelvis handdatorer, mobiltelefoner och nätverksutrustning.

4.1 ÖVERGRIPANDE KRAV PÅ IT-SYSTEM

9 § säkerhetsskyddslagen
12–13 §§ säkerhetsskyddsförordningen
4 kap. 2–22 §§ RPSFS 2010:03

4.1.1 Allmänt om säkerhetsskyddet i IT-system

4 kap. 2–4, 8 §§ RPSFS 2010:03

Hemliga uppgifter och kvalificerat hemliga uppgifter får endast hanteras i IT-system som har godkänts för sådan hantering av den myndighet för vars verksamhet systemet har inrättats.

För system som är avsedda för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism krävs att mål och riktlinjer för IT-säkerheten dokumenteras. Klara instruktioner för användare om hur de ska använda systemet är nödvändiga för att det inte ska råda oklarheter kring användningen av systemet. Vidare krävs instruktioner för de administratörer som förvaltar och underhåller IT-systemet. Denna dokumentation ska fastställas av myndighetens chef eller motsvarande organ.

Myndigheten ansvarar för IT-systemets säkerhet under hela dess livscykel och ska svara för att ett betryggande säkerhetsskydd upprätthålls i och kring systemet, från dess anskaffning till dess avveckling.

En myndighet som överväger att skaffa, använda, utveckla eller förändra ett IT-system ska göra en översiktlig analys av vilket säkerhetsskydd systemet kommer att kräva.

Dokumentation
Mål och riktlinjer för systemets IT-säkerhet
Instruktioner för användning, förvaltning och drift av IT-systemet

4.1.2 Risk- och sårbarhetsanalys av IT-system

4 kap. 5, 7, 22 §§ RPSFS 2010:03

En myndighet som beslutar att anskaffa, använda, utveckla eller förändra ett IT-system som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism ska noga analysera de säkerhetsrisker och de sårbarheter som finns i och kring systemet. Analysen ska inkludera behovet av skydd mot röjande signaler (RÖS). Ytterligare information om röjande signaler finns i avsnitt 4.2.7.

Denna risk- och sårbarhetsanalys ska resultera i en sammanställning över de åtgärder som ska genomföras för att säkerhetsskyddet ska vara godtagbart. I analysen är myndigheten även skyldig att göra en bedömning av säkerhetsskyddsnivån av såväl de enskilda uppgifterna som den totala informationsmängden som systemet är tänkt att hantera. Analysen ska dokumenteras. Analysen bör inkludera de konsekvenser som kan uppstå om uppgifterna i systemet röjs för obehöriga, inte är riktiga, inte är spårbara eller inte är tillgängliga.

Detta ska tillämpas även innan en myndighet upplåter ett IT-system till en annan myndighet, en annan stat eller en mellanfolklig organisation.

Dokumentation
Risk- och sårbarhetsanalys
Sammanställning över skyddsåtgärder

4.1.3 Samråd med Säkerhetspolisen

12 § första stycket säkerhetsskyddsförordningen

Innan en myndighet beslutar sig för att inrätta ett IT-system för hantering av sådana hemliga uppgifter som var för sig eller sammanställda kan skada totalförsvaret, ska samråd ske med Försvarsmakten och i vissa fall med Säkerhetspolisen. När det gäller hemliga uppgifter i övrigt ska samråd ske med Säkerhetspolisen.

4.1.4 Att avstå från eller begränsa ett IT-system

4 kap. 6 § RPSFS 2010:03

Kan erforderligt säkerhetsskydd för IT-systemet inte uppnås ska myndigheten avstå från IT-systemet eller begränsa dess innehåll. Det är viktigt att dokumentera den rutin som i ett sådant fall kommer att ersätta det tänkta IT-systemet för att tydliggöra syftet med rutinen. Rutinen blir då också kontrollfunktion för hantering av hemliga handlingar så att detta inte sker på ett felaktigt sätt.

4.1.5 IT-system som används av annan myndighet med flera

4 kap. 10 § RPSFS 2010:03

En myndighet kan förvalta ett IT-system som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism och som är avsett att användas av en annan myndighet, en annan stat eller en mellanfolklig organisation. Om så är fallet ska myndigheten upprätta en dokumentation avseende IT-systemets drift, förvaltning och säkerhet.

Dokumentation
Driftsdokumentation
Förvaltningsdokumentation
Säkerhetsdokumentation

4.1.6 Driftgodkännande

12 § tredje stycket säkerhetsskyddsförordningen
4 kap. 11 § RPSFS 2010:03

IT-system som är avsett för behandling av hemliga uppgifter och som kommer att användas av flera personer ska godkännas av den för vars verksamhet systemet har inrättats. I samband med godkännandet ska även IT-systemets säkerhet granskas, och då särskilt eventuell samverkan med andra system. Granskningen underlättas givetvis om myndigheten har följt bestämmelserna i föreskrifterna angående analys och dokumentation av säkerhetsrisker och sårbarheter inför och vid anskaffning, användning, utveckling och förändring av systemet. Den myndighet som inrättar systemet ska dokumentera granskningen och driftgodkännandet.

För att säkerställa ett gott säkerhetsskydd för system som behöver skyddas mot terrorism rekommenderar Säkerhetspolisen normalt att processen med driftgodkännande och granskning av säkerheten även följs för dessa system.

Dokumentation
Beslut om godkännande av drift
Resultat av granskning av IT-systemets säkerhet

4.1.7 Systemsäkerhetsansvarig

4 kap. 13 § RPSFS 2010:03

För IT-system där behandling av hemliga uppgifter sker eller som särskilt behöver skyddas mot terrorism ska det finnas en av myndighetens chef eller motsvarande organ utsedd person som ansvarar för säkerheten i systemet.

Den systemsäkerhetsansvariges arbetsuppgifter varierar givetvis beroende på systemets storlek, komplexitet, antal användare och andra faktorer. Vad gäller ansvaret för arbetsuppgifter bör åtminstone den systemsäkerhetsansvarige se till att:

- Nödvändiga analyser för IT-systemet genomförs
- Säkerhetsrelaterad dokumentation upprättas och underhålls
- Säkerhetsgranskningar av IT-systemet genomförs löpande
- Beslut tas gällande vilka tekniska och administrativa åtgärder som behövs för att säkerställa systemets säkerhet
- Ovanstående beslut genomförs i praktiken
- Säkerhetsincidenter inrapporteras och följs upp
- En kontinuitetsplan för systemet upprättas och underhålls.

Det är olämpligt att arbetsuppgiften utförs av myndighetens IT-chef, eller denne underställd tekniker, eftersom man kan hamna i en konfliktsituation då den utsedde i princip blir både beställare och mottagare. Kostnader för säkerhetsskyddsåtgärder skulle komma att ställas mot andra mål hos myndigheten. Det bör därför finnas en särskild säkerhetsorganisation som hanterar IT-säkerheten.

4.2 SKYDD AV HEMLIGA UPPGIFTER I IT-SYSTEM

9 § säkerhetsskyddslagen
12–13 §§ säkerhetsskyddsförordningen
2 kap. 2 §, 4 kap. 12–26 §§ RPSFS 2010:03

4.2.1 Skydd av kommunikation av hemliga uppgifter

13 § säkerhetsskyddsförordningen
2 kap. 2 §, 4 kap. 12 § RPSFS 2010:03

När hemliga uppgifter ska sändas i ett datanätverk utanför deras kontroll ska myndigheten, innan sändningen äger rum, förvissa sig om att det finns en fullgod informationssäkerhet för uppgifterna i det externa nätverket. Hemliga uppgifter får endast krypteras med kryptosystem som har godkänts av Försvarsmakten.

Det svenska myndighetsgemensamma nätverket SGSI – Swedish Government Secure Intranet – medger endast överföring upp till och med säkerhetsskyddsnivå EU-Restricted.*

En okrypterad dataförbindelse får användas för hemliga uppgifter inom ett område eller en lokal som disponeras av en myndighet först sedan myndigheten har vidtagit betryggande åtgärder mot obehörig avlyssning av dataförbindelsen. Ett exempel på en sådan åtgärd är inspekterbar eller larmad fiberkabel (även kopplingspunkterna måste skyddas) inom ett inhägnat och bevakat område.

4.2.2 Behörighetskontroll

12 § andra stycket säkerhetsskyddsförordningen
4 kap. 14–15 §§ RPSFS 2010:03

Ett IT-system som är avsett att hantera hemliga uppgifter och som kommer att användas av flera personer ska vara åtgärdat med tekniska och/eller administrativa verktyg för:

- Identifiering av användaren
- Verifiering av den föregivna identiteten
- Styrning av användarens åtkomsträttigheter till systemet
- Registrering av användarens aktiviteter.

Detta bör även tillämpas i fråga om IT-system som särskilt behöver skyddas mot terrorism.

Avsikten med behörighetskontroll är att enbart behöriga användare ska få tillgång till systemet. Tillförlitlig identifiering av användare är en förutsättning för att med säkerhet kunna spåra en användares aktiviteter i systemet genom säkerhetsloggar, något som är särskilt viktigt i samband med incidenter. I sådana fall utgör en säker identifiering också en trygghet för användarna. Ett IT-system avsett för behandling av hemliga uppgifter eller i behov av skydd mot terrorism och som är avsett att användas av flera personer, bör förses med ett förstärkt inloggningsskydd. Aktiva kort, säkerhetsdosor och biometriska verifieringssystem är exempel på förstärkt inloggningsskydd.

Kod, lösenord eller motsvarande funktioner som används för att få tillgång till IT-system avsedda för behandling av hemliga uppgifter ska ha ett säkerhetsskydd som motsvarar den högsta säkerhetsskyddsnivån för sådan information. Kod, lösenord eller motsvarande till IT-system som behöver särskilt

* Myndigheten för samhällsskydd och beredskap (MSB) är systemägare.

skydd mot terrorism ska förvaras så att inte obehöriga medges åtkomst.

4.2.3 Säkerhetsloggning

12 § andra stycket säkerhetsskyddsförordningen
4 kap. 16–18 §§ RPSFS 2010:03

Med säkerhetsloggning avses manuell eller automatisk registrering av händelser som är av betydelse för säkerheten i eller kring ett IT-system. Exempel på manuell registrering är en kvittenslista där nyttjande av systemet registreras. Begreppet spårbarhet innebär att verksamheten och tillhörande system ska innehålla funktioner som gör det möjligt att entydigt härleda utförda operationer till enskilda individer.

I ett IT-system avsett för behandling av hemliga uppgifter och som används av flera personer ska loggning ske av:
- Användaridentitet
- Datum och tidpunkt för in- och utloggning
- Sådana användaraktiviteter som i övrigt är av betydelse för säkerheten i systemet.

Exempel på sådana användaraktiviteter är:
- Förändringar i systemets tid, datum och tidszon
- Förändringar i logginställningarna (det vill säga vad som loggas)
- Radering eller modifiering av loggposter
- Skapande eller borttagande av konton i systemet
- Förändringar av kontons behörighet
- In- och utloggningar av användare
- Åtkomst (läsning, modifiering eller radering) till kritiska och/eller hemliga objekt (filer, registerposter, etc.).

Motsvarande säkerhetsloggning bör även tillämpas i fråga om IT-system som behöver särskilt skydd mot terrorism.

En myndighet ska besluta om och dokumentera:
- Hur ofta säkerhetsloggarna ska analyseras
- Vad som ska analyseras
- Vem som ansvarar för att analysen görs
- Hur länge säkerhetsloggar ska sparas.

Dokumentation
Dokumentation över logghantering

4.2.4 Skydd mot skadlig kod

4 kap. 19–20 §§ RPSFS 2010:03

Skadlig kod är ett samlingsnamn för olika typer av programvaror med illasinnade funktioner. Det engelska begreppet är malicious software eller kortformen malware. I begreppet skadlig kod ingår bland annat virus, mask, trojan och annonsprogram (adware).

Skydd mot skadlig kod syftar till att skydda IT-systemet mot programkod som otillbörligt är tänkt att användas för att ändra, röja, förstöra eller avlyssna uppgifter, filer eller program som lagras eller kommuniceras till eller från IT-systemet. Ett IT-system som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism, ska ha ett av myndigheten godkänt skydd mot skadlig kod.

Det vanligaste skyddet mot skadlig kod är antivirusprogramvara. Då det hela tiden framställs nya typer av skadlig kod är det väsentligt att antivirusprogramvaran uppdateras löpande. Uppdatering av antivirusprogramvara ska, i ett system som hanterar hemliga uppgifter, inte göras genom att tillfälligt ansluta systemet mot internet. I stället kan ett annat IT-system användas för hemtagning av uppdateringar som sedan på ett kontrollerat sätt förs över till det system som hanterar hemliga uppgifter.

Andra skydd mot skadlig kod kan vara integritetskontrollsystem, olika typer av behörighetsbegränsningar och system för programexekveringskontroll.

Rutiner som specificerar hur uppdatering av skydd mot skadlig kod går till ska dokumenteras. Vidare bör rutiner för att kontrollera att skyddet mot skadlig kod är aktivt tas fram och dokumenteras. Vid ett funktionstest kan bland annat testviruset EICAR användas.

Dokumentation
Rutiner för uppdatering av skydd mot skadlig kod

4.2.5 Intrångsdetektering och skydd mot intrång

4 kap. 21 § RPSFS 2010:03

Med intrångsdetektering menas administrativa och tekniska åtgärder som vidtas för att upptäcka intrång eller försök eller förberedelse till intrång. Med intrångsskydd avses administrativa och tekniska åtgärder som vidtas för att skydda IT-system mot obehörig åtkomst från ett elektroniskt kommunikationsnät. Med elektroniskt kommunikationsnät avses exempelvis förbindelser med andra myndigheter eller samarbetspartners, samt internetanslutning.

Ett IT-system som är avsett för behandling av hemliga uppgifter eller som kräver särskilt skydd mot terrorism och som kommunicerar med andra IT-system ska vara försett med ett av myndigheten godkänt intrångsskydd och av myndigheten godkända funktioner för intrångsdetektering. Detta kan bestå av bland annat brandväggar och intrångsdetekteringssystem.

Det finns inget krav på att ett IT-system som används för behandling av hemliga uppgifter och vars röjande endast kan antas medföra ringa men för rikets säkerhet ska förses med funktioner för intrångsdetektering. Detta bör dock övervägas.

En helt fristående dator som inte är ansluten till andra system bör vara försedd med ett antivirusprogram eftersom anslutning av extern minnesmedia, såsom exempelvis USB-minne eller extern hårddisk, kan innebära risk för smitta av skadlig kod.

4.2.6 Skydd mot obehörig avlyssning

13 § säkerhetsskyddsförordningen
4 kap. 22 § RPSFS 2010:03

Data skickas allt oftare trådlöst, vilket medför ytterligare säkerhetsrisker eftersom radiovågor kan passera genom väggar och på så sätt även nå platser som man inte har kontroll över. Trådlös teknik, exempelvis WLAN och bluetooth, bör därför undvikas vid arbete med hemliga uppgifter som rör rikets säkerhet.

Ett IT-system som är avsett för behandling av hemliga uppgifter ska vara försett med ett betryggande skydd mot obehörig avlyssning. Skyddet i detta fall innebär oftast att myndigheten avstår från att använda utrustning och teknik som kan möjliggöra obehörig avlyssning.

4.2.7 Skydd mot röjande signaler (RÖS)

4 kap. 22 § RPSFS 2010:03

Med röjande signaler – RÖS – avses de inte önskvärda elektromagnetiska eller akustiska signaler som alstras i till exempel informationsbehandlande utrustningar, och som kan uppfångas med olika typer av mottagare och användas för underrättelseverksamhet. I vissa fall kan uppfångande av RÖS vara det enda sättet att skaffa information från ett i övrigt säkerhetsmässigt fullgott system.

För att uppnå ett fullgott skydd mot avlyssning av RÖS från en viss utrustning krävs i allmänhet att utrustningen antingen konstrueras på ett visst sätt eller placeras i ett RÖS-skyddat rum. Ett RÖS-skyddat rum fungerar enligt principen om Faradays bur, där alla elektromagnetiska fält avskärmas genom ett elektriskt ledande hölje. Skyddet kan även bestå av speciellt avskärmade datorer och bildskärmar som minimerar möjligheten att uppfånga signaler. Vissa myndigheter bestyckar exempelvis med RÖS-skydd de bärbara datorer som oundvikligen måste användas utanför myndigheten och som är avsedda att hantera hemlig information. Även med enkla åtgärder såsom placering av IT-system på mindre exponerade platser kan ibland goda resultat uppnås.

IT-system som regelbundet bearbetar kvalificerat hemlig information bör alltid hanteras i RÖS-skyddad utrustning eller inom RÖS-skyddad lokal.

Behovet av skydd mot RÖS i ett IT-system som är avsett för behandling av hemliga uppgifter ska analyseras. Resultatet av analysen tillsammans med genomförda åtgärder för RÖS-skyddet av systemet ska dokumenteras.

Dokumentation
Risk- och sårbarhetsanalys (där behovet av skydd mot RÖS ingår; se avsnitt 4.1.2)

4.2.8 Incidenthantering

10 § säkerhetsskyddsförordningen
4 kap. 23 § RPSFS 2010:03

Med incidenter avses uppsåtliga eller oavsiktliga händelser som medför störningar i ett IT-systems konfidentialitet, riktighet eller tillgänglighet. Incidenter kan till exempel vara dataintrång och/eller olovlig avlyssning, intrångs- och avlyssningsförsök, stöld och manipulation av utrustning, kablage och lagringsmedia samt förekomst och spridning av skadlig kod.

Säkerhetspolisen är den myndighet som i första hand ska kontaktas vid anmälning av incidenter som rör IT-system som används för hantering av hemliga uppgifter.

En viktig aspekt av incidenthantering är att, så långt det går, planera och förbereda för incidenter i förväg. Att till exempel identifiera och testa programvaror för incidentutredning innan snarare än under en incident rekommenderas.

En myndighet ska fastställa och dokumentera rutiner för hantering, rapportering och uppföljning av incidenter av betydelse för säkerheten i eller kring

ett IT-system som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism.

Dokumentation
Incidenthanteringsrutiner

4.2.9 Säkerhetskopiering

4 kap. 24–25 §§ RPSFS 2010:03

Syftet med säkerhetskopieringen är att säkerställa tillgång till uppgifter om en incident skulle inträffa. Vid säkerhetskopiering i ett IT-system som hanterar stora mängder hemliga uppgifter överförs data ibland till ett litet, bärbart lagringsmedium vilket kräver särskild uppmärksamhet vid den fortsatta hanteringen. Säkerhetskopiorna blir i vissa fall att betrakta som kvalificerat hemliga handlingar på grund av den sammanlagda mängden hemlig information de innehåller.

Säkerhetskopiering ska ske av uppgifter i ett IT-system som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism. Myndigheten ska regelbundet kontrollera att informationen på säkerhetskopiorna går att återskapa. En säkerhetskopia ska förvaras avskilt från den plats där IT-systemet finns.

4.2.10 Kontinuitetsplan

4 kap. 26 § RPSFS 2010:03

En kontinuitetsplan syftar till att minska skadan vid incidenter och katastrofer. För att reservrutiner ska fungera vid incidenter är det viktigt att dessa testas kontinuerligt och att all berörd personal deltar i sådana övningar. Kontinuitetsplanen måste revideras så att den följer förändringar i verksamheten och täcker nya identifierade risker. Det är lämpligt att kontinuitetsplanen utgår från de analyser av systemet som görs redan när myndigheten överväger att anskaffa och sedan beslutar att använda, utveckla eller förändra systemet. Kontinuitetsplanen bör kompletteras med rutiner kring andra hot såsom naturkatastrofer och olyckor.

En myndighet ska besluta om den längsta tid som ett IT-system bedöms kunna vara ur funktion utan att verksamheten störs i väsentlig omfattning. Myndigheten ska vidare besluta om vilka reservrutiner som ska tillämpas vid avbrott och störningar i IT-systemets funktion. Besluten ska dokumenteras.

Dokumentation
Kontinuitetsplan

5 Tillträdesbegränsning

10 § säkerhetsskyddslagen
5 kap. RPSFS 2010:03

5.1 VAD SYFTAR TILLTRÄDESBEGRÄNSNING TILL?

Tillträdesbegränsning syftar till att hindra obehöriga att få tillträde till anläggningar, inrättningar, fordon, fartyg, luftfartyg samt andra föremål eller områden där hemlig uppgift eller annat av betydelse för rikets säkerhet förvaras eller där verksamhet av sådan betydelse bedrivs. Tillträdesbegränsning ska även förebygga terrorism. Tillträdesbegränsningen kan också, beroende på utformning, utgöra ett skydd mot bland annat inbrott och våldsbrott i övrigt.

Bestämmelserna om tillträdesbegränsning i lagstiftningen ålägger den som omfattas av reglerna att pröva i vilken utsträckning en tillträdesbegränsning är påkallad och att i förekommande fall utforma begränsningen på ett tillfredsställande sätt. Prövningen bör utgå från myndighetens säkerhetsanalys. Prövningen kan utmynna i att man anser att byggnaden eller området bör förklaras som skyddsobjekt.

Tillträdesbegränsningen kan utformas på olika sätt. I vissa fall räcker det att tillträdesförbudet avser utomstående. I andra fall kan det behöva omfatta även den egna personalen. För särskilt känsliga delar kan tillträdesrätten behöva begränsas till dem av de anställda som har ett oundgängligt behov av att vistas inom det aktuella området. Begränsningen ska utformas så att allmänhetens rätt att röra sig fritt inte inskränks mer än nödvändigt.

Hur tillträdesbegränsningen utformas för en myndighets anläggningar, lokaler, områden med mera där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism bör framgå av myndighetens särskilda föreskrifter.

Tillträdesbegränsning i säkerhetsskyddslagstiftningen har ett nära samband med reglerna om förbud mot tillträde i skyddslagen. Beslut om skyddsobjekt enligt skyddslagen kan sägas vara en kvalificerad form av tillträdesbegränsning.

Prövningen beträffande behovet av tillträdesbegränsning kan utmynna i att man anser att denna kvalificerade form av tillträdesbegränsning är påkallad. Myndigheten tar i så fall initiativ till att en byggnad eller ett område förklaras som skyddsobjekt. Av skyddslagen och säkerhetsskyddsförordningen framgår vem som har rätt att fatta beslut om skyddsobjekt.

5.2 TILLTRÄDESBEGRÄNSNINGENS FORMER

Tillträdesbegränsningen kan hindra, fördröja eller förvarna om obehörigt tillträde till platser där säkerhetskänslig verksamhet bedrivs eller där hemliga uppgifter bearbetas eller förvaras.

Tillträdesbegränsning kan ske genom:

- Utfärdande och tillkännagivande av tillträdesförbud
- Passerkontroll, antingen personell eller teknisk kontroll för in- och utpassering eller båda i kombination
- Byggnadstekniska åtgärder såsom byggnadskonstruktioner, sektioneringar, lås eller stängsel
- Bevakningstekniska hjälpmedel, larmanordningar, tv-övervakning
- Inre och yttre bevakning.

5.3 TILLTRÄDESRÄTT

Vem som har rätt att få tillträde till en myndighets anläggningar, lokaler, förvaringsenheter eller områden bör regleras i myndighetens särskilda föreskrifter. Om flera myndigheter, företag eller organisationer bedriver verksamhet inom samma anläggning bör en överenskommelse träffas om hur tillträdesbegränsningen ska utformas för de delar som är gemensamma.

Notera dock att den som önskar tillträde till en myndighet för att ta del av en allmän handling har rätt att utan identitetskontroll, men under uppsikt, få tillträde till ett lämpligt utrymme som disponeras av myndigheten.

5.4 PASSERKONTROLL

5 kap. 1–2 §§ RPSFS 2010:03

Passerkontroll kan avse:

- Att vid inpassering fastställa en persons identitet och rättighet att få tillträde till myndigheten
- Att vid utpassering fastställa att den besökare som har inpasserat till myndigheten utpasserar, samt vid behov även kontrollera besökarens tillträdesrätt och uppehållstid inom myndigheten.

Vid besök ska myndigheten utfärda ett skriftligt besökstillstånd för utomstående personer som ges tillträde till en plats där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism. Myndigheten ska kontrollera att endast personer med tillstånd ges tillträde. Vid alla passerställen till tillträdesskyddade platser ska det finnas personell bevakning eller utrustning för teknisk tillträdeskontroll, eller båda i kombination.

Vid passerställen där endast anställda och motsvarande får inpassera kan ett automatiskt passerkontrollsystem med fördel användas. Ett sådant system kan också vara att föredra vid inre sektionering. En personbemannad passerkontroll bör finnas vid minst en ingång och då lämpligen vid huvudentrén, för att möjliggöra ett mottagande av besökare.

Vid automatiska passerställen bör kort med personlig kod användas vid passeringen. In- och utpassering som sker med kort och kod bör loggas i en dator. Inpassering med generella koder (koder gällande för flera personer) bör inte användas.

De besökare som har medgivits tillträde till en myndighets lokaler bör förses med besökskort som ska bäras väl synligt. Besökarna bör vidare skrivas in i en besöksliggare med ankomsttid, uppgift om vilken myndighet eller företag som de representerar, besöksmottagare samt eventuellt nummer på det besökskort som de tilldelas. Besökskortet måste alltid återlämnas efter besöket. Förteckningen över besökare bör sparas i minst ett år.

5.5 BYGGNADSTEKNISKA ÅTGÄRDER OCH HJÄLPMEDEL

För att tekniska skyddsåtgärder ska bli effektiva och rationella måste man ta hänsyn till vad som ska skyddas och till förhållandena på platsen.

Byggnadsteknisk tillträdesbegränsning ska i allmänhet utföras så att intrång eller intrångsförsök av obehöriga hindras, försvåras eller upptäcks på ett tidigt stadium. Vanligtvis läggs begränsningen i en byggnads omslutningsyta, såsom ytterväggar, tak, golv, dörrar eller fönster. Begränsningen kan även ligga inne i en byggnad, till exempel mellan olika hyresgäster eller runt det som särskilt bedöms vara skyddsvärt, så kallad inre sektionering.

Om öppningsbara fönster är belägna lägre än fyra meter över mark- eller ståplan bör en bedömning göras om fönstren ska förses med lås eller förstärkas.

I samband med ny-, om- eller tillbyggnad av en myndighets lokaler bör det i ett tidigt stadium övervägas vilka byggnadskonstruktioner som ska användas för att minska riskerna och begränsa behovet av övriga skyddsåtgärder som annars måste vidtas.

5.5.1 Mekaniska inbrottsskydd

Mekaniskt inbrottskydd omfattar:

- Inkrypningsskydd och galler
- Låsenheter
- Stängsel och andra typer av inhägnader
- Körgrindar och bommar
- Rotations- och gånggrindar samt inpasseringsslussar
- En byggnads omslutningsytor, det vill säga tak, golv, väggar, fönster, luckor, dörrar samt vik-, skjut- och jalusiportar.

När det gäller utformningen av det mekaniska inbrottsskyddet kan Svenska stöldskyddsföreningens regler för mekaniskt inbrottsskydd, SSF 200, vara en vägledning. Observera dock att dessa regler är utformade mot bakgrund av försäkringsbolagens krav. För inbrottsskyddande låsenheter, dörrar och glas hänvisas till aktuella standarder.

5.5.2 Larm

Med larm menas olika tekniska åtgärder för att uppmärksamma ett tillbud och för att en insats ska kunna åtgärda ett angrepp. Larm kan utgöras av överfallslarm, inbrottslarm, brandlarm eller driftlarm. Larmen kan bestå av en siren som enbart ljuder vid larmobjektet eller bestå av ett larm som indikerar ett tillbud hos en larmcentral, eller av en kombination av dessa. Ett tyst larm indikerar endast hos larmcentralen.

En inbrottslarmanläggning bör projekteras av en certifierad godkänd anläggarfirma och följa aktuella standarder och normer hos branschorganen. I

de flesta fall bör säkerhetsskyddsavtal träffas med företag som ansvarar för myndighetens larm.

5.5.3 Kameraövervakning

Kameror ger ökade möjligheter att bevaka undanskymda eller viktiga platser, grindar samt obevakade inpasseringsställen. Uppsättningen av övervakningskameror är reglerad för områden dit allmänheten har tillträde och kräver i de flesta fall länsstyrelsens beslut (se vidare lagen om allmän kameraövervakning). Oavsett var kameraövervakningen sker måste man upplysa om detta genom tydlig skyltning på övervakningsplatsen.

5.5.4 Inre och yttre bevakning

Inre bevakning innebär uppmärksamhet på att obehöriga inte vistas inom tillträdesbegränsat område och att där inte förekommer olovlig verksamhet. Rutiner bör upprättas så att det vid arbetstidens slut kontrolleras att ingen obehörig finns kvar och att fönster och dörrar är stängda och låsta.

Den inre bevakningen vid större arbetsplatser underlättas om anställda och besökare bär identitetshandlingar, väl synliga.

Yttre bevakning innebär att kontroll av obehörigt tillträde inte sker genom bevakningsobjektets yttre begränsning. Denna bevakning kan ske genom bevakningspersonal, rondering, tekniska (elektroniska) hjälpmedel eller genom en kombination av dessa.

5.6 KORT, KODER OCH NYCKLAR

5 kap. 3–6 §§ RPSFS 2010:03

För låsning av förvaringsutrymmen är kombinationslås att föredra. Används nyckellås uppkommer annars alltid frågan om var och hur nycklar ska förvaras efter arbetstidens slut. Myndigheten ska se till att den som har tilldelats ett förvaringsutrymme själv bestämmer koden till utrymmet och om möjligt också själv ställer in koden.

En kod till ett förvaringsutrymme bör ställas om minst en gång per år, när någon slutar, eller inte längre behöver tillgång till förvaringsutrymmet. Vid val av kod bör enkla sifferkombinationer undvikas, såsom 10–20–30–40. Det egna eller anhörigs telefonnummer, personnummer eller liknande bör inte heller användas.

5.6.1 Förvaring och förteckning

Kort, koder och nycklar till utrymmen där hemliga uppgifter förvaras eller där säkerhetskänslig verksamhet bedrivs ska förvaras så att ingen obehörig kan komma åt dem. Förvaringen av kort, koder och nycklar ska ges minst samma skydd som utrymmet som de avser att skydda.

Det bör i detta sammanhang framhållas att de entreprenörer och leverantörer som anlitas för installationer och andra uppdrag som avser säkerhetsskyddet kan behöva upphandlas med säkerhetsskyddsavtal. Ytterligare information om säkerhetsskyddad upphandling finns i kapitel 7.

Hos myndigheten ska det finnas ett system där myndigheten har tillgång till samtliga nycklar, kort och koder avseende utrymmen där hemliga uppgifter förvaras, där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism.

Hos en myndighet ska det finnas en förteckning över samtliga nycklar till förvaringsutrymmen. Av förteckningen ska det framgå till vem nyckel, kort eller kod har lämnats, när detta har skett och var reservnyckel, reservkort och kod finns. Dessutom ska det framgå när ett kort, en kod eller en nyckel har återlämnats.

En myndighet bör i särskilda föreskrifter reglera ansvaret för förvaringsutrymmen där hemliga uppgifter finns.

Dokumentation
Förteckning över kort, koder och nycklar

5.6.2 Förlust

Om det befaras att ett kort eller en nyckel har förlorats eller kopierats, att en kod har röjts eller att ett kort, en kod eller en nyckel har använts av någon obehörig person, ska detta omedelbart anmälas till myndighetens säkerhetsskyddschef. Finns det ingen säkerhetsskyddschef ska anmälan göras till myndighetens chef eller motsvarande organ.

6 Säkerhetsprövning

11 § säkerhetsskyddslagen
14, 38 §§ säkerhetsskyddsförordningen
6 kap. RPSFS 2010:03

6.1 NÄR SKA SÄKERHETSPRÖVNING GÖRAS?

Säkerhetsprövningen omfattar alla de åtgärder som berörd myndighet bör göra för att skaffa sig så mycket information som möjligt om den som ska prövas. Informationen ska utgöra ett underlag för myndighetens bedömning och beslut om en person kan bedömas lojal och pålitlig från säkerhetssynpunkt så att han eller hon kan anställas eller anlitas i verksamhet som har betydelse för rikets säkerhet eller som är viktig för skyddet mot terrorism.

Det är viktigt att påpeka att säkerhetsprövningen inte kan jämställas med registerkontroll, eftersom registerkontrollen bara utgör en liten del av underlaget i säkerhetsprövningen. Observera även att en person kan bli föremål för säkerhetsprövning utan att registerkontroll genomförs (se nedan). En väl genomförd säkerhetsprövning kräver tid, och ska vara gjord innan personen anställs eller anlitas.

Bestämmelserna om säkerhetsprövning gäller inte bara vid nyanställning utan ska även tillämpas om en redan anställd eller anlitad person får nya arbetsuppgifter som har betydelse för rikets säkerhet eller som är viktiga för skyddet mot terrorism.

Säkerhetsprövning av en person ska inte ses som en engångsföreteelse. Myndigheten har ett ansvar att kontinuerligt följa upp den som är anställd eller som på annat sätt deltar i verksamhet som är av betydelse för rikets säkerhet eller till skyddet mot terrorism. Ett viktigt instrument är utvecklingssamtal eller medarbetarsamtal som inte bara handlar om utveckling och motivation, utan också ger en möjlighet att följa upp medarbetarens allmänna levnadssituation utanför arbetet. Att vara observant på ändrat beteende är också en viktig del i uppföljningen. Säkerhetsprövningen ska dokumenteras när det gäller en person som har bedömts vara pålitlig från säkerhetssynpunkt.

En myndighet som till exempel har tillsynsansvar inom ett specifikt verksamhetsområde och som beslutar om registerkontroll av någon som inte ska anlitas i den egna verksamheten, ska vid behov samråda med den faktiska arbetsgivaren om säkerhetsprövningsåtgärderna. Detta gäller inte registerkontroll och särskild personutredning.

Dokumentation
Förteckning över anställningar som är placerade i säkerhetsklass, anställningar som registerkontrolleras till skydd mot terrorism samt anställningar som endast omfattas av säkerhetsprövning

6.2 GRUNDER, UNDERLAG OCH PROCESS FÖR SÄKERHETSPRÖVNING

Säkerhetsprövningen ska grundas på:

1. Den personliga kännedom som finns om den som ska prövas
2. Uppgifter som framgår av betyg, intyg och referenser med mera
3. I förekommande fall, uppgifter som har kommit fram vid registerkontroll och särskild personutredning.

Identitetskontroll ska göras, om det inte är obehövligt.

Grunden för säkerhetsprövningen är en noggrann personbedömning. De två viktigaste instrumenten för att hämta in underlaget för denna bedömning är personlig intervju och inhämtning av referenser.

Ansökningshandlingar utgör ett viktigt komplement och i förekommande fall ska utlämnade uppgifter från registerkontroll vägas in i säkerhetsprövningen. Självklart måste kompetensen för anställningen eller uppdraget klaras ut i intervjun, men de personliga egenskaperna och andra personliga förhållanden måste prioriteras. Exempelvis kan en person bedömas som lojal och pålitlig men skulle på grund av sitt umgänge eller dubbla lojaliteter kunna bli sårbar och utsättas för påtryckning; det är svårare att säga nej till en god vän jämfört med en tillfällig bekantskap. ”Det förhållande att en person inte bedöms vara pålitlig från säkerhetssynpunkt behöver i och för sig inte alltid utgöra

ett negativt omdöme om vederbörande. Det kan räcka att en person är särskilt sårbar i det att han eller hon på grund av dubbla lojaliteter riskerar att hamna i en intressekonflikt eller att utsättas för påtryckningar" (prop. 1995/96:129, s. 28).

Nedan följer exempel på frågeområden som kan behandlas vid en intervju, i syfte att bredda underlaget för personbedömningen:

• *Personalia* – uppgifter om personen, familj och släkt. Är anhöriga bosatta utomlands?

• *Umgänge* – i vilken krets det finns vänner och eventuella ovänner. Kan personen bli sårbar och utsättas för påtryckning?

• *Utbildning* – genomgång av utbildningar, främst från gymnasiet och framåt, belysning av speciella färdigheter, positiva och negativa erfarenheter från studietiden. Tänk på att det bland annat med hjälp av internet har blivit allt vanligare att betyg eller examina är förfalskade. Högskoleverket kan hjälpa till om det skulle uppkomma misstankar om förfalskningar.

• *Anställningar* – tillbakablick på tidigare anställningar såväl inom Sverige som utomlands, och varför personen har valt olika typer av arbeten. Eventuella tidsluckor i CV bör klaras ut. Finns bisysslor?

• *Ekonomi* – belysning av den ekonomiska situationen som den ser ut i dag och framöver. Observera skyldigheten i säkerhetsklasserna 1 och 2 att lämna information om den ekonomiska situationen i samband med registerkontroll.

• *Utlandsresor* – avser resor såväl privat som arbetsrelaterade. Har personen kommit i kontakt med företrädare för underrättelseorganisationer, och finns det andra händelser som kan uppfattas som kontroversiella?

• *Fritidsintressen* – föreningsengagemang, hobby, idrott, etc.

• *Missbruksproblematik* – frågor kring missbruk och beroenden av alkohol, narkotika, spel, medicin med mera.

• *Kriminalitet* – personen ges möjlighet att berätta om han eller hon varit föremål för rättsingripande eller blivit dömd för brott, eller om det finns någon relation till grovt kriminella personer.

• *Personlig status* – frågeställningar kring medicinska problem, sjukskrivningar och den fysiska statusen.

• *Personliga egenskaper* – exempel på frågeområden är ambition, arbetstillfredsställelse, samarbetsförmåga, framgångsresultat, anpassningsförmåga, arbetssätt, etik/moral, rätts- och säkerhetsmedvetande, personlig stabilitet och konflikthantering.

• *Intressekonflikter* – mot bakgrund av nämnda frågeområden bör intervjun ge svar på om det kan finnas något som gör personen sårbar eller att han eller hon skulle kunna hamna i en intressekonflikt.

Inom ramen för den beskrivna processen är det viktigt att personen får klart för sig vilka sekretess- och säkerhetskrav som kommer att ställas. Personen bör också få frågan om han eller hon anser sig ha kunnat ge en rättvis bild av sig själv eller om det behövs någon komplettering i det avseendet.

När det gäller inhämtning av referenser kan det finnas anledning att även tala med andra än de som personen själv har uppgivit. Detta förutsätter dock att man gjort en bedömning utifrån ett etiskt hänsynstagande. Exempelvis vill kanske personen ifråga inte avslöja för nuvarande arbetsgivare att han eller hon söker en ny anställning.

Dokumentation
Förteckning över personer som har godkänts vid säkerhetsprövningen

7 Säkerhetsskyddad upphandling

8 § säkerhetsskyddslagen
15 § säkerhetsskyddsförordningen
7 kap. RPSFS 2010:03

Kapitlet syftar till att ge en övergripande bild av förfarandet vid en säkerhetsskyddad upphandling. En mer detaljrik beskrivning av processen kring säkerhetsskyddad upphandling finns i *Säkerhetsskyddad upphandling – en vägledning* (Säkerhetspolisen, uppdaterad 2010).

Det bör framhållas att lagen om offentlig upphandling eller lagen om upphandling inom områdena vatten, energi, transporter och posttjänster i tillämpliga delar ska beaktas vid en upphandling.

I samband med säkerhetsskyddad upphandling är det nödvändigt med ett nära samarbete mellan beställare, beställarens säkerhetsfunktion och upphandlingsfunktionen.

7.1 NÄR BEHÖVS SÄKERHETSSKYDDAD UPPHANDLING?

Innan en upphandling påbörjas är en myndighet skyldig att pröva om upphandlingen helt eller delvis ska omges av säkerhetsskydd. Ska upphandlingen omges av säkerhetsskydd ska myndigheten fortlöpande pröva och anpassa skyddet med hänsyn till aktuell hotbild, upphandlingens omfattning och skyddsvärdet hos de uppgifter som kommer att hanteras av det berörda företaget. Bedömningar och åtgärder bör dokumenteras i en säkerhetsplan.

När en myndighet avser att begära in anbud eller träffa avtal om upphandling där det förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess, ska myndigheten träffa en skriftlig överenskommelse – säkerhetsskyddsavtal – med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet. Ett företag som vill konkurrera om ett upphandlingsavtal får acceptera upphandlarens uppfattning att ett säkerhetsskyddsavtal krävs. Gäller säkerhetsskyddslagen för företaget, exempelvis på grund av att det bedriver verksamhet av betydelse för rikets säkerhet, kan åligganden enligt lagen inte inskränkas genom avtalet.

Avgörande för om ett säkerhetsskyddsavtal ska träffas är alltså om det i anbudet eller i upphandlingen förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess. Myndigheten ska träffa ett säkerhetsskyddsavtal innan anbudsförfarandet inleds eller avtal om upphandling ingås (affärsavtalet). Har ett säkerhetsskyddsavtal träffats inför en anbudsinfordran ska säkerhetsskyddsavtalet, om det behövs, revideras när ett avtal träffas om upphandling.

7.2 BEDÖMNING AV FÖRETAGETS LÄMPLIGHET

Innan en myndighet får lämna ut hemliga uppgifter till företaget ska myndigheten göra en säkerhetsprövning och, i förekommande fall, även en registerkontroll av företagets ledning samt övriga som avses få del av hemliga uppgifter. Kravet på svenskt medborgarskap gäller inte för personal som anlitas i uppdrag med säkerhetsskyddsavtal. Den allmänna bedömningen av företagets lämplighet bör ha gjorts innan säkerhetsskyddsavtalet ingås.

Om företaget ska hantera och förvara hemliga uppgifter i egna lokaler ska myndigheten genom ett så kallat förstagångsbesök kontrollera att företagets lokaler och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt.

Säkerhetsskyddade upphandlingar brukar med hänsyn till uppdragets art indelas och hanteras på olika nivåer beroende på var uppgifterna ska hanteras.

7.3 SÄKERHETSSKYDDSAVTAL OCH SÄKERHETSSKYDDSINSTRUKTION

Vid förhandlingar om säkerhetsskyddsavtal företräds det allmänna av den myndighet som avser att begära in anbud eller träffa avtal. Myndighetens säkerhetsskyddschef eller annan säkerhetsansvarig ska medverka vid förhandlingen.

När ett säkerhetsskyddsavtal har ingåtts ska företaget upprätta en säkerhetsskyddsinstruktion. I instruktionen ska företaget redovisa vilka säkerhetsskyddsåtgärder som ska vidtas mot eventuella hot och risker. Det betyder att företaget ska reglera sitt säkerhetsskydd kring den kommande hanteringen av hemliga uppgifter. Säkerhetsskyddsinstruktionen ska godkännas av myndigheten. I det fall företaget ska utföra arbete i myndighetens lokaler eller i lokaler som har anvisats av myndigheten, får myndigheten medge att en säkerhetsskyddsinstruktion inte behöver upprättas.

Myndigheten ska träffa säkerhetsskyddsavtal med såväl huvudleverantör som eventuella underleverantörer.

7.4 SLUTFÖRANDE AV SÄKERHETSSKYDDSARBETE

När företaget har fullgjort uppdraget som omgetts av säkerhetsskydd ska myndigheten säga upp säkerhetsskyddsavtalet. Information, utrustning, nycklar och passerkort ska återlämnas och i förekommande fall ska koder till larm ändras och behörighet i IT-system avslutas. Myndigheten ska säkerställa att det som har avtalats om tystnadsplikt ska bestå.

7.5 UNDERRÄTTELSE TILL SÄKERHETSPOLISEN

En myndighet ska utan dröjsmål underrätta Säkerhetspolisen om säkerhetsskyddsavtal som har träffats och om säkerhetsskyddsavtal som har upphört att gälla. Det enklaste sättet är att använda blankett Underlag säkerhetsskyddad upphandling (SÄPO 070). Blanketten kan hämtas på Säkerhetspolisens webbplats, www.sakerhetspolisen.se.

7.6 ÖVRIGT

Utmynnar säkerhetsbedömningen inför en förestående upphandling i att någon säkerhetsskyddad upphandling inte ska ske, kan bedömningen ändå vara att det är lämpligt att vidta vissa säkerhetsskyddsåtgärder. I sådant fall kan den aktuella personalen ges utbildning och information om tystnadsplikt och därefter underteckna en bekräftelse på detta. Krav på sådana säkerhetsskyddsåtgärder kan ingå i affärsavtalet.

Dokumentation
Säkerhetsskyddsavtal
Säkerhetsskyddsinstruktion
Underlag säkerhetsskyddad upphandling (SÄPO 070)

8 Säkerhetsklasser och andra grunder för registerkontroll

12–16, 20 §§ säkerhetsskyddslagen
18–25 §§ säkerhetsskyddsförordningen
6, 8 kap. RPSFS 2010:03

8.1 BESLUT OM PLACERING I SÄKERHETSKLASS

17, 20 §§ säkerhetsskyddslagen
6 kap. 2 § RPSFS 2010:03

Beslut om placering i säkerhetsklass har ansetts i första hand vara en uppgift för myndigheten. Kommuner, landsting samt de myndigheter som anges i en bilaga till säkerhetsskyddsförordningen ska besluta om placering i säkerhetsklass 2 och 3 i följande fall:

- I fråga om den egna verksamheten
- När det gäller bolag, föreningar och stiftelser som de utövar ett rättsligt bestämmande inflytande över
- När det gäller anställning eller uppdrag hos en anbudsgivare eller leverantör med vilken de har ingått säkerhetsskyddsavtal.

De myndigheter och andra som förordningen gäller för men som enligt bestämmelserna inte har rätt att besluta om registerkontroll ska vid behov begära att regeringen fattar ett sådant beslut.

Med utgångspunkt från myndighetens säkerhetsanalys bör det inte vara svårt att besluta vilka anställningar som ska vara placerade i säkerhetsklass, vilka anställningar som endast ska vara föremål för säkerhetsprövning eller – i förekommande fall – vilka anställningar som är viktiga med hänsyn till skyddet mot terrorism. När det gäller bedömningen om inplacering i säkerhetsklass bör man beakta den sammanlagda mängden av sekretessbelagd information som en person kan komma att få del av. Vid bedömningen av inplacering i säkerhetsklass 3 kan en förtida menbedömning göras, det vill säga att klara ut vilket men och skada för rikets säkerhet det skulle innebära om sådan sekretess skulle röjas från anställningen. Resulterar menbedömningen i endast ringa men behöver anställningen inte placeras i säkerhetsklass och personen ska då inte bli föremål för registerkontroll, men övriga delar av säkerhetsprövningen ska genomföras.

En myndighet ska föra förteckning över de anställningar som myndigheten har beslutat ska vara inplacerade i säkerhetsklass, de anställningar som är viktiga med hänsyn till skyddet mot terrorism samt de anställningar som endast omfattas av säkerhetsprövning.

I de fall en myndighet anser att en anställning bör inplaceras i säkerhetsklass 1, ska myndigheten vända sig till regeringen för att få ett beslut. Detsamma gäller för en myndighet som inte har rätt att besluta om inplacering i säkerhetsklass, det vill säga de myndigheter som inte finns nämnda i bilagan till säkerhetsskyddsförordningen.

Dokumentation
Förteckning över anställningar som är placerade i säkerhetsklass, anställningar som registerkontrolleras till skydd mot terrorism samt anställningar som endast omfattas av säkerhetsprövning

8.2 REGISTERKONTROLL NÄR ANSTÄLLNINGEN ÄR PLACERAD I SÄKERHETSKLASS

13, 20 §§ säkerhetsskyddslagen
18–25 §§ säkerhetsskyddsförordningen
8 kap. 4 § RPSFS 2010:03

Registerkontroll ska göras vid säkerhetsprövning som gäller anställning, uppdrag, tjänstgöring enligt lagen om totalförsvarsplikt, utbildning, besök eller något annat deltagande i verksamhet, om anställ-

ningen eller verksamheten har placerats i säkerhetsklass.

En anställning eller ett annat deltagande i verksamheten ska placeras i säkerhetsklass om den anställde eller den som deltar i verksamheten:

- I stor omfattning får del av uppgifter som omfattas av sekretess och är av synnerlig betydelse för rikets säkerhet (säkerhetsklass 1)
- I en omfattning som inte är obetydlig får del av uppgifter som omfattas av sekretess och är av synnerlig betydelse för rikets säkerhet (säkerhetsklass 2)
- I övrigt får del av uppgifter som omfattas av sekretess och som är av betydelse för rikets säkerhet, om ett röjande av uppgifterna kan antas medföra men för rikets säkerhet som inte endast är ringa (säkerhetsklass 3).

Det är viktigt att komma ihåg att det är anställningen eller uppdraget som är placerat i en säkerhetsklass, inte individen. Skillnaden mellan säkerhetsklasserna beror på i vilken omfattning personen får del av hemliga uppgifter.

Registerkontroll ska inte göras när det gäller uppdrag som offentlig försvarare eller annat ombud inför domstol än offentligt ombud enligt 27 kap. 27 § rättegångsbalken. Registerkontroll ska inte heller göras när det gäller uppdrag som ledamot i riksdagen, i fullmäktige eller liknande uppdrag.

Däremot kan en förtroendevald som utses till ledamot i en styrelse eller nämnd som bedriver säkerhetskänslig verksamhet bli föremål för säkerhetsprövning och registerkontroll för det specifika uppdraget.

8.3 REGISTERKONTROLL TILL SKYDD MOT TERRORISM

14, 20 §§ säkerhetsskyddslagen
26–27 a §§ säkerhetsskyddsförordningen
6 kap. RPSFS 2010:03

Registerkontroll till skydd mot terrorism är inte kopplad till någon säkerhetsklass. Kontrollmöjligheten är i stället inriktad på omständigheter som har särskild betydelse för bedömningen av risker för terroristaktioner. Syftet är att stoppa presumtiva aktörer eller personer som skulle kunna vara till hjälp åt aktörer.

När det gäller registerkontroll till skydd mot terrorism ska myndigheten noga pröva behovet av en sådan kontroll, och kontroll får endast göras om skyddsbehovet inte kan tillgodoses på något annat sätt.

En registerkontroll får enligt säkerhetsskyddsförordningen göras i fråga om den som ska anställas eller på annat sätt delta i verksamhet vid:

- Civila flygplatser, flygstationer och flygpassagerarterminaler
- Statschefens residens och bostäder, statsministerns bostäder samt statens egendom Harpsund
- Anläggningar inom elförsörjningen som är skyddsobjekt
- Regeringskansliets byggnader
- Vissa skyddsobjekt enligt skyddslagen.

Registerkontroll får också göras beträffande de personer som ska förordnas enligt 16 § lagen om sjöfartsskydd eller 4 kap. 3 § lagen om hamnskydd. I 27 § säkerhetsskyddsförordningen framgår närmare vilka myndigheter eller motsvarande som får besluta om en sådan kontroll.

När det gäller riksdagens förvaltningsområde och anställda vid riksdagen anges i 20 § säkerhetsskyddslagen vem som beslutar om sådan kontroll.

8.4 REGISTERKONTROLL EFTER FRAMSTÄLLAN FRÅN ANNAN STAT ELLER ORGANISATION

15, 20 §§ säkerhetsskyddslagen
22 § säkerhetsskyddsförordningen

För registerkontroll efter framställan från en annan stat krävs att den person som framställan avser har eller har haft hemvist i Sverige och att personen ska delta i en verksamhet på det sätt som anges i 13 § säkerhetsskyddslagen. Vidare krävs det att det för deltagandet i den andra staten gäller regler om registerkontroll som motsvarar reglerna i säkerhetsskyddslagen samt att personen har lämnat sitt samtycke till kontrollen.

En förutsättning för att en registerkontroll av en person ska få göras efter framställan från en mellanfolklig organisation där Sverige är medlem, är att personen har eller har haft hemvist i Sverige och ska delta i en säkerhetskänslig verksamhet hos organisationen. Personen ska också ha lämnat sitt samtycke. En sådan framställan ska göras till Säkerhetspolisen.

8.5 FRAMSTÄLLAN OM REGISTERKONTROLL

29–30 §§ säkerhetsskyddsförordningen
8 kap. 1–4, 6 §§ RPSFS 2010:03

Den myndighet som har beslutat om registerkontroll ska skicka framställan till:

Säkerhetspolisen
Säkerhetsskyddsenheten
Box 12312
102 28 Stockholm

Registerkontroll är en del av säkerhetsprövningen och den bör vara avslutad innan det slutgiltiga beslutet om säkerhetsprövning fattas av myndigheten.

En framställan om registerkontroll ska göras på de blanketter som finns på Säkerhetspolisens webbplats, www.sakerhetspolisen.se, om det inte finns någon annan överenskommelse mellan myndigheten och Säkerhetspolisen.

Den som fattar beslut i säkerhetsprövningen efter genomförd registerkontroll måste, för säkerhetsklass 1 och 2, komma ihåg att ta del av uppgifterna i blanketterna SÄPO 073 och 074 (Särskild personutredning för säkerhetsklass 1 och 2, respektive Särskild personutredning för säkerhetsklass 1) innan dessa sänds in till Säkerhetspolisen. Dessa uppgifter bör ingå som en del av myndighetens säkerhetsprövning. Blanketterna behålls av Säkerhetspolisen. Den som har utsetts som kontaktperson och har rätt att besluta om framställan ska även kontrollera att alla uppgifter är rätt ifyllda samt noga beskriva kontrollorsaken. Den som beslutar om registerkontroll ska också dokumentera att samtycke till registerkontroll och, i förekommande fall, särskild personutredning har inhämtats.

Samtliga blanketter kan beställas hos säkerhetsskyddsenheten eller hämtas via Säkerhetspolisens webbplats, www.sakerhetspolisen.se. Observera att framställan inte kan mottas via telefax eller e-post.

Vid den första framställan om registerkontroll för uppdrag med säkerhetsskyddad upphandling ska underrättelse om att säkerhetsskyddsavtal ingåtts redovisas på blankett SÄPO 070 (Underlag säkerhetsskyddad upphandling). Det är avtalet som är grunden till att registerkontroll får göras. Till framställan ska bifogas ett registreringsbevis för företaget som inte får vara äldre än tre månader.

Vid samtliga registerkontroller görs en sökning i belastningsregistret, misstankeregistret och Säkerhetspolisens register oavsett om kontrollen gäller säkerhetsklassad anställning eller till skydd mot terrorism. När det gäller registerkontroll för säkerhetsklass 1 och 2 görs även sökning i andra register enligt 12 § säkerhetsskyddslagen.

Dokumentation
Samtycke

8.6 SÄRSKILD PERSONUTREDNING OCH PERSONLIGT SAMTAL

11, 18 §§ säkerhetsskyddslagen
34–37 §§ säkerhetsskyddsförordningen

En särskild personutredning ska göras vid registerkontroll som avser en anställning eller annat deltagande i verksamheten som har placerats i säkerhetsklass 1 eller 2. Detsamma kan gälla vid kontroll på begäran från en annan stat eller en mellanfolklig organisation. Utredningen ska omfatta en undersökning av vissa personliga förhållanden, bland annat den ekonomiska situationen.

För en anställning som har placerats i säkerhetsklass 1 ska normalt även ett personligt samtal hållas med den som är föremål för säkerhetsprövningen. För säkerhetsklass 2 kan det också hållas ett sådant samtal om det behövs. En tjänsteman vid Säkerhetspolisen genomför det personliga samtalet. Under samtalet går man igenom de ifyllda formulären och personen ges möjlighet att kommentera eller förklara eventuella uppgifter som framkommit vid registerkontrollen. I syfte att höja säkerhetsmedvetandet beskrivs bland annat risker, hot och andra liknande situationer. Slutligen görs en allmän bedömning av personen utifrån intryck och vad som har framkommit under samtalet.

8.7 SAMTYCKE

19 § säkerhetsskyddslagen
28 § säkerhetsskyddsförordningen
8 kap. 3 § RPSFS 2010:03

Innan en registerkontroll och särskild personutredning får göras ska den som säkerhetsprövningen gäller ha gett sitt samtycke till åtgärderna. Samtycket innebär också att personen redovisar de uppgifter som framgår av blanketterna SÄPO 073 och 074 om kontrollen avser säkerhetsklass 1 eller 2. För att den som ger sitt samtycke ska förstå vad registerkontroll innebär är det angeläget att myndigheten som beslutar om registerkontroll lämnar

information som åtminstone omfattar i vilka register som kontroll görs (belastningsregistret, misstankeregistret och Säkerhetspolisens register) – se även 12 § säkerhetsskyddslagen. Myndigheten ska dokumentera samtycket och bevara dokumentationen eftersom samtycket även gäller för nya kontroller och utredningar så länge som den kontrollerade innehar samma anställning. Vid kontroll i säkerhetsklass 1 och 2 kontrolleras också make, maka eller sambo men dessa behöver inte lämna samtycke till kontrollen.

Dokumentation
Samtycke till registerkontroll och särskild personutredning

8.8 SVENSKT MEDBORGARSKAP

29 § säkerhetsskyddslagen

För att få en anställning som är inplacerad i säkerhetsklass i staten, en kommun eller ett landsting krävs att personen är svensk medborgare. Det kravet gäller inte för den som deltar i verksamhet som vid sidan om anställningen kräver registerkontroll, till exempel vid uppdrag med säkerhetsskyddad upphandling. Regeringen har möjlighet att efter begäran från en myndighet i ett enskilt fall medge undantag från kravet på svenskt medborgarskap. Personer som har dubbelt medborgarskap räknas som svenska medborgare om det ena medborgarskapet är svenskt. Det finns inget krav på svenskt medborgarskap för registerkontroll till skydd mot terrorism.

8.9 HANDLÄGGNING HOS SÄKERHETS- OCH INTEGRITETSSKYDDSNÄMNDENS REGISTERKONTROLLDELEGATION

21–26 §§ säkerhetsskyddslagen
29–37, 50 §§ säkerhetsskyddsförordningen
2 § förordningen med instruktion för Säkerhets- och integritetsskyddsnämnden

Säkerhetspolisen ska överlämna ärendet till registerkontrolldelegationen. Registerkontrolldelegationen ska i varje enskilt fall besluta om uppgifter som har framkommit vid registerkontroll eller särskild personutredning ska lämnas ut till den myndighet som har begärt kontrollen. Vilka uppgifter som kan lämnas ut i olika fall av registerkontroll anges närmare i 21–23 §§ säkerhetsskyddslagen. Exempelvis gäller för säkerhetsklass 1 och 2 att en utlämning får omfatta varje uppgift som finns tillgänglig om den kontrollerade. När det gäller den medkontrollerade ställs kravet att det ska vara oundgängligen nödvändigt att den som har begärt kontrollen får uppgiften. Om det finns synnerliga skäl får även uppgifter som har framkommit vid särskild personutredning lämnas ut. Vidare gäller ett allmänt krav på relevans för att en uppgift ska få lämnas ut. Det kravet är uttryckt på så sätt att uppgiften får lämnas ut för säkerhetsprövning endast om den kan antas ha betydelse för prövningen av den kontrollerades pålitlighet från säkerhetssynpunkt. För att underlätta delegationens bedömning är det viktigt att den som har gjort framställan om registerkontroll tydligt har angett vilken typ av verksamhet den kontrollerade ska delta i.

Det får inte framgå av svaret till den myndighet som har begärt registerkontrollen att det finns en uppgift om den kontrollerade som inte har lämnats ut. Vare sig registerkontrolldelegationen eller Säkerhetspolisen får lämna någon kommentar eller rekommendation i ett ärende. Däremot får en kommentar lämnas som ett förtydligande till den utlämnade uppgiften.

Kommunicering
Innan en uppgift som har framkommit vid registerkontroll eller särskild personutredning får lämnas ut för säkerhetsprövning, ska den som uppgiften avser ges tillfälle att yttra sig över uppgifterna. Detta kallas kommunicering. Detta gäller dock inte om uppgiften omfattas av sekretess i förhållande till den enskilde enligt någon annan bestämmelse i offentlighets- och sekretesslagen än den så kallade registersekretessen i 35 kap. 3 §. Även om uppgiften omfattas av sådan sekretess, ska den som uppgiften avser ges tillfälle att få yttra sig innan uppgiften lämnas ut, om personens intresse av att få yttra sig skäligen bör ha företräde framför det intresse som sekretessen ska skydda.

Kommuniceringen har fyra syften:

- Att den som är föremål för kontroll ska ha möjlighet att få reda på vilka uppgifter om honom eller henne som har bedömts vara av sådan betydelse att de bör lämnas ut
- Att eventuella förväxlingar och andra missförstånd kan redas ut
- Att man kan undvika onödigt hemlighetsmakeri
- Att personen ges möjlighet att via myndigheten som har gjort framställan återkalla sin ansökan till en säkerhetsklassad anställning eller anställning som behöver kontrolleras till skydd mot terrorism.

Om en person har kommit in med ett yttrande föredras ärendet på nytt för registerkontrolldelegationen, som därefter fattar ett slutgiltigt beslut som inte kan överklagas.

Ytterligare information om Säkerhets- och integritetsskyddsnämnden finns på myndighetens webbplats, www.sakint.se.

8.10 PRÖVNING AV DE UTLÄMNADE UPPGIFTERNA OCH ÅTERRAPPORTERING

27–28 §§ säkerhetsskyddslagen
8 kap. 5 § RPSFS 2010:03

Den myndighet som beslutar om registerkontroll ska självständigt avgöra om den person som prövas ska anställas eller anlitas. Myndighetens bedömning ska grundas på den personbedömning som myndigheten tidigare har gjort, de uppgifter som eventuellt har kommit fram vid registerkontrollen och särskild personutredning samt eventuella övriga omständigheter. Den samlade informationen ska också bedömas ihop med den verksamhet som personen ska arbeta inom.

Sedan myndigheten har fattat ett beslut med anledning av säkerhetsprövningen, ska de handlingar som har erhållits från Säkerhetspolisen snarast återställas dit. Återrapporteringen ska ske skyndsamt, då det är nödvändigt bland annat för att förfarandet med spontanuppföljning (se avsnitt 8.14) ska kunna fungera tillfredsställande.

8.11 NY KONTROLL

24–25 §§ säkerhetsskyddsförordningen
8 kap. 6 § RPSFS 2010:03

En ny registerkontroll ska göras minst vart femte år av den som har anlitats i säkerhetsklass 1 eller 2. En ny registerkontroll ska också göras när den som har en anställning i säkerhetsklass 1 eller 2 har ingått äktenskap, registrerat partnerskap eller inlett ett samboförhållande efter den senaste registerkontrollen. Vidare ska en ny registerkontroll göras när det finns särskild anledning till det. Exempel på särskild anledning kan vara att myndigheten har fått kännedom om att det finns brottsmisstankar mot en person eller andra problem som skulle kunna komma fram i en registerkontroll, eller att personen har fått andra arbetsuppgifter. Ansvaret för att en ny registerkontroll görs ligger på den som har beslutat om registerkontroll.

Innan någon som redan har anlitats i anställning eller annat deltagande i verksamhet som har placerats i säkerhetsklass får anlitas i en högre säkerhetsklass, ska en ny registerkontroll göras.

8.12 ANMÄLAN VID ÄNDRING AV DEN KONTROLLERADES FÖRHÅLLANDEN

8 kap. 7 § RPSFS 2010:03

Den som har beslutat om registerkontroll ska skriftligen underrätta Säkerhetspolisen om en person har slutat i verksamhet som har placerats i säkerhetsklass, kontrollerats till skydd mot terrorism eller övergått till verksamhet som har placerats i lägre säkerhetsklass.

Säkerhetspolisen ska även underrättas, när det gäller registerkontrollerade i säkerhetsklass 1 och 2, om den kontrollerades äktenskap eller registrerade partnerskap har upplösts eller samboförhållande har upphört.

8.13 UNDERLÅTELSE AV REGISTERKONTROLL

16 § säkerhetsskyddslagen
8 kap. 8 § RPSFS 2010:03

En myndighet kan avstå från en registerkontroll om det står klart att någon kontroll inte behövs därför att den som ska säkerhetsprövas i en ny anställning tidigare har kontrollerats på motsvarande sätt. I förarbetena till säkerhetsskyddslagen (prop. 1995/96:129) sägs att även tidsaspekten har betydelse i detta sammanhang och att en ny kontroll bör underlåtas endast om den tidigare kontrollen ligger något eller högst några år tillbaka i tiden. Om myndigheten underlåter att göra en ny kontroll ska Säkerhetspolisen underrättas skriftligt och skälen till underlåtelsen ska anges.

Dokumentation
Skäl för att underlåta registerkontroll

8.14 SPONTANUPPFÖLJNING

29 § säkerhetsskyddsförordningen

Säkerhetspolisen har en skyldighet att följa upp om det har tillförts uppgifter i polisregister efter det att en registerkontroll har gjorts. Vid en sådan förekomst föredras ärendet för registerkontrolldelegationen på samma sätt som tidigare har beskrivits.

Det är därför av yttersta vikt att den som beslutar om registerkontroll anmäler om en person har slutat sin anställning eller om någon annan förändring har skett (exempelvis ändrade relationsförhållanden när det gäller säkerhetsklass 1 och 2), så att spontanuppföljning inte sker i större omfattning än nödvändigt.

8.15 KONTAKTPERSON

8 kap. 9 § RPSFS 2010:03

Vid en myndighet som beslutar om registerkontroll ska det finnas en kontaktperson som svarar för kontakterna med Säkerhetspolisen. Kontaktpersonen ska även ha en ersättare.

9 Utbildning

9.1 UTBILDNING

30 § säkerhetsskyddslagen
9 kap. 1–3 §§ RPSFS 2010:031

En förutsättning för ett effektivt säkerhetsskydd är att all personal får grundläggande utbildning i ämnet. Utbildning i säkerhetsskydd ska främst syfta till att klargöra varför och hur man ska vidta skyddsåtgärder mot hot av olika slag. Myndigheter eller företag som omfattas av säkerhetsskyddslagstiftningen är skyldiga att anordna utbildning för eget behov.

Ytterligare utbildning bör ges till dem som har sin arbetsplats förlagd i ett område där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism. Denna personalkategori kan till exempel innefatta olika chefsgrupper, säkerhetsskyddsansvariga, IT-handläggare, expeditionspersonal, personalhandläggare, inköpsansvariga och vaktpersonal.

Varje myndighet ska ha en plan för utbildning i säkerhetsskydd samt föra en förteckning över de anställda som har säkerhetsprövats och som har genomgått utbildning i säkerhetsskydd. Detta bör även tillämpas beträffande företag med vilka myndigheten har träffat säkerhetsskyddsavtal.

Dokumentation
Utbildningsplan
Förteckning över de anställda som har säkerhetsprövats och som har genomgått utbildning i säkerhetsskydd

9.2 KONTROLL OCH TILLSYN

30–31 §§ säkerhetsskyddslagen
39–42 §§ säkerhetsskyddsförordningen
9 kap. 4–6 §§ RPSFS 2010:03

Varje myndighet eller företag som omfattas av säkerhetsskyddslagstiftningen ska kontrollera det egna säkerhetsskyddet. Dessa kontroller ska ske fortlöpande och det ska föras protokoll över genomförda kontroller. Protokollen ska förvaras samlade vid myndigheten. Närmare bestämmelser om internkontrollerna ges lämpligen i planen för intern kontrollverksamhet. I planen bör även ingå tillsyn över de företag med vilka myndigheten har träffat säkerhetsskyddsavtal.

Varje myndighet ska också kontrollera säkerhetsskyddet hos de företag med vilka man har träffat säkerhetsskyddsavtal. Sådan kontroll kan också ske i samråd med Säkerhetspolisen.

De funktionsansvariga myndigheter som anges i säkerhetsskyddsförordningen ska utöver det egna säkerhetsskyddet även kontrollera att de bolag, föreningar och stiftelser över vilka staten, kommuner eller landsting har ett rättsligt bestämmande inflytande har ett tillfredsställande säkerhetsskydd. De sektorsansvariga myndigheterna har också tillsynsansvar när gäller säkerhetsskyddet hos enskilda företag. Sådana kontroller som anges ovan kan också ske i samråd med Säkerhetspolisen.

Ytterligare information om myndigheters ansvar för säkerhetsskydd samt Säkerhetspolisens roll som tillsynsmyndighet finns i Inledning, avsnitten Ansvar för säkerhetsskydd samt Säkerhetspolisens roll som tillsynsmyndighet.

Dokumentation
Plan för intern kontrollverksamhet

10 Internationella förhållanden

10 kap. RPSFS 2010:03

Inom alla områden i samhället sker och har det skett en snabb internationalisering. Det gäller givetvis också på säkerhetsskyddsområdet. Ett problem är att alla inblandade parter, länder, organisationer med flera har olika sekretessregler och benämningar på sina sekretessbelagda handlingar. Det pågår ett nationellt och internationellt samarbete för att finna godtagbara lösningar. Det finns därför inget enkelt svar att ge på hur man ska tolka och jämföra de internationella bestämmelserna med de svenska. Det krävs därför sannolikt att man gör enskilda bedömningar från fall till fall och inte följer någon generell bedömningsmall.

Sverige och svenska myndigheter har i flera fall ingått internationella överenskommelser om gemensamt säkerhetsskydd. Ett exempel är Europeiska unionens råds säkerhetsbestämmelser (2001/264/EG). Andra liknande avtal har ingåtts med ESA (European Space Agency), NATO och VEU (Västeuropeiska unionen). Dessa avtal gäller och måste beaktas, likväl som RPSFS 2010:03.

De internationella beteckningarna för sekretessbelagda handlingar är följande:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED.

Information som har klassificerats enligt de internationella beteckningarna bör hanteras som hemlig eller kvalificerat hemlig information, även om det inte är klarlagt att de utgör hemliga uppgifter i säkerhetsskyddslagstiftningens mening.

Har handlingen TOP SECRET -benämningen anses den som en kvalificerat hemlig handling. Handlingar som har benämningen SECRET eller CONFIDENTIAL bör hanteras som hemliga handlingar. När handlingen är benämnd RESTRICTED kan den sannolikt hanteras som en hemlig handling vars röjande endast kan antas medföra ringa men för rikets säkerhet.

Det är inte möjligt att ge tydliga direktiv och anvisningar om hur hanteringen av internationella handlingar ska ske. Det är, som tidigare nämnts, upp till varje myndighet att i det enskilda ärendet bedöma innehållet i handlingen och följa ingångna avtal.

När hemliga handlingar skickas från Sverige till en annan stat, utländsk myndighet eller mellanfolklig organisation ska internationella beteckningar användas enligt samma mönster som när hemliga handlingar kommer till Sverige. I vissa avtal som har ingåtts krävs det att handlingen märks med den internationella beteckningen trots att handlingen endast kommer att förvaras i Sverige.

Det finns inget entydigt svar på i vilken säkerhetsklass personer som ska ta del av hemliga handlingar med utländsk beteckning ska vara placerade. Denna fråga har utretts av flera berörda parter för att hitta en godtagbar lösning, men utan slutgiltigt resultat. Tills vidare krävs det alltså att varje enskild handling bedöms för sig.

11 Myndighetens särskilda föreskrifter m.m.

45 § säkerhetsskyddsförordningen
1 kap. 5 § RPSFS 2010:03
3 kap. 5–7, 9–11, 14–16, 18–21, 23–24 §§ RPSFS 2010:03
4 kap. 31 § RPSFS 2010:03
5 kap. 2, 6 §§ RPSFS 2010:03

En myndighet som ska följa säkerhetsskyddslagstiftningen ska meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen i fråga om säkerhetsskyddet inom sitt verksamhetsområde. Detta behöver inte göras om det inte är uppenbart obehövligt. Vid behov ska myndigheten samråda med Säkerhetspolisen innan föreskrifter meddelas. Myndighetens särskilda föreskrifter får endast avvika från RPSFS 2010:03 efter Säkerhetspolisens medgivande.

Enligt RPSFS 2010:03 bör myndigheter meddela särskilda föreskrifter angående:
- Arbetsrutiner för hemlig handling i skrift eller bild
- Kvittering, tillfällig förvaring och inventering av hemliga handlingar
- Arbetsrutiner vid distribution av hemliga handlingar
- Hantering av elektroniska hemliga handlingar
- Tillträdesbegränsning till platser där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism
- Tillträde till och ansvar för förvaringsutrymme där hemliga uppgifter finns.

I dessa föreskrifter kan myndigheten vidare besluta om undantag från vissa av hanteringskraven i 3 kap. RPSFS 2010:03 när det gäller hemliga handlingar i skrift eller bild, under förutsättning att ett eventuellt röjande endast kan medföra ringa men för rikets säkerhet.

Säkerhetspolisen rekommenderar att myndigheter utformar särskilda rutiner och checklistor när det gäller säkerhetsprövning och säkerhetsskyddad upphandling.

Ytterligare information om krav på dokumentation för IT-system finns i kapitel 4.

Bilaga: Lagar och förordningar

I DENNA VÄGLEDNING refereras till lagar och förordningar utifrån vilka säkerhetsskydd ska bedrivas. I listan nedan återfinns i bokstavsordning alla de lagar och förordningar som nämns i texten, även om inte alla direkt reglerar utan enbart knyter an till säkerhetsskyddsverksamhet.

I vägledningens löpande text skrivs lagar och förordningar utan nummer.

För aktuell lagtext, se www.lagrummet.se.

Arkivlagen (1990:782)

Brottsbalken (1962:700)

Förordning (2007:1266) med instruktion för Försvarsmakten

Förordning (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden

Förordning (2002:1050) med instruktion för Säkerhetspolisen

Förordning (2006:942) om krisberedskap och förhöjd beredskap

Försvarsmaktens föreskrifter inom signalskyddstjänsten inom totalförsvaret; FFS 2005:2
→ *förkortas i texten FFS 2005:2*

Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter; FFS 2010:1

Försvarsmaktens föreskrifter om säkerhetsskydd; FFS 2003:7

Lagen (1998:150) om allmän kameraövervakning

Lagen (2006:1209) om hamnskydd

Lagen (2007:1091) om offentlig upphandling

Lagen (2004:487) om sjöfartsskydd

Lagen (1993:1742) om skydd för landskapsinformation

Lagen (2003:148) om straff för terroristbrott

Lagen (1992:1403) om totalförsvar och höjd beredskap

Lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster

Myndigheten för samhällsskydd och beredskaps föreskrifter om civila myndigheters kryptoberedskap; MSBFS 2009:11

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet; MSBFS 2009:10

Offentlighets- och sekretessförordningen (2009:641)

Offentlighets- och sekretesslagen (2009:400)

Polislagen (1984:387)

Regeringsformen (1974:152)

Rikspolisstyrelsens föreskrifter och allmänna råd om förordnande av sjöfarts- och hamnskyddskontrollanter; RPSFS 2009:21

Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd; RPSFS 2010:03
→ ersatte RPSFS 2004:11 den 1 februari 2010
→ *förkortas i texten RPSFS 2010:03*

Rikspolisstyrelsens föreskrifter och allmänna råd om utbildning och utrustning av skyddsvakter samt bevakning av civila skyddsobjekt; RPSFS 1991:5

Skyddsförordning (2010:523)

Skyddslag (2010:305)

Säkerhetsskyddsförordningen (1996:633)

Säkerhetsskyddslagen (1996:627)

Tryckfrihetsförordningen (1949:105)

Yttrandefrihetsgrundlagen (1991:1469)

Säkerhetspolisen

Säkerhetspolisen

Box 12312, 102 28 Stockholm
Tfn 010-568 70 00 Fax 010-568 70 10
E-post sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se