

PLAN SÄKERHETSSKYDD

Innehållsförteckning

1 Allmänt	3
2 Organisation.....	4
3 Säkerhetsskydd	5
3.1 Säkerhetsskyddschefens uppgifter	5
3.2 Säkerhetsskyddsanalys.....	5
3.3 Informationssäkerhet	5
3.3.1 Informationssäkerhetsklasser	6
3.3.2 Upprättande av handling	6
3.3.3 Sändande av handling	6
3.3.4 Mottagande av handling.....	6
3.3.5 Diarieföring av handling	7
3.3.6 Förvaring och kopiering av handling	7
3.3.7 Upphörande och förstöring av handling.....	7
3.3.8 Inventering av handlingar	7
3.4 Fysisk säkerhet.....	8
3.5 Personalsäkerhet	8
3.5.1 Säkerhetsprövning.....	8
3.5.2 Säkerhetsklasser	9
3.5.3 Registerkontroll	9
4 Säkerhetsskyddad upphandling.....	10
5 Utbildning och kontroll.....	11

1 Allmänt

Med säkerhetsskydd avses

1. Skydd mot spioneri, sabotage, terroristbrott och andra brott som kan hota säkerhetskänslig¹ verksamhet, samt
2. Skydd i andra fall av säkerhetsskyddsklassificerade² uppgifter.

Enligt säkerhetsskyddslagen ska den som är ansvarig för en säkerhetskänslig verksamhet bl a se till att

1. Behovet av säkerhetsskydd utreds (säkerhetsskyddsanalys).
2. Säkerhetsskyddsåtgärder enligt 1 planeras och vidtas för att säkerställa det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter.
3. Säkerhetsskyddet kontrolleras.

Så långt det är möjligt ska säkerhetsskyddsåtgärderna utformas så att de inte medför skada eller annan olägenhet för andra allmänna eller enskilda intressen.

Säkerhetsskyddet ska särskilt genom

1. *Informationssäkerhet* förebygga dels att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, dels skadlig inverkan på andra informationstillgångar som avser säkerhetskänslig verksamhet
2. *Fysisk säkerhet* förebygga dels att obehöriga får tillträde till områden, byggnader, och andra anläggningar eller objekt där de kan få åtkomst till säkerhetsskyddsklassificerade uppgifter eller där verksamhet som av annan anledning är säkerhetskänslig bedrivs, dels skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt
3. *Personalsäkerhet* förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet där de kan få åtkomst till säkerhetsskyddsklassificerade uppgifter eller i verksamhet som av annan anledning är säkerhetskänslig (säkerhetsprövning) samt säkerställa att de som deltar i säkerhetskänslig verksamhet har en tillräcklig kunskap om säkerhetsskydd (utbildning i säkerhetsskydd)

Säkerhetsskyddet ska även i övrigt förebygga terrorism.

Regionens säkerhetsskydd kontrolleras av Säkerhetspolisen (Säpo).

¹ Med säkerhetskänslig verksamhet avses sådan verksamhet hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet eller omfattas av ett internationellt säkerhetsskyddsåtagande.

² Med säkerhetsskyddsklassificerad uppgift avses en uppgift som rör säkerhetskänslig verksamhet och som av den anledningen omfattas av sekretess enligt offentlighets- och sekretesslagen eller som skulle ha omfattats av sekretess, om uppgiften istället förekommit i en verksamhet där bestämmelser om sekretess i offentlighets- och sekretesslagen gäller.

2 Organisation

Regionens ordinarie samt ställföreträdande säkerhetsskyddschef (SSC) utses av regiondirektör och ska på tjänstemannanivå samordna och handlägga ärenden inom säkerhetsskyddet. SSC ska bl a medverka i att genomföra regionens säkerhetsskyddsanalys, vilken i korthet innebär att undersöka vilka säkerhetsskyddsklassificerade uppgifter (SSKU) och vilka anläggningar som ska skyddas med hänsyn till Sveriges säkerhet eller till skydd mot terrorism. SSC och dennes ställföreträdare är direkt underställd regiondirektören i frågor rörande säkerhetsskyddet.

3 Säkerhetsskydd

Det ingår i verksamhetschefernas ansvar att i samråd med SSC undersöka vilka SSKU i verksamheten som ska skyddas med hänsyn till Sveriges säkerhet. Detsamma gäller de anläggningar som kräver ett säkerhetsskydd med hänsyn till Sveriges säkerhet eller skyddet mot terrorism.

3.1 Säkerhetsskyddschefens uppgifter

- Upprätta och följa upp rutiner avseende hantering av SSKU, t ex upprättande, diarieföring, förvaring och inventering
- Mottagare av SSKU
- Pröva behörighet att hantera SSKU
- Säkerhetsprövning av personal
- Rutin för säkerhetsbedömning av entreprenörer och leverantörer
- Delta vid upprättande av säkerhetsskyddsavtal
- Genomföra utbildning i säkerhetsskydd
- Kontaktperson mot Säpo
- Stöd vid upprättande av säkerhetsskyddsanalys
- I samverkan med polisen och regionens direktör fortlöpande bedöma hotbilder mot folkvalda politiker och vid behov vidta åtgärder.

3.2 Säkerhetsskyddsanalys

Säkerhetsskyddsanalysen är grunden för säkerhetsskyddet. Analysen är en inventering av skyddsvärda resurser kopplat till hot, risk och sårbarheter och ska leda till en konkret handlings- och åtgärdsplan. Analysen innebär att undersöka vilka SSKU och vilka anläggningar som ska skyddas med hänsyn till Sveriges säkerhet eller till skydd mot terrorism.

Resultatet av säkerhetsskyddsanalysen ska dokumenteras och revideras vid behov.

Se bilaga 1 för sammanfattning av säkerhetsskyddsanalys.

3.3 Informationssäkerhet

SSKU behöver ett anpassat säkerhetsskydd, oavsett vilken form den har. Den kan finnas på papper eller vara elektronisk. Den kan vara en allmän handling eller ett internt arbetsmaterial.

3.3.1 Informationssäkerhetsklasser

SSKU ska utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet, delas in i informationssäkerhetsklass enligt följande:

1. *Kvalificerat hemlig* vid en synnerligen allvarlig skada
2. *Hemlig* vid en allvarlig skada
3. *Konfidentiell* vid en inte obetydlig skada
4. *Begränsad* vid en ringa skada

SSKU ska inte förvaras på ett sådant sätt att obehöriga kan komma åt dem.

Behörig att ta del av SSKU, enligt säkerhetsskyddsförordningen, endast den som

- bedöms som pålitlig från säkerhetssynpunkt
- har tillräckliga kunskaper om säkerhetsskyddet
- behöver uppgifterna för sitt arbete i den verksamhet där SSKU förekommer

3.3.2 Upprättande av handling

När en allmän handling innehållande SSKU upprättas ska handlingen förses med uppgifter enligt följande, på första sidan ska anges:

- Handlingens beteckning
- Exemplarnummer
- Sidantal
- Antalet bilagor (om bilagor följer med handlingen)
- Sidorna i handlingen ska numreras i löpande följd

När det gäller framställande av handling i digitalform ska datorn inte vara kopplad till nätverket eller Internet när handlingen upprättas eller arbetas med. Dokumentet ska enbart sparas på en lös hårddisk alternativt ett USB-minne (krypterat). Hårddisken eller USB-minnet ska vara inlåst i godkänt säkerhetsskåp.

Fristående skrivare för utskrift ska användas.

3.3.3 Sändande av handling

Ska handling innehållande SSKU skickas ska den skickas med mottagningsbevis. Handlingen kan även lämnas över direkt till berörd person och ett mottagningsbevis ska upprättas.

Assuranstejp och stämpel ska förvaras som SSKU.

En handling innehållande SSKU ska aldrig skickas som epost eller bifogad fil.

3.3.4 Mottagande av handling

Den som hämtar försändelsen hos distributör ska kontrollera att försändelsen stämmer med kvittenslista och att försändelsen är oskadad. Om försändelsen är skadad ska den som hämtar försändelsen begära att distributören gör anteckning om skadans beskaffenhet. Mottagaren av försändelsen skall underrätta avsändaren av försändelsen om skadan.

En *kvalificerat hemlig* eller *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* eller *hemlig* handling muntligen eller genom visning ska det göras en kvittering eller anteckning om detta göras.

3.3.5 Diarieföring av handling

Inkommande handlingar som innehåller SSKU får inte öppnas på diariet. Breven känns igen på att de har skickats som REK eller ASS och på kuvertet står t ex Försvarsmakten, Säpo eller Länsstyrelsen.

Registratorn ska meddela SSC att en försändelse har anlänt. Kopia på kvitterat REK eller ASS behålls på diariet med bevakning att handlingen återkommer före registrering.

SSC öppnar själv brevet och låter sedan registratorn diarieföra handlingen. Om SSC inte finns på plats har stf SSC befogenhet att öppna och ta hand om handlingen. Om inte heller denna är tillgänglig ska diariet låsa in försändelsen i säkerhetsskåp. Försändelsen tas därefter omhand av SSC.

3.3.6 Förvaring och kopiering av handling

Handlingar innehållande SSKU ska förvaras i godkänt säkerhetsskåp.

Om handläggaren har tagit fram en handling och denne behöver lämna rummet ska handlingen bäras med, alternativt låsas in.

Obehöriga får inte lämnas ensam på rummet om handling innehållande SSKU finns framme.

Kopiering av handlingar ska undvikas. Men om en kopiering eller utdrag måste göras ska det godkännas av SSC och en anteckning om detta göras på handlingen. Där ska det också antecknas till vem som kopierat eller utdraget har lämnats. På ett utdrag ska det även antecknas från vilken handling utdraget har gjorts.

Kopiering/utskrift får inte ske på skrivare eller kopieringsmaskin som är kopplad till nätverk eller har en minnesfunktion (hårddisk).

3.3.7 Upphörande och förstöring av handling

Handlingar eller materiel som innehåller SSKU ska förstöras på ett sådant sätt att åtkomst och återskapande av uppgifterna omöjliggörs. Förstöringen ska dokumenteras. Förstöring kan t ex ske maskinellt (dokumentförstörare) eller genom bränning.

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

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

3.3.8 Inventering av handlingar

Handlingar innehållande SSKU ska inventeras årligen och protokollföras.

3.4 Fysisk säkerhet

Fysisk säkerhet innebär att hindra obehöriga att få tillgång till olika områden, t ex platser eller anläggningar där det finns SSKU eller bedrivs verksamhet som har betydelse för Sveriges säkerhet. Fysisk säkerhet kan också användas för att förhindra terrorattentat samt skydda personer eller egendom mot angrepp och brott.

Den fysiska säkerheten kan t ex regleras på följande sätt:

- Kort, koder och nycklar för olika förvaringsutrymmen och platser.
- Byggnadstekniska åtgärder kan vara att en byggnad har delats in i olika sektioner. Det kan också vara uppsatta lås, stängsel och larm samt kameraövervakning.
- Inre och yttre bevakning innebär rutiner och åtgärder för att kontrollera att ingen obehörig finns kvar i byggnaden eller i närområdet.
- Passerkontroll, till exempel vakter som kontrollerar och registrerar in- och utpasserande eller passerkort med tillhörande personliga koder.

Exempel på platser eller anläggningar kan vara serverrum, plats för reservkraft, ställverk m m.

3.5 Personalsäkerhet

3.5.1 Säkerhetsprövning

Säkerhetsprövning ska göras innan en person deltar i säkerhetskänslig verksamhet. Prövningen ska klarlägga om personen kan antas vara lojal mot de intressen som ska skyddas enligt säkerhetsskyddslagen och i övrigt är pålitlig ur säkerhetssynpunkt. Prövningen ska innefatta en grundutredning samt registerkontroll, vilken är ett underlag i säkerhetsprövningen. Den som berörs ska lämna sitt samtycke och delge de uppgifter som krävs. Regionen genom SSC är ansvarig för prövningen.

Säkerhetsprövning kan bl a grunda sig på:

- personlig kännedom om den person prövningen gäller
- uppgifter som framgår av till exempel betyg, intyg och referenser samt
- uppgifter från registerkontroll och särskild personutredning som kan ingå som en del i prövningen.

3.5.2 Säkerhetsklasser

En anställning eller ett annat deltagande i säkerhetskänslig verksamhet ska placeras i säkerhetsklass enligt följande:

- I *säkerhetsklass 1*, om den anställde eller den som på annat sätt deltar i verksamheten i en omfattning som inte är ringa får del av uppgifter i informationssäkerhetsklassen *kvalificerat hemlig*, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka synnerligen allvarlig skada för Sveriges säkerhet.
- I *säkerhetsklass 2*, om den anställde eller den som på annat sätt deltar i verksamheten i en omfattning som inte är ringa får del av uppgifter i informationssäkerhetsklassen *hemlig* eller i ringa omfattning får del av uppgifter i informationssäkerhetsklassen *kvalificerat hemlig*, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka allvarlig skada för Sveriges säkerhet.
- I *säkerhetsklass 3*, om den anställde eller den som på annat sätt deltar i verksamheten i en omfattning som inte är ringa får del av uppgifter i informationssäkerhetsklassen *konfidentiell* eller i ringa omfattning får del av uppgifter i informationssäkerhetsklassen *hemlig*, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka en inte obetydlig skada för Sveriges säkerhet.

Det är regionen som beslutar om vilka tjänster som ska placeras i säkerhetsklass. Regionen kräver svenskt medborgarskap för att få anställning på en säkerhetsklassad befattning.

3.5.3 Registerkontroll

Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller lagen (2010:362) om polisens allmänna spaningsregister. Med registerkontroll avses också att uppgifter hämtas som behandlas med stöd av polisdatalagen (2010:361).

Särskild personutredning

Denna ska göras vid registerkontroll som avser anställning eller annat deltagande i verksamhet som placerats i säkerhetsklass 1 eller 2.

4 Säkerhetsskyddad upphandling

Regionen ska pröva om upphandlingen helt eller delvis ska säkerhetsskyddas. Det som avgör om en upphandling ska säkerhetsskyddas eller inte är om företaget kan få del av SSKU i förfrågningsunderlaget eller under uppdragets utförande.

Vid tveksamheter ska SSC pröva om upphandlingen helt eller delvis ska omges av säkerhetsskydd.

Om upphandlingen ska säkerhetsskyddas ska regionen träffa ett skriftligt *säkerhetsskyddsavtal* innan affärsavtalet träffas.

Säkerhetsskyddsavtalet är en överenskommelse om det säkerhetsskydd som behövs i det särskilda fallet. När ett säkerhetsskyddsavtal har ingåtts ska företaget upprätta en *säkerhetsskyddsinstruktion*. I instruktionen, som ska godkännas av regionen, ska företaget redovisa vilka säkerhetsskyddsåtgärder de kommer att vidta.

Om företaget ska hantera och förvara SSKU i sina egna lokaler ska regionen också besöka företaget för att kontrollera att lokaler och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt.

Alla som ska delta i uppdraget och som kan antas få del av SSKU ska säkerhetsprövas. Om uppdraget är placerat i säkerhetsklass ska även en registerkontroll göras. De som får del av SSKU ska upplysas om den tystnadsplikt som gäller för uppgifterna.

När uppdraget är avslutat ska regionen säga upp säkerhetsskyddsavtalet. Regionen ska också se till att exempelvis nycklar och passerkort återlämnas, koder till larm ändras samt ev behörighet i IT-system med mera avslutas. Regionen ska meddela Säpo när ett säkerhetsskyddsavtal har ingåtts eller upphört att gälla.

5 Utbildning och kontroll

Regionen har skyldighet att se till så att personal som har säkerhetsprövats får utbildning i frågor om säkerhetsskydd. Därutöver ska regionen se till att det finns ett tillfredsställande säkerhetsskydd hos aktiebolag, föreningar och stiftelser över vilka regionen utövar ett rättsligt bestämmande inflytande samt hos anbudsgivare och leverantörer med vilka har träffats säkerhetsavtal.

Regionens SSC och ersättare ska ha genomfört utbildning i säkerhetsskydd. Andra berörda i regionen, vilka i mindre eller större omfattning kommer att hantera SSKU ska orienteras om lag, förordning och föreskrifter. Denna utbildningsuppgift åligger SSC.