Länsstyrelsen
GOTLANDS LÄN

FÖRSVARSMAKTEN

Totalförsvar för ett starkare Gotland

Slutrapport för regeringens uppdrag till Försvarsmakten och Länsstyrelsen i Gotlands län

Bilaga 3: Regler för hantering av hemlig information

Utgiven av: Länsstyrelsen i Gotlands län

Slutrapportens diarienummer: 459-3824-2017

Kontaktperson: Martin Gouthering, Länsstyrelsen i Gotlands Län

Tryckår: 2022

Slutrapporten med bilagor finns att hämta i PDF-format på Länsstyrelsens webbplats: www.lansstyrelsen.se/gotland

Länsstyrelsen
GOTLANDS LÄN

Datum
2020-06-09

Dnr
108-2362-2020

Regler för hantering av hemlig information

Länsstyrelsen Gotlands län

POSTADRESS
621 85 VISBY

BESÖKSADRESS
Visborgsallén 4

TELEFON
010-223 90 00

E-POST
gotland@lansstyrelsen.se

WEBBPLATS
www.lansstyrelsen.se/gotland

De som medverkat i beslutet.

Beslut i detta ärende har fattats av landshövding Anders Flanking efter föredragning på länsledningsmöte av säkerhetsskyddschef Martin Gouthering. I beredningen av ärendet har registrator Lena Norén, handläggare Marie-Louise Hellqvist och arkivarie Hanna Johansson deltagit. Beslutet gäller tillsvidare.

Visby den ..... juni 2020

Anders Flanking

Innehåll

1 Regler för hantering av säkerhetsskyddsklassificerad information

1.1 Bakgrund

Med säkerhetsskydd[1] avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter[2].

Säkerhetsskyddslagstiftningen regleras i säkerhetsskyddslagen och säkerhetsskyddsförordningen, vilka träder ikraft den 1 april 2019. Säkerhetspolisens föreskrifter för säkerhetsskydd reglerar närmare vad som ska beaktas i säkerhetsskyddshänseende.

Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.[3]

Säkerhetsskyddet ska gällande informationssäkerhet:[4]

1. Förebygga att säkerhetsskyddsklassificerade uppgifter röjs, ändras, görs otillgängliga eller förstörs och
2. Förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt som avses i 1.
3. Regler kring myndighetens administrativa hantering av säkerhetsskyddsklassificerad information återfinns i detta dokument.

1.2 Säkerhetsskyddsklasser

Säkerhetsskyddsklassificering av information regleras i Säkerhetsskyddslagen.[5] Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelning i säkerhetsskyddsklasser ska göras enligt följande:

---

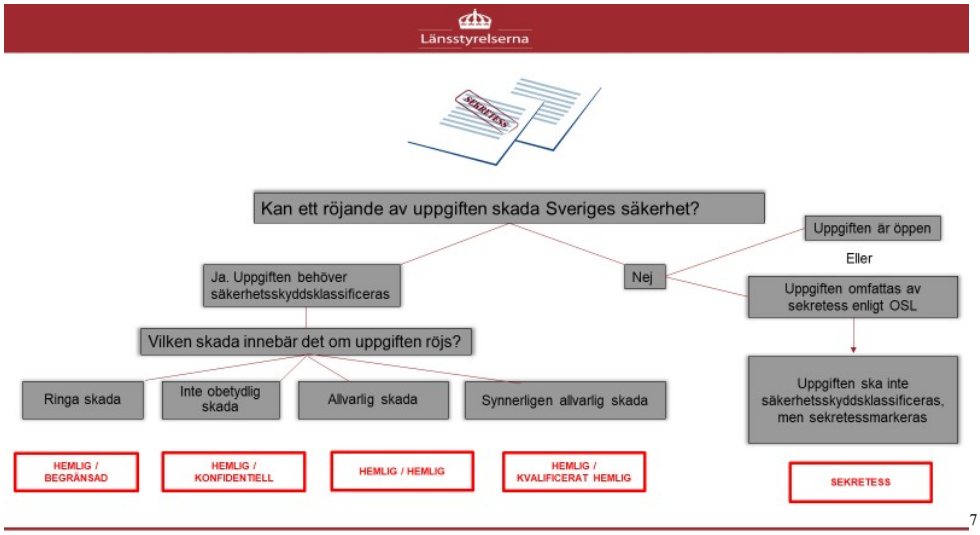
[1] 1 kap. 2 § 1 st Säkerhetsskyddslagen (2018:585)
[2] Se PMFS 2019:2 Säkerhetspolisens föreskrifter om säkerhetsskydd
[3] 1 kap. 2 § 2 st Säkerhetsskyddslagen (2018:585)
[4] 2 kap. 3 § Säkerhetsskyddslagen (2018:585)
[5] 2 kap. 5 § Säkerhetsskyddslagen (2018:585)

1. kvalificerat hemlig vid en synnerligen allvarlig skada,
2. hemlig vid en allvarlig skada
3. konfidentiell vid en inte obetydlig skada, eller
4. begränsat hemlig vid endast ringa skada

Att klassificera information för högt kan medföra att de som behöver ta del av informationen inte får det. Att klassificera informationen för lågt kan medföra sämre skydd och risk att någon obehörig tar del av den. Som Informationssäkerhetsinstruktionen betonar delar vår myndighet in information i tre klasser[6]:

1. Öppen information (Information som inte omfattas av någon sekretessbestämmelse i OSL)
2. Sekretessbelagd information (Information som omfattas av en sekretessbestämmelse i OSL)
3. Säkerhetsskyddsklassificerad information (Information som omfattas av en sekretessbestämmelse i OSL och som har betydelse för Sveriges säkerhet)

Modellen nedan kan användas som stöd.



[6] Se Informationssäkerhet. Instruktion för anställda på Länsstyrelsen Gotlands län, s. 4

[7] Framtagen inom ramen för projektet Säkra kommunikationer av Martin Gouthering och Per Cavalli Björkman

1.3 Behörig att ta del av hemlig information

Personalsäkerhet ska[8]:

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

Behörig att ta del av säkerhetsklassificerade uppgifter eller i övrigt delta i säkerhetskänslig verksamhet får endast den som[9]:

1. Har bedömts pålitlig från säkerhetssynpunkt,
2. Har tillräckliga kunskaper om säkerhetsskydd, och
3. Behöver uppgifterna eller annan tillgång till verksamheten för att kunna utföra sitt arbete eller på annat sätt delta i den säkerhetskänsliga verksamheten.

Den som genom anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas.[10] Säkerhetsprövningen syftar till att klarlägga om en person kan antas vara lojal mot de intressen som skyddas i denna lag och i övrigt är pålitlig från säkerhetssynpunkt. Vid säkerhetsprövningen ska sådana omständigheter beaktas som kan antas innebära sårbarheter i säkerhetshänseende.[11]

För Länsstyrelsen i Gotlands län innebär det att behörig att ta del av säkerhetsklassificerade uppgifter eller i övrigt delta i säkerhetskänslig verksamhet får endast den som:

- Har genomgått säkerhetsprövning och är inplacerad i säkerhetsklass
- Har genomgått utbildning i säkerhetsskydd vid myndigheten
- Har behov av uppgifterna för att kunna utföra sitt arbete eller annars delta i viss säkerhetskänslig verksamhet

[8] 2 kap. 4 § Säkerhetsskyddslagen (2018:585)
[9] 2 kap. 3 § Säkerhetsskyddsförordningen (2018:658)
[10] 3 kap. 1 § Säkerhetsskyddslagen (2018:585)
[11] 3 kap. 2 § Säkerhetsskyddslagen (2018:585)

2 Livscykelhantering av säkerhetsskyddsklassificerad information

Nedan tecknas en bild av livscykeln för säkerhetsskyddsklassificerad information.[12]

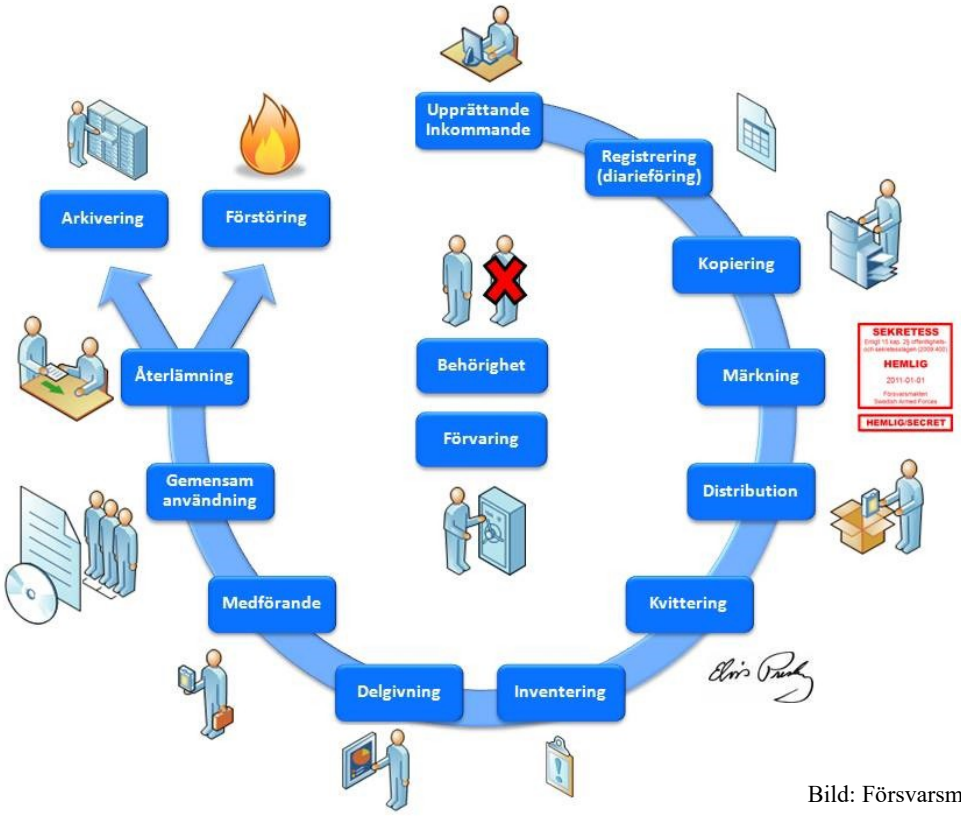


Bild: Försvarsmakten

Varje steg i livscykeln och den administrativa hanteringen av säkerhetsskyddsklassificerad information beskrivs i de följande avsnitten. Säkerhetspolisens föreskrifter gällande säkerhetsskydd anger de minimiregler som gäller för hantering av säkerhetsskyddsklassificerade uppgifter i en verksamhet.[13]

Säkerhetspolisens föreskrifter anger att en verksamhetsutövare ska ha rutiner för behandling av säkerhetsskyddsklassificerade uppgifter och handlingar.[14]

---

[12] Ur Försvarsmaktens handbok i informationssäkerhet s. 85
[13] Se 3 kap. PMFS 2019:2 Säkerhetspolisens föreskrifter om säkerhetsskydd
[14] 3 kap. 3 § PMFS 2019:2 Säkerhetspolisens föreskrifter om säkerhetsskydd

I fortsättningen används begreppen säkerhetsskyddsklassificerad och hemlig synonymt.

1.4 2.1 Inkommen och upprättad information

För hemlig information finns det ett absolut registreringskrav, vilket innebär att **all hemlig information** som antingen inkommer eller upprättas vid myndigheten enligt lag snarast ska registreras.[15]

Information som är hemlig i någon av de 4 säkerhetsskyddsklasserna ovan kan antingen inkomma till myndigheten, förvaras eller upprättas vid myndigheten.

En handling är allmän när den inkommit, upprättats eller förvaras hos myndigheten. En handling kan inkomma på olika sätt (brev, mail, fax, fysisk överlämning) och i olika form (nedtecknat i skrift, digitalt med ett tekniskt hjälpmedel eller muntligen). En handling anses upprättad när den har expedierats eller när ärendet har slutbehandlats.[16]

Alla handlingar är inte allmän handling. Som exempel kan anges minnesanteckning eller arbetsunderlag som tillkommit endast som hjälpmedel under beredningen eller föredragningen av ett ärende, och som inte tillfört ärendet nytt sakmaterial.[17] En minnesanteckning som har gjorts hos en myndighet och som inte har expedierats ska inte heller efter den tidpunkt då den enligt 10 § är att anse som upprättad anses som allmän handling hos myndigheten.

Minnesanteckningen anses dock som upprättad om den har tagits om hand för arkivering. Utkast eller koncept till en myndighets beslut eller skrivelse och andra därmed jämställda handlingar som inte har expedierats anses inte som allmänna. Handlingen anses dock vara allmän om den tas om hand för arkivering.[18]

Allmänna handlingar kan vara offentliga eller sekretessbelagda. Huvudregeln är att allmänna handlingar är offentliga, men i vissa fall sekretessbeläggs en allmän handling med stöd av någon bestämmelse i Offentlighets- och sekretesslagen (OSL 2009:400). Sekretess innebär förbud att röja uppgift, vare sig det sker

[15] Jfr 5 kap. 1 § OSL, 3 kap. 7 § Säkerhetsskyddsförordningen (2018:658).
[16] Se 2 kap. 1-10 §§ Tryckfrihetsförordningen (1949:105)
[17] 2 kap. 12-13 §§ Tryckfrihetsförordningen (1949:105)
[18] 2 kap. 12 § Tryckfrihetsförordningen (1949:105)

muntligen eller genom att exempelvis lämna en sekretessbelagd handling vidare. Sekretessen för uppgiften gäller oavsett i vilken form den förkommer.[19]

Det ska tydligt framgå om en handling omfattas av sekretess samt vilket lagrum som ger stöd för detta. Sekretessen kring en handling prövas vid varje tillfälle då någon begär ut handlingen.

2.1.1 Inkommen information

Hemliga handlingar kan komma till myndigheten på följande sätt:

- Per post i sekretesspåse/säkerhetskuvert eller i dubbla kuvert i fysisk form eller i elektronisk form (krypterad e-post, digital lagringsmedia som exempelvis USB eller CD-skiva).
- Via kryptofax.
- Medarbetare medtar hemlig information som denne fått externt till myndighetens lokaler.
- En fysisk överlämning av hemlig information till myndigheten.

Följande regler gäller för hantering av inkommen information till myndigheten:

- Endast den som är behörig får mottaga hemlig information. Med behörig avses att mottagaren är säkerhetsprövad och inplacerad i säkerhetsklass.
- Den som är behörig är uppförd på behörighetsförteckning över behöriga medarbetare på Länsstyrelsen. Registraturen ansvarar för förvaring av behörighetsförteckningen. Säkerhetsskyddschefen ansvarar för att hålla behörighetsförteckningen uppdaterad.
- Den post som inkommer till myndigheten och som bedöms innehålla hemlig information tas omedelbart omhand av personal vid registraturen som ansvarar för vidare hantering.
- Post som bedöms innehålla hemlig information får endast överlämnas till behörig personal vid registratur. Registraturen låser in information som bedöms vara hemlig i säkerhetsskåp i avvaktan på att mottagaren av handlingen ska delges handlingen. För det fall registratur inte finns närvarande ska posten som bedöms innehålla hemlig information tillfälligt överlämnas för förvaring till säkerhetsskyddschef.
- Post som innehåller hemlig information öppnas **ALLTID** av minst två personer samtidigt närvarande. Post öppnas antingen av personal ur registraturen och den mottagare som ska ha informationen (som är att anse som behörig att mottaga informationen) eller två ur personalen vid registraturen.

[19] 3 kap. 1 § Offentlighets- och sekretesslagen (2009:400)

- Den som mottar hemlig post 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 kontaktas säkerhetsskyddschefen eller informationssäkerhetssamordnaren. Därefter ska avsändaren omedelbart underrättas. Om det uppkommer en misstanke om att en obehörig har tagit eller försökt ta del av innehållet i en försändelse med hemliga uppgifter kan straffansvar för vårdslöshet med hemlig uppgift bli aktuell[20].

2.1.2 Inkommen information

Innan du upprättar en handling ska du bedöma om handlingen kan komma att innehålla hemlig information eller inte. Ska du skapa ett dokument eller på annat sammanställa information som väntas bli hemlig *i någon av de 4 säkerhetsskyddsklasserna* ska nedanstående följas.

- Digitalt skapande av hemlig information får *enbart* får ske på särskilt avsedd och godkänd dator. Information som är hemlig i någon av de 4 säkerhetsskyddsklasserna får aldrig upprättas eller hanteras i Lst-IT- miljön, dvs på en bärbar eller stationär Länsstyrelsedator, mobiltelefon eller surfplatta.
- De standardiserade myndighetsmallarna som finns i det hemliga IT-systemet ska alltid användas. Av dessa framgår diarienummer, handlingsnummer, säkerhetsskyddsklass, sidnummer, sidantal, datum och författare och sändlista.
- Det ska framgå av en myndighetsmall för sändlista hur många exemplar av den hemliga handlingen som har framställts och vilka som är mottagare av dessa. Ett missiv eller en ärendemening ska inte innehålla någon hemlig uppgift.
- Mottagarens kontaktuppgifter ska framgå av sändlistan (exv. postadress, kryfaxnummer).
- Kontakta registratur om du behöver starta ett nytt ärende med ett nytt diarienummer.
- Handlingen ska alltid åsatt ett av myndigheten framtaget diarienummer.

2.1.3 Hemligt arbetsmaterial

[20] Jfr. 18 kap. 9 § Brottsbalken

Hemlig information kan upprättas vid myndigheten och då vara under bearbetning/framtagande, det som vanligen benämns som hemligt arbetsmaterial. Hemlig information betraktas som hemligt arbetsmaterial till dess det är upprättat i form av att en handling är utskriven eller man har skrivit för hand på en handling.

De hanteringsregler som omnämns i detta dokument gäller **ALLA** former av hemlig information, oavsett i vilken form de förekommer (i fysisk form, på digitalt lagringsmedium, föremål etc.) eller i vilket stadium de behandlas (som hemligt arbetsmaterial eller en diarieförd hemlig handling).

Om en avsändare har säkerhetsskyddsklassificerat en handling som inkommer till myndigheten och stämplat den som hemligt arbetsmaterial följer handlingen likafullt samma hanteringsregler som för slutbehandlad och diarieförd hemlig information vid Länsstyrelsen Gotland. Om hemlig information upprättas vid eller inkommer till myndigheten ska den diarieföras direkt och erhålla ett diarienummer, handlingsnummer, säkerhetsskyddsklass etc. Den informationen kommer sedan att registreras av registraturen.

För användaren innebär ovan i praktiken att en handling som ska upprättas – och som kanske ska remitteras internt – kommer att registreras och kvitteras enligt reglerna i detta dokument. För användaren blir det ett synsätt som närmast kan liknas vid versionshantering. Även om användaren vet att det är version 1 och att det sannolikt kommer fler versioner, så kommer det erhålla ett diarienummer och handlingsnummer. Om det blir version 2, 3 och 4 och så vidare kommer varje enskild version att ha ett unikt handlingsnummer. Detta görs av följande skäl:

- För att skapa spårbarhet för varje handling
- För att undvika säkerhetsskyddsincidenter
- För att kunna utreda inträffade säkerhetsskyddsincidenter

1.5 2.2 Registrering och diarieföring

När informationen inkommit till eller upprättats vid myndigheten och mottagits av behörig personal överlämnas den till registratur för hantering enligt nedan:

- Registratorn diarieför handlingen i Platina där enbart en handlingsrubrik skrivs in. Handlingen diarieförs oavsett om det är markerat som arbetsmaterial eller inte men läggs inte fysiskt in i Platina då hemlig information ALDRIG får hanteras på en

Lst-IT dator.
- Ett ärendekort upprättas i Platina.
- Första handlingen i Platina-ärendet är en tjänsteanteckning vid ärenden som upprättas vid myndigheten.
- VÄS-kod anges.
- Säkerhetsskyddsmarkering med angivande av lagrum görs i Platina.
- Publicering i WEB-diarium kryssas ur.
- Handlingen stämplas på förstasidan med **säkerhetsskyddsstämpel** med angivande av lagrum och datum. Samtliga sidor ska säkerhetsskyddsmarkeras med stämpel.
- Om ett lagringsmedium med hemlig information inkommit ska detta märkas med säkerhetsskyddsklass och identifieringsuppgift (spårbarhet till diarienummer). Märkningen fästs på USB-minnet. CD-skivas uppmärks med märkpenna. Informationen på lagringsmediet ska alltid skrivas ut.
- Den utskrivna handlingens säkerhetsskyddsklassificering finns angiven längst upp till höger på dokumentet.
- Säkerhetsskyddsmarkering med angivande av lagrum görs om inte den redan finns på de utskrivna sidorna. Samtliga sidor ska vara säkerhetsskyddsmarkerade.

1.6 2.3 Kopiering och kvittering

När handlingen diarieförts i Platina vidtas följande åtgärder:

- Handlingen kopieras på H-kopiator (särskilt avsedd kopiator där hemliga handlingar ska kopieras). Kopiering av hemlig handling får endast utföras på registraturen och endast utföras på där avsedd och godkänd kopiator.
- Kopian av handlingen behåller handläggaren. Originalet sparas i diariet hos registraturen tillsammans med eventuellt lagringsmedium.
- Handläggaren kvitterar antal exemplar denne har på ett delgivningskvitto enligt vad som framgår.
- Delgivningskvittot (grön och rosa del) förvaras tillsammans med originalhandlingen i det hemliga diariet samt i särskild pärm.
- Handläggaren erhåller blå och gul del av delgivningskvittot som förvaras tillsammans med kopian av den hemliga handlingen.

1.7 2.4 Kommunikation av hemlig information

Vid kommunikation av hemlig information krävs kryptolösningar som är godkända av Försvarsmakten, så kallade signalskyddsystem. Signalskydd är system och åtgärder som syftar till att förhindra

obehörig insyn i och påverkan av telekommunikations- och IT-system. Med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder förhindras de hemliga uppgifterna från att manipuleras och kan också kommuniceras på ett korrekt och säkert sätt.

De kryptolösningar som är godkända för att kommunicera hemlig information upp till säkerhetsskyddsnivån HEMLIG/HEMLIG är:

- Krypterad fax (kryfax)
- Krypterad telefon (krytel)
- MGS-dator

För mer information kring användning av myndighetens signalskyddsmateriel kontaktas Länsstyrelsens signalskyddschef.

1.8 2.5 Distribution av hemlig information

En hemlig handling i någon av de fyra säkerhetsskyddsklasserna ***kan*** delges en part på något av följande sätt:

- Genom att sändas som rekommenderad post (REK-post).
- Genom att sändas via kryfax med ett försättsblad eller missiv.
- Genom att överlämna handlingen vid ett fysiskt möte (mottagaren måste vara behörig att ta emot handlingen) eller förevisa handlingen vid ett fysiskt möte utan att denna överlämas.
- Genom att sändas via MGS.
- Genom att kommuniceras muntligen via krytel eller under fysiskt möte (se 2.5.2).

En hemlig handling i någon av de fyra säkerhetsskyddsklasserna ***får*** delges en part på något av följande sätt:

Säkerhetsskyddsklass	Kryfax	REK-post	Kryfil MGS	Krytel	Fysisk överlämning
Begränsat hemlig	Ja	Ja	Ja	Ja	Ja
Konfidentiell	Ja	Ja	Ja	Ja	Ja
Hemlig	Ja	Ja	Ja	Ja	Ja
Kvalificerat hemlig[21]	Nej	Nej	Nej	Nej	Ja

[2121] Det som styr kommunicering av kvalificerat hemlig information via signalsskyddsmaterial är vilken/vilka inlästa nycklar som finns aktuella. Det sagda innebär att kvalificerat hemlig information *kan* kommuniceras via exempelvis kryfax under förutsättning att rätt signalsskyddsnycklar finns inlästa.

2.5.1 Delgivning av hemlig information – internt

Om hemlig handling ska delges inom myndigheten vidtas följande åtgärder:

- Handläggare ser till att det finns en komplett ifylld sändlista. Sändlista ska återfinnas tillsammans med all hemlig information som upprättas digitalt på myndigheten.
- Diariet förbereder kvittens.
- Registratur hör av sig till den eller de som har hemlig handling att kvittera ut och hämta.
- Den eller de som enligt sändlista ska ta del av hemlig handling går till registratur för att kvittera ut hemlig handling.
- Rutinen för kvittering under 2.3 följs.

2.5.2 Delgivning av hemlig information – externt

Om hemlig handling ska delges utom myndigheten vidtas följande åtgärder:

- Ansvarig handläggare ansvarar för att sändlistan är ifylld. Av sändlista ska kontaktuppgifter till mottagaren framgå för att registratur ska kunna se på vilket sätt och till vem hemlig information ska delges.
- Om en hemlig handling ska överlämnas vid ett fysiskt möte är handläggaren ansvarig för att på sändlistan ha påfört namn och organisation på den som ska delges handlingen.

2.5.3 Delgivning av hemlig information – externt

När hemlig information ska distribueras sker följande hantering.

- Registratur ansvarar för att sända REK-post med hemlig information i.
- REK-post som innehåller hemlig information ska alltid kunna spåras med angivande av handlingsnummer och försändelse-id.
- Handläggare kontaktar registratur för det fall man ska sända hemlig information.
- Hemlig handling som ska sändas som REK-post läggs i ett myndighetskuvert. På myndighetskuvert kan viss mottagaren anges (exv. att; Anna Andersson eller viss enhet/organisation). På myndighetskuvert ska det framgå att det innehåller information som är hemlig.
- Myndighetskuvert läggs sedan i ett säkerhetskuvertet, på vilken adress skrivs ut.

2.5.4 Delgivning av hemlig information – externt

Om hemlig information ska delges en part muntligen – via krytel eller under ett fysiskt möte – ska följande beaktas:

- Den som ska delge hemlig information är alltid skyldig att tillse att den eller de som ska mottaga hemlig information muntligen är behöriga.
- Den som ska delges hemliga uppgifter ska informeras om innebörden och räckvidden av sekretessen innan delgivning sker. Ansvaret för detta ligger hos den som avser att delge de hemliga uppgifterna.
- Om hemlig information ska kommuniceras muntligt under ett fysiskt möte mellan en eller flera personer ska risken för överhörning beaktas.
- Risken för obehörig avlyssning ska också beaktas vilket ställer krav på i vilka lokaler som hemlig information kan kommuniceras muntligt.
- Sårbarhetsreducerande åtgärder ska vidtas, vilket innebär att all elektronisk utrustning som avger RÖS (Röjande signaler) ska tas bort, ut ur ett rum före det att hemlig information delges muntligen.
- Det ska antecknas på blå del av kvittensset att information delgivits muntligen med angivande av namnteckning och namnförtydligande, datum. För det fall fler än 4 personer ska delges muntligen, exempelvis i samband med ett möte, ska delgivningslista för muntlig delgivning fyllas i.

1.9 2.6 Förvaring

En hemlig handling ska förvaras i ett förvaringsutrymme med en sådan skyddsnivå att den inte obehörigen röjs, ändras eller förstörs. Skyddsnivån ska motsvara stöldskyddsföreningens krav enligt SSF 3492 (tidigare SS 3492, alternativt SS 3493 som också skyddar mot brand) eller värdeskåp enligt svensk standard SS-EN 1143-1 (Grade 0-III) eller nyare med motsvarande krav.[22] Se även Riksarkivets föreskrifter RA-FS 2013:4 gällande vatten, skadlig fukt, brandgas etc. Vidare gäller följande regler för förvaring av hemlig information:

- Ansvarig handläggare förvarar den hemliga informationen i ett låst förvaringsutrymme som endast den person som kvitterat de hemliga handlingarna kan komma åt.
- Förvaringsutrymme för flera personer som innehåller låsbara innerfack för respektive person tilldelas efter det att säkerhetsskyddschef fattat beslut

[22] Jfr. 3 kap. 10 § PMFS 2019:2 Säkerhetspolisens föreskrifter om säkerhetsskydd

om samförvaring. Endast de personer som förvarar de hemliga handlingarna i ett förvaringsutrymme får ges tillträde till det.

- Det är inte tillåtet att ge ut kod eller nyckel till någon som inte har tilldelats ett låsbart innerfack i ett säkerhetsskåp.
- Nyckeln till respektive låsbart innerfack är individuell och ska förvaras på ett säkert sätt som förhindrar obehörig åtkomst till den.
- Kod och nyckel får aldrig förvaras tillsammans.
- Förvaring av kvalificerat hemlig handling beslutas av myndighetens chef eller säkerhetsskyddschefen och får endast ske på särskilt

anvisad plats i särskilt anvisat säkerhetsskåp.[23]
- Förlust av nyckel eller kod till säkerhetsskåp ska omedelbart rapporteras till säkerhetsskyddschefen eller den som denne utser i sitt ställe.
- USB-minne som används för säkerhetskopiering av hemlig information förvaras i särskild ordning efter direktiv av säkerhetsskyddschefen.

Varje medarbetare har ett ansvar att alltid beakta den sammanlagda mängden hemlig information som förvaras i visst förvaringsutrymme.

Beroende på mängd och art kan den aggregerade mängden information göra att andra förvaringsregler måste ombesörjas för att tillse att korrekt säkerhetsskyddsdimensionering hålls.

1.10 2.7 Medförande

Med medförande menas när en person i sin tjänsteutövning behöver ta med hemliga handlingar från myndighetens lokaler.[24] Om en hemlig handling ska medföras utanför myndighetens lokaler ska den hållas under omedelbar uppsikt eller förvaras på ett sätt som så långt som möjligt motsvarar det säkerhetsskydd som gäller för förvaringen av handlingen inom verksamhetens lokaler. Följande regler gäller för distribution och medförande av hemlig information vid myndigheten:

Distribution/Medförande - tillstånd krävs	**Kryfax**	**REK-post**	**Kryfil MGS**	**Krytel**	**Fysiskt medförande**
Begränsat hemlig	Nej	Nej	Nej	Nej	Ja
Konfidentiell	Nej	Nej	Nej	Nej	Ja
Hemlig	Nej	Nej	Nej	Nej	Ja
Kvalificerat hemlig[25]	Ja	Ja	Ja	Ja	Ja

1. Landshövding, länsråd eller säkerhetsskyddschef beslutar i varje fall om medförande av hemlig handling i samtliga säkerhetsskyddsklasser.

[23] Jfr. 3 kap. 11 § PMFS 2019:2 Säkerhetspolisens föreskrifter om säkerhetsskydd
[24] Jfr. 3 kap. 21-23 §§ PMFS 2019:2 Säkerhetspolisens föreskrifter om säkerhetsskydd
[25] Ej aktuellt för kryfax, MGS eller krytel.

2. Det finns således inget generellt tillstånd att medföra hemliga handlingar utanför myndighetens lokaler utan beslut tas i varje enskilt fall och ska dokumenteras på delgivningskvittot tillhörande ärendet i diariet.
3. För att medta en handling utanför myndighetens lokaler krävs alltid tillstånd oavsett vilken säkerhetsskyddsklass handlingen har.
4. Kvalificerat hemliga handlingar får överhuvudtaget inte tas med från myndigheten utan tillstånd av minst två personer i förening (landshövdingen, länsrådet eller säkerhetsskyddschefen). Beslut om sådant tillstånd måste fattas skriftligen i särskilt beslut som diarieförs i det ärende som handlingen som ska medföras hör till.
5. Ovanstående gäller även vid tjänsteresa utomlands.
6. MGS-dator får ALDRIG tas med från myndigheten.
7. Om USB-minne med hemlig information ska tas med från myndigheten måste ett USB-minne med bitlocker- och lösenordsfunktion användas.
8. USB-minnet ska märkas med säkerhetsskyddsklass och identifieringsuppgift (spårbarhet till särskilt diarienummer). Märkningen fästs på USB-minnet. USB-minnet ska förpackas i ett säkerhetskuvert och förvaras på ett säkert sätt.
   De överväganden som görs före det att ett beslut om medförande av hemlig handling fattas tar hänsyn till följande:

- för vilket ändamål den hemliga handlingen medförs och
- till vilka platser den hemliga handlingen ska medföras
- att den övriga hanteringen av den hemliga handlingen har följts enligt vad som framgår ovan (det vill säga att handlingen är diarieförd, originalhandlingen inlagd i det hemliga diariet och även i övrigt vederbörligt kvitterad och hanterad).
- När hemlig handling ska tas med utanför verksamhetens lokaler ska den:

9. Hållas under ständig uppsikt.
10. Förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av handlingen inom myndighetens lokaler.[26]
11. Handlingen ska förvaras i förseglat emballage (säkerhetskuvert) så att eventuellt försök till intrång i emballaget kan uppmärksammas. Om förvaringen i säkerhetskuvert bryts – i samband med distribution av den hemliga handlingen – måste extra säkerhetskuvert medtas när handlingen ska återföras till myndigheten.
12. Handläggaren är ansvarig för att före det att handlingen ska medföras

[26] Som exempel härpå kan anges att det således inte är tillåtet att förvara en hemlig handling i exempelvis ett hotellrums säkerhetsfack då denna förvaring inte uppfyller kraven för förvaring av hemlig information.

med hjälp av registratur anteckna i listan för det hemliga diariet vem som ska medföra en handling, vart och när.

13. När handling är återförd till myndighetens lokaler – om det inte ska överlämnas till part – är den som medtagit handlingen skyldig att tillse att det antecknas i listan för det hemliga diariet att handlingen är återförd.
    Säkra förvaringsmöjligheter är ofta begränsade vid tjänsteresor. Ett USB-minne, en annan digital lagringsmedia eller en väska som innehåller en hemlig handling får inte lämnas obevakad i till exempel en bil, en tågkupé.

1.112.8 Användning och återlämning

Hemliga handlingar ska återlämnas till registraturen för införande i hemligt diarium i följande fall:

1. När ett ärende avslutas i vilket hemlig handling ingår.
2. När en handläggare som är ansvarig för ärende i vilket hemliga handlingar ingår byter tjänst internt.
3. När en handläggare som är ansvarig för ärende i vilket hemliga handlingar ingår slutar sin tjänst.

1.12 2.9 Arkivering och förstöring

När ett ärende som innehåller hemlig handling ska avslutas gäller följande hantering:

1. Handläggare fyller i beslutsdatum och avslutsdatum (som är samma datum) i Platina och avslutar ärendet i Platina.
2. Handläggare underrättar registratur att ärende har avslutats som innehåller hemlig information.
3. Samtliga kopior av den hemliga handlingen ska återlämnas till registratur för att förstöras.
4. Den hemliga originalhandlingen ska arkiveras i det hemliga arkivet. Detsamma gäller för digitala lagring medium som finns i ett ärende.
5. Kvittens skrivs under av registrator och handläggare att en hemlig handling återlämnats eller att alla kopior har förstörts. Kvittensen förvaras hos myndigheten i minst 10 år. Är informationen kvalificerat hemlig ska kvittensen förvaras i 25 år.[27]
6. Handläggare får rosa del av kvittoset från registratur som bevis

[27] Se 3 kap. 17 § PMFS 2019:2 Säkerhetspolisens föreskrifter om säkerhetsskydd

för att handling är återlämnad.

7. Handläggare förvarar rosa del av kvittoset för att kunna visa upp denna i samband inventering.

För förstöring av kopior av hemliga handlingar gäller följande:

1. Samtliga kopior av den hemliga handlingen ska förstöras.
2. Förstöringen ska **ALLTID** genomföras av minst 2 behöriga personer i förening.
3. Hemliga handlingar eller utrustning som innehåller hemliga uppgifter ska förstöras på sådant sätt att åtkomst och återskapande av uppgifterna omöjliggörs under hela destruktionsprocessen. Kvittensetets blå del sätts i särskild pärm i datumordning (förstöringsliggare).
4. Förstöring ska ske maskinellt.
5. För maskinell förstöring ska särskilt anvisade dokumentförstörare användas.
6. För bränning av hemliga handlingar gäller särskild rutin som säkerhetsskyddschef är ansvarig för.

För gallring av hemliga originalhandlingar gäller följande:

1. Notera att gallring av allmänna handlingar för statliga myndigheter ska ske enligt särskilda föreskrifter som meddelats av Riksarkivet och gällande lagar på området, däribland Arkivlagen (1990:782).
2. Gallringen ska **ALLTID** genomföras av minst 2 behöriga personer i förening.
3. Hemliga handlingar eller utrustning som innehåller hemliga uppgifter ska gallras på sådant sätt att åtkomst och återskapande av uppgifterna omöjliggörs under hela destruktionsprocessen.

Förstöringen ska dokumenteras i särskild förstöringsliggare.

Om en hemlig handling hanteras på ett vårdslöst sätt och en hemlig uppgift röjs, kan straffansvar för vårdslöshet med hemlig uppgift komma att bli aktuell. Om hemlig handling inte funnits under omedelbar uppsikt eller på annat sätt kan ha röjts ska du omedelbart upprätta en incidentrapport och skicka denna till säkerhetsskyddschefen.

Misstänker Länsstyrelsen att hemlig uppgift kan ha röjts ska detta skyndsamt anmälas till Säkerhetspolisen (SÄPO) om röjandet kan innebära men för Sveriges säkerhet som inte endast är ringa.[28]

Istället för att medföra en hemlig handling på resa, vilket medför betydande risker, kan följande sätt användas för att riskreducera hanteringen:

1. I förväg sända den hemliga handlingen via krypterad fax (kryfax) till mottagaren.
2. I förväg sända den hemliga handlingen via krypterad fil med MGS till mottagaren.
3. I förväg sända den hemliga handlingen som rekommenderad post (REK-post) i ett kuvert som sedan läggs i ett säkerhetskuvert. På säkerhetskuvertet ska det inte framgå att det är fråga om en hemlig handling som finns i säkerhetskuvertet. Därför ska ingen HEMLIG-stämpel åsättas på säkerhetskuvertet. HEMLIG-stämpel åsätts som framgår ovan enbart på kuvert som placeras i säkerhetskuvert.
I vissa fall är emellertid inget av ovanstående lämpligt då informationen är av sådan art och karaktär att den inte bör förevisas mottagaren i förväg. Reglerna för medförande som finns ovan ska då följas.

1.13 2.10 Inventering

Följande regler gäller för inventering av hemlig information (såväl fysiska handlingar som digitala lagringsmedia):

1. Alla hemliga handlingar som är utkvitterade och hemliga handlingar i öppna ärenden ska inventeras minst en gång per år. Säkerhetsskyddschef är tillsammans med utpekad i registratur ansvarig för att myndighetens hemliga information inventeras minst en gång per år.
2. Inventeringen ska protokollföras i inventeringsprotokoll.
3. Inventeringsprotokoll registreras och diarieförs i ärende i Platina.
4. Protokollet innehåller uppgifter om vilka personer som har genomfört inventeringen, om någon hemlig handling saknas samt en samlad sammanfattning av genomförd inventering.
5. I samband med inventering kan personal komma att kallas för att förevisa exemplar av hemlig handling.

1.14 2.11 Begäran om utlämnande av hemlig information

[28] 2 kap. 10 § Säkerhetsskyddsförordningen (2018:658)

När en begäran om utlämnande av en handling som är hemlig inkommer till myndigheten gäller följande:

1. Begäran om utlämnade av en hemlig handling inkommer till registraturen eller handläggare.
2. Registrator kontaktar – efter kontroll i hemligt diarium – ansvarig handläggare hos vilken kopia av den hemliga handlingen förvaras.
3. Handläggaren avgör om handlingen är en allmän handling eller inte; vid behov hämtas stöd av den som upprättat handlingen alternativt jurist, säkerhetsskyddschef eller informationssäkerhetssamordnare.
4. Säkerhetsskyddsklassbedömning görs av handläggaren och avgör om den allmänna handlingen omfattas av sekretess enligt offentlighets- och sekretesslagen till del, helt eller inte alls.
5. Bedöms delar av den hemliga handlingen kunna lämnas ut ska resterande del som inte ska lämnas ut maskas (det som är sekretessbelagt ska tas bort) innan utlämnande.
6. Vid maskning av handlingen ska en svart överstrykningspenna användas. Därefter ska den maskade texten kopieras i H-kopiatorn av registrator. Alternativt sker maskning i ordbehandlingsprogram på MGS där informationen har upprättats.
7. Om hela handlingen bedöms som hemlig eller del av en handling bedöms som hemlig ska den som efterfrågat utlämnandet informeras om detta. Det ska alltid framgå en motivering till vilken sekretessbestämmelse enligt OSL som beslutet att inte lämna ut handlingen eller del av handlingen grundar sig på. Den som begär ut en hemlig handling ska meddelas att de har rätt att få ett överklagbart beslut om avslag på begäran om utlämnande.
8. Om ett överklagbart beslut om avslag på begäran om utlämnande önskas kontaktas jurist för att formulera ett överklagbart beslut.
9. Det ska på kvittensen antecknas att handlingen begärts utlämnad och även lämnats ut.
10. En kopia av den utlämnade (maskade) handlingen ska tillsammans med originalhandlingen förvaras i det hemliga diariet. En maskad handling ska inte förstöras utan förvaras i det hemliga diariet eller arkivet tillsammans med originalhandlingen.
11. Om det finns indikation på att en hemlig handling som begärs utlämnad även begärs utlämnad vid en eller flera andra
12. länsstyrelser ska jurist vid myndigheten underrättas. Detta för att en gemensam bedömning ska kunna göras i juristnätverket mellan berörda länsstyrelser.

Vid övervägande att använda möjligheten till sekretessförbehåll enligt OSL ska säkerhetsskyddschefen kontaktas. Denna möjlighet

kan användas när en myndighet finner risk för skada, men eller annan olägenhet som enligt en bestämmelse om sekretess hindrar att en uppgift lämnas till en enskild, kan undanröjas genom förbehåll som inskränker den enskildes rätt att lämna uppgiften vidare eller utnyttja den.[29]

Den som efterfrågat utlämnandet av den allmänna handlingen och som nekas ska alltid informeras om rätten att överklaga beslutet. Utlämnade av en allmän handling som är av synnerlig betydelse för rikets säkerhet (kvalificerat hemlig) ska prövas enligt 1 § offentlighets- och sekretessförordning (2009:641).

1.15 2.12 Intern begäran om att ta del av hemlig handling ur myndighetens hemliga diarium eller arkiv

Om en medarbetare önskar ta del av hemlig information som finns i myndighetens hemliga diarium eller arkiv (genom sökning i hemligt diarium eller hemligt arkiv eller genom att utfå en specifik hemlig handling) gäller följande:

1. Medarbetaren ska vara behöriga att ta del av hemlig information.
2. Medarbetare måste ha behov av informationen för sin tjänst och i sin tjänst.
3. Medarbetaren gör en beställning hos registraturen på särskild beställningsblankett.
4. Registraturen samverkar med landshövding, länsråd eller säkerhetsskyddschef angående en behovsbedömning om en person är behörig att ta del av informationen.
5. Beställningsblanketten godkänns av landshövding, länsråd eller säkerhetsskyddschef.

1.16 2.13 Överträdelse av riktlinjerna i denna instruktion

Om det framkommer att reglerna i denna instruktion överträtts kommer ärendet att utredas av säkerhetsskyddschef i samråd med ansvarig enhetschef och länsledning.

[29] Se 10 kap. OSL (2009:400)