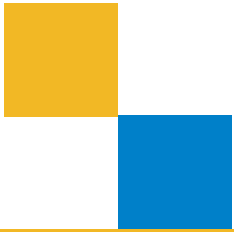




Ystads kommun



Rutin för säkerhetsskyddsklassificerade uppgifter

RUTIN

Aktiverande - Vad vi vill uppnå

Program

Är vägledande och beskriver önskvärd utveckling av verksamheten.

Strategi

Utgör grund för prioritering och beskriver hur kommunen ska uppnå uppsatta mål inom ett område.

Plan

Konkreta mål och åtgärder och svarar på vad, vem, när och hur.

Normerande - hur vi ska tänka och göra

Förhållningssätt

Vägleder och klargör Ystads kommuns övergripande syn och inställning till något.

Riktlinje

Säkerställer ett korrekt agerande och god kvalitet vid handläggning och utförande.

Rutin

Anger hur en fråga ska hanteras eller hur ett uppdrag ska verkställas.

Övrig dokumentinformation

Medverkande	T f kanslichef/kommunjurist Lisa Syrén Mandelkonvalj, kommunsekreterare Åsa Björkman Holmberg och säkerhetsstrateg Niklas Åkesson
Dokumentet gäller för	Ystads kommun
Gäller fr o m – t o m	2023-02-13 - tillsvidare
Fastställd av	Kommundirektör Randi Graungaard
För revidering ansvarar	Säkerhet- och beredskapschef
Ärendenummer	Ks 2023/60
Ansvarig för uppdatering	Säkerhet- och beredskapschef

Innehåll

1. Inledning	4
1.1 Målgrupp	4
1.2 Ansvar och organisation.....	4
1.3 Säkerhetsskyddschef	4
1.4 Säkerhetsskydd och säkerhetsskyddsklassificerade uppgifter	5
1.5 Säkerhetsskyddsanalys	5
1.6 Säkerhetsklassning	5
1.7 Behörighet att få ta del av säkerhetsskyddsklassificerade uppgifter 6	
1.8 Behörighetsförteckning	6
1.9 Säkerhetsprövningssamtal.....	6
1.10 Förvaring av dokumenterade säkerhetsprövningssamtal	7
2. Hanteringsrutiner	7
2.1 Vägledning för indelning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass.....	8
2.2 Indelning av säkerhetsskydds-klassificerade uppgifter	11
2.2.1 Anteckning om säkerhetsskyddsklass (märkning).....	11
2.2.2 Registrering.....	12
2.3 Märkning/diarienummer	15
2.4 Distribuering	15
2.5 Kvittering	19
2.6 Inventering	20
2.7 Återlämning	20
2.8 Arkivering och gallring (förstöring)	21

1. Inledning

Enligt säkerhetsskyddslagen (2018:585) samt säkerhetsskyddsförordningen (2021:955) åläggs det Ystads kommun att vidta förebyggande åtgärder för att skydda mot brott som kan hota Sveriges säkerhet och förebygga terroristbrott med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Ansvar för vad gäller säkerhetsskydd regleras även i rikspolisstyrelsens föreskrifter om säkerhetsskydd samt offentlighets- och sekretesslagen (2009:400). Dessa rutiner för säkerhetsskydd i Ystads kommun har upprättats i enlighet med bestämmelserna i säkerhetsskyddslagen och i säkerhetsskyddsförordningen.

1.1 Målgrupp

Målgrupp är alla inom kommunen som kommer i kontakt med eller hanterar säkerhetsskyddsklassificerade uppgifter. Målgruppen är således alla befattningar som hanterar säkerhetsskyddsklassificerade uppgifter. Utöver detta är målgrupp även säkerhetsklassad personal samt av kommunen utpekade registratorer som ska registrera säkerhetsskyddsklassificerade uppgifter.

1.2 Ansvar och organisation

Det yttersta ansvaret för säkerhetsskyddet i Ystads kommun vilar på kommunstyrelsen. Kommundirektören är ytterst ansvarig. Säkerhetsskyddschefen leder, samordnar och kontrollerar säkerhetsskyddsarbetet.

1.3 Säkerhetsskyddschef

Säkerhetsskyddschefen ansvarar för att stödja, följa upp och samordna kommunens säkerhetsskydd. Säkerhetsskyddschefen är direkt underställd kommundirektören. Säkerhetsskyddschefens ansvarsområden är som primär mottagare av säkerhetsskyddsklassificerade uppgifter exempelvis kontaktperson gentemot säkerhetspolisen och Försvarsmakten, ansvar för säkerhetsprövning och säkerhetsklassning samt genomförande av säkerhetsskyddsanalys och upprättande av säkerhetsskyddsplan. Säkerhetsskyddsplanen ska fastställas av säkerhetsskyddschefen.

1.4 Säkerhetsskydd och säkerhetsskyddsklassificerade uppgifter

Inom offentlig verksamhet är säkerhetsskyddsklassificerade uppgifter sådana uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).

Med säkerhetsskydd avses enligt säkerhetsskyddslagen:

- Skydd mot spioneri, sabotage och andra brott som kan hota Sveriges säkerhet.
- Skydd av uppgifter som omfattas av sekretess (hemliga uppgifter), enligt offentlighets- och sekretesslagen, och som rör Sveriges säkerhet.
- Skydd mot brott som innebär användning av våld, hot eller tvång för politiska syften (terrorism) även om brotten inte hotar Sveriges säkerhet.

Säkerhetsskyddets funktion ska utifrån detta särskilt beakta och förebygga:

- Att uppgifter som omfattas av sekretess och som berör Sveriges säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet).
- Att obehöriga inte får tillträde till platser där de kan få tillgång till uppgifter som avses i punkt ovan eller där verksamhet som har betydelse för Sveriges säkerhet bedrivs (tillträdesbegränsning), och
- att de personer som inte är pålitliga ur säkerhetssynpunkt deltar i verksamhet som har betydelse för Sveriges säkerhet (säkerhetsprövning).

1.5 Säkerhetsskyddsanalys

I säkerhetsskyddförordningen finns föreskrifter om säkerhetsskyddsanalys. Varje myndighet ska genomföra och dokumentera en säkerhetsanalys avseende vilka hot, risker och sårbarheter som kan påverka myndighetens säkerhetskänsliga verksamhet. En sådan säkerhetsskyddsanalys ska hållas uppdaterad. Säkerhetsskyddsanalysen ska utgå från en beskrivning av myndighetens verksamhet och organisation (verksamhetsanalys). Med säkerhetsskyddsanalys som grund ska en säkerhetsskyddsplan upprättas där lämpliga säkerhetsskyddsåtgärder anges.

1.6 Säkerhetsklassning

Säkerhetsklassning görs för de befattningar som kommer hantera säkerhetsskyddsklassificerade uppgifter eller på något sätt delta i säkerhetskänslig verksamhet. För säkerhetsklassade befattningar krävs säkerhetsprövning. Ystads kommun beslutar om placering i säkerhetsklass 2 och 3. Om kommunen bedömer att det finns behov av att placera en anställning eller befattning eller annat deltagande i säkerhetsklass 1, ska kommunen begära att regeringen beslutar om en sådan placering.

1.7 Behörighet att få ta del av säkerhetsskyddsklassificerade uppgifter

Information som omfattas av säkerhetsskyddslagen och säkerhetsskyddsförordningen får endast hanteras av behörig personal som bedöms pålitlig från säkerhetssynpunkt, besitter tillräckliga kunskaper om säkerhetsskydd samt är i behov av uppgifterna för sitt arbete i den verksamhet där de hemliga uppgifterna förekommer. Den som tillåts hantera hemliga handlingar ska upplysas om räckvidden samt innebörden av sekretessen.

1.8 Behörighetsförteckning

Behörighetsförteckningen tydliggör vilken befattning med tillhörande säkerhetsklass som får ta del av vilka uppgifter beroende på säkerhetsskyddsklass.

Säkerhetsklass	Information inom säkerhetsskyddsklass
Personer inom säkerhetsklass 1 får ta del av	Kvalificerat säkerhetsskyddsklassificerade uppgifter
Personer inom säkerhetsklass 2 får ta del av	Hemlig eller i ringa omfattning kvalificerat säkerhetsskyddsklassificerade uppgifter
Personer inom säkerhetsklass 3 får ta del av	Begränsat hemliga upp till konfidentiella säkerhetsskyddsklassificerade uppgifter

1.9 Säkerhetsprövningssamtal

Som en del i helhetsbedömningen avseende säkerhetsprövningen ingår att genomföra ett säkerhetsprövningssamtal. Samtalet ingår i den grundutredning som omfattar, registerkontroll och utbildning i säkerhetsskydd. Under säkerhetsprövning bedöms lojalitet, pålitlighet och sårbarhet hos den som prövas. Det är säkerhetsskyddschef tillsammans med utsedda personer med relevant och god insyn om säkerhetsskydd som genomför säkerhetsprövningssamtalet.

Viktiga frågeområden att behandla under ett säkerhetsprövningssamtal är:

- Utbildning (högskola, körkort, säkerhet, språk, militärt)
- Jobb (trivsel, tidigare arbetsgivare, umgänge, konflikter, ansvar)
- Brott (dömd, vänner/familj, utsatt)

- Lojalitet (familj, utländsk underrättelsetjänst, kriminella kontakter, medborgarskap)
- Ekonomi (lån, skulder, sparande, anmärkning, lön, tillgångar, utgifter, spel)
- Liv (vänner, fritid, digitalt fotavtryck, kriser, familj, resor, boende, alkohol)

Innan säkerhetsprövningssamtal ska säkerhetsskyddschef eller motsvarande gå igenom Säkerhetspolisens vägledning i säkerhetsskydd för personalsäkerhet. Säkerhetsprövningssamtal ska genomföras i trygg miljö som är lämpligt för samtal som är av integritetskänslig art. Uppföljning av säkerhetsprövningssamtal ska ske årligen av närmsta chef samt vid avslutande av anställning.

1.10 Förvaring av dokumenterade säkerhetsprövningssamtal

Dokumenterade säkerhetsprövningssamtal, registerutdrag samt besked/resultat av säkerhetsprövning ska förvaras av säkerhetsskyddschef så att ingen obehörig har åtkomst till dem. Handlingarna bedöms inte hamna i säkerhetsskyddsklass, men är av känslig karaktär för individens integritet och ska hanteras som sekretessbelagda uppgifter. Indelning och uppgifter om säkerhetsklass 2 hamnar under försvarssekretess och är därmed säkerhetsskyddsklassade uppgifter som ska hanteras enligt hanteringsrutiner listade nedan.

2. Hanteringsrutiner

Alla verksamheter är beroende av att kunna inhämta, lagra, bearbeta och kommunicera information i olika former. Den tekniska utvecklingen har på senare år gjort informationssystem till viktiga verktyg i hanteringen, men även pappersdokument används fortfarande. Dessa hanteringsrutiner är säkerhetsskyddsåtgärder som syftar till att skydda information oavsett form och förekomst, elektronisk såväl som fysisk.

Säkerhetskänslig verksamhet är verksamhet som är av betydelse för Sveriges säkerhet. För att säkerhetsskyddslagen ska vara tillämplig krävs inte att hela verksamheten ska utgöra säkerhetskänslig verksamhet, utan det är tillräckligt att någon del av verksamheten utgör säkerhetskänslig verksamhet. Uppgifter som kan omfattas av säkerhetsskyddslagen och som kan vara säkerhetsskyddsklassade (hemliga) kan till exempel röra verksamheter inom totalförsvaret, rättsväsendet, energi- eller vattenförsörjning, telekommunikation, livsmedelsförsörjning eller transportsektorn.

All säkerhetsskyddsklassificerad information i Ystads kommun som används eller hanteras enligt olika scenarion listade nedan ska skyddas mot hot oavsett hur den hanteras eller förvaras.

2.1 Vägledning för indelning av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass

Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen i säkerhetsskyddsklasser ska göras enligt följande:

- Kvalificerat hemlig
- Hemlig
- Konfidentiell
- Begränsat hemlig

Den typ av skada som röjande av information kan medföra ska graderas utifrån konsekvensnivåer, vilka är:

- Nivå A: Synnerligen allvarlig skada för Sveriges säkerhet
- Nivå B: Allvarlig skada för Sveriges säkerhet
- Nivå C: Inte obetydlig skada för Sveriges säkerhet
- Nivå D: Ringa skada för Sveriges säkerhet

Röjande av **kvalificerat hemlig** handling innebär synnerligen allvarlig skada för Sverige och har konsekvensnivå A.

Röjande av **hemlig** handling innebär allvarlig skada för Sverige och har konsekvensnivå B.

Röjande av **konfidentiell** handling innebär en inte obetydlig skada för Sverige och har konsekvensnivå C.

Röjande av **begränsat hemlig** handling innebär endast ringa skada för Sverige och har konsekvensnivå D.

Att klassificeringen ska ske utifrån den skada som ett röjande kan medföra för Sveriges säkerhet innebär att det inte ska beaktas vilken skada det kan medföra om uppgifterna blir otillgängliga för verksamhetsutövaren eller om de manipuleras och inte längre kan anses riktiga. Vid indelningen av uppgifter i säkerhetsskyddsklasser bör eventuella konsekvenser av ett röjande som framstår som helt orimliga inte beaktas. I stället för att utgå ifrån det värsta tänkbara scenariot bör bedömningen ske utifrån vad som är det värsta rimliga scenariot om uppgifterna röjs. Enligt samma princip bör man inte heller beakta vad som skulle hända om andra uppgifter skulle röjas vid samma tidpunkt. I annat fall riskerar indelningen i säkerhetsskyddsklasser att leda till att i princip samtliga uppgifter delas in i någon av de högre klasserna, vilket inte är syftet med lagstiftningen. I förarbetena till den nya säkerhetsskyddslagen ges ingen närmare förklaring till vad som avses med respektive skadenivå. Det är därför ytterst upp till rättstillämpningen att avgöra vad som utgör en skada för Sveriges säkerhet. Nedanstående värdeord kan dock tjäna som viss vägledning när det gäller indelning i säkerhetsskyddsklass.

Säkerhetsklass	Den skada som ett röjande av uppgifterna kan medföra	Värdeord till stöd för bedömningen om en viss typ av skada föreligger
Kvalificerat hemlig	Ett röjande kan medföra synnerligen allvarlig skada	Synnerligen allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa.
Hemlig	Ett röjande kan medföra en allvarlig skada	Allvarliga/betydande negativa konsekvenser, av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funktioner. Svårt att återställa.
Konfidentiell	Ett röjande kan medföra en inte obetydlig skada	Påtagliga negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott.
Begränsat hemlig	Ett röjande kan medföra endast ringa skada	Ringa negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning.
Ingen	Ingen skada på Sveriges säkerhet men kan medföra allvarliga informations-säkerhetsrisker	Negativa konsekvenser som kan medföra allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar eller på enskilda individ.

2.2 Indelning av säkerhetsskydds-klassificerade uppgifter

Nedanstående hanteringsrutiner är sammanställda utifrån scenarion. I respektive scenario anges rutiner för hantering av handlingar som finns reglerad för någon av ovanstående säkerhetsklasser.

Rutinerna är härledda från säkerhetsskyddslag (2018:585), säkerhetsskydds-förordningen (2021:955), Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2022:1 och Säkerhetspolisens vägledningsdokument för informations-säkerhet.

2.2.1 Anteckning om säkerhetsskyddsklass (märkning)

En säkerhetsskyddsklassificerad handling ska föras med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har, i syfte att klargöra vilka hanteringsregler som gäller för handlingen. Kravet på anteckning gäller både för fysiska och elektroniska säkerhetsskyddsklassificerade handlingar. Om det i samma handling förekommer uppgifter som är indelade i olika säkerhetsskyddsklasser ska den högsta säkerhetsskyddsklassen anges.

En säkerhetsskyddsklassificerad handling ska på första sidan föras med en anteckning. Om handlingen innehåller bilagor, ska varje bilaga på första sidan föras med den högsta säkerhetsskyddsklassen som uppgifterna i bilagan är placerade i. Ytterligare en stämpel för säkerhetsskyddsklass ska användas på övriga sidor om en säkerhetsklassificerad handling består av flera sidor. Om handlingen består av flera sidor ska sidan två och följande sidor stämplas med säkerhetsskyddsklassen som finns på första sidan. Den stämpeln visar dock enbart vilken säkerhetsklass som handlingen avser. Även bilagor som består av flera sidor ska märkas upp på samma sätt. Anteckning om säkerhetsskyddsklass ska göras för samtliga hemliga handlingar, oavsett säkerhetsskyddsklass.

Konfidentiella och begränsat hemliga handlingar ska föras med anteckning plus antal sidor och uppgift om bilagor.

Hemliga och kvalificerat hemliga handlingar ska föras med anteckning plus antal sidor och uppgift om bilagor samt exemplarnummer.

Begränsat hemliga, konfidentiella och hemliga handlingar ska föras med en anteckning som bör vara röd och omgärdas av en enkel ram. För kvalificerat hemliga handlingar bör anteckningen omgärdas av dubbel ram.

Endast de stämplat som är inköpta speciellt till Ystads kommuns hemliga handlingar godkänns.



Figur 1 – exempel på hur anteckningar kan formos för offentliga verksamhetsutövare (Säkerhetspolisen, 2019)

2.2.2 Registrering

Roller

Följande roller är iblandade i registrering av säkerhetsskyddsklassificerade uppgifter:

Registrator: Ansvarar för att diarieföra/registrera säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskyddschef: Ansvarar för att det finns riktlinjer för en säker hantering samt har kontrollansvaret att hanteringen av säkerhetsskyddsklassificerade uppgifter sker efter angivna riktlinjer.

Instruktion

Inkommande och utgående post

- Handlingar med säkerhetsskyddsklassificerade uppgifter som inkommer till organisationen får inte öppnas av personal som inte är säkerhetsklassad.
- Säkerhetsskyddsklassificerade uppgifter får aldrig distribueras med internposten.
- Säkerhetsskyddsklassificerade uppgifter ska skickas med postens värdepåse/rekommenderat brev.
- Posten ska överlämnas öppen till säkerhetsklassad registrator.

Postöppning och märkning av pappershandlingar

- Säkerhetsskyddsklassificerade uppgifter öppnas endast av Ystads kommuns utpekad säkerhetsklassad registrator.
- Säkerhetsskyddsklassificerade uppgifter ska hanteras omedelbart och hanteras genom hela processen tills den är inlåst. Den får aldrig lämnas oövervakad.
- En säkerhetsskyddsklassificerad uppgift ska som vanligt stämpas med datum när den inkommit men både inkomna och upprättade handlingar ska även förses med en sekretessmarkering.
- Innan en uppgift lämnas ut till någon, som begärt att få ta del av allmän handling, måste en sekretessprövning av innehållet göras oavsett om

handlingen är sekretessmarkerad eller inte enligt 5 kap. 5 § offentlighets- och sekretesslagen (2009:400).

Märkning av andra typer av lagringsmedia förutom papper

- Om andra lagringsmedium än papper används för uppgifter som är säkerhetsskyddsklassificerade så ska höljet på dessa förses med en anteckning (märkning) om den högsta säkerhetsklasslagringsmediet är avsett för. Bestämmelsen gäller såväl lagringsmedier som en person har kvitterat ut för personligt tjänstebruk, som lagringsmedier som används för drift och säkerhetskopiering, till exempel i en server.
- Med hölje avses den yttersta delen som omsluter lagringsmediet, till exempel utsidan på en hårddiskcassett eller ett USB-minne.
- Vissa fast monterade lagringsmedier, vanligtvis sådana som är avsedda för drift och säkerhetskopiering, är inte alltid möjliga att märka. Om lagringsmedierna inte kan märkas placeras istället märkningen synligt och i så nära anslutning till medierna som möjligt.
- För att märka upp andra lagringsmedia än papper finns klisterlappar anskaffade för ändamålet. Märkningen ska se likadan ut som den gör för pappershandlingar.

Ändring av märkning av handlingar och lagringsmedia

- Säkerhetsskyddschef tar beslutet om ändring och borttagning av märkning.
- Ändring av märkning sker genom att den ursprungliga märkningen överkorsas och en ny märkning tillförs tillsammans med en anteckning om datum för när ändringen görs. Det ska även framgå vem som beslutat om ändringen och när.
- Borttagning görs genom att märkningen överkorsas och datum för när borttagning gör antecknas. Det ska även framgå vem som genomfört borttagningen.
- Ändring och borttagning av märkning av säkerhetsskyddsklass kvalificerat hemligt sker efter att man kontaktat den myndighet som upprättat handlingen och fått ett samtycke.

Registrering i allmänna dokument- och ärendehanteringssystemet

- En säkerhetsskyddsklassificerad handling ska alltid registreras i kommunens ärende- och dokumenthanteringssystem. Existensen av en allmän handling får inte undanhållas allmänheten, även om uppgifterna om handlingen i registret som allmänheten har insyn i kan vara begränsade.
- En säkerhetsskyddsklassificerad handling i fysisk form **ska inte skannas** in i dokument- och ärendehanteringssystemet (diariet). Den ska ändå registreras i diariet med ankomst- eller utgåendedatum, diarienummer, avsändare eller mottagare samt beskrivning av handlingen (ärendemening) och ansvarig handläggare.
- En beskrivning av handlingen (ärendemening) kan till exempel formuleras på ett sådant sätt att den inte avslöjar några sekretesskyddade uppgifter men ändå anger vad det handlar om. Detta sätt underlättar återsökningen.
- Vid registreringen ska en bedömning göras om handlingen innehåller en uppgift som är sekretessbelagd. En märkning görs på den fysiska handlingen och elektroniskt i dokument- och ärendehanteringssystemet med aktuell sekretessparagraf. I normalfallet är det offentlighets- och sekretesslagen 15 kap. 2 § ("Skydd för Sveriges säkerhet") som gäller för kommuner och regioner.
- Den fysiska säkerhetsskyddsklassificerade handlingen ska förvaras i ett utrymme som motsvaras skyddsnivån för handlingen. I diariet ska det framgå var handlingen förvaras.

Register över säkerhetsskyddsklassade handlingar

I det utrymme som förvarar säkerhetsskyddsklassade handlingar ska det finnas en förteckning/register där det ska framgå:

- Datum då handlingen mottagits eller avsänts, diarienummer, avsändare och mottagare
- Beskrivning av handlingens innehåll i korthet
- Exemplarnummer
- Ansvarig handläggare
- Utlånad/återlämnad datum

2.3 Märkning/diarienummer

Exemplar av allmänna handlingar som är säkerhetsskyddsklassade ska kunna följas upp så att myndigheten vet var ett exemplar förvaras eller om det förkommit eller förstörts. Handlingen ska vara märkt med identifierade uppgifter som kan användas i ett register över exemplaren. Syftet är att uppnå spårbarhet för varje exemplar av sådana handlingar.

Roller

Säkerhetsskyddschefen: Ansvarar för att samtliga säkerhetsskyddsklassificerade uppgifter märks upp med rätt diarienummer.

Instruktion

- Märkningen ser ut enligt följande modell: Ordinarie diarienummer: exempel; Ks 2022/501–1(2) –
Ks=aktuell nämnd, 2022=År, 501=diarienummer, 1(2) exemplar 1 av 2

Denna märkning ska också medfölja andra lagringsmedia ex. hårddisk, USB, skrivare, kopiator och server.

- Ett säkerhetsskyddsklassificerat lagringsmedium ska märkas med identifieringsuppgift på höljet.
- Om lagringsmediet är fast monterat i utrustning som omöjliggör märkning på lagringsmediet ska märkningen i stället göras på utrustningen eller annan lämplig plats i anslutning till lagringsmediet.

2.4 Distribuering

För att en säkerhetsskyddsklassad uppgift oavsett om det är original, kopia eller utdrag ska kunna lämnas till en handläggare så måste uppgift om behörigheten som visar vilka handläggare/övriga anställda som är behöriga att ta del av informationen i en säkerhetsskyddsklassad uppgift finnas. Listan över vilken personal som är behörig att ta del av säkerhetsskyddsklassad information kallas distributionslista.

Roller

Följande roller är inblandade i distribution av säkerhetsskyddsklassificerade handlingar:

Registrator: Ansvarar för kopiering och överlämning av säkerhetsskyddsklassificerad uppgift till handläggare samt uppdaterar liggare. Ansvarar för upprättade handlingar, diariet för och uppdaterar liggare samt skickar i väg extern post. Ska säkerställa handläggares behörighet att ta del av säkerhetsskyddsklassificerad uppgift innan distribution.

Handläggare: Ansvarig handläggare mottar handling och ansvarar för förvaring. Överlämnar upprättade handlingar som säkerhetsskyddsklassats till registrator för registrering och expediering.

Personalansvarig chef: Ansvarar för att säkerhetsklassade handläggare förs upp på förteckningen över säkerhetsklassad/behörig personal.

Instruktion

Medförande

En säkerhetsskyddsklassificerad handling i säkerhetsklassen kvalificerat hemlig får inte medföras från Ystads kommuns lokaler utan tillstånd från säkerhetsskyddschefen. Särskilt godkännande krävs dessutom om handling ska tas med till utlandet. Vid försändelser till och från utlandet ska Utrikesdepartementets kurirförbindelse användas. Tillsynsmyndigheterna får medge undantag från detta krav. Undantagsfall är såvida inte handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarmakten.

Myndigheten ska besluta i vilken omfattning säkerhetsskyddsklassificerade handlingar och lagringsmedier som är placerade i säkerhetsskyddsklassen konfidentiell eller högre får medföras från myndighetens lokaler eller områden. Beslutet ska dokumenteras. Vid medförande utanför verksamhetsutövarens lokaler ska handlingen hållas under omedelbar uppsikt eller förvaras på ett sätt som motsvarar det säkerhetsskydd som gäller för förvaring inom verksamhetens lokaler. Undantagsfall är såvida inte handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarmakten.

Säkerhetsskyddsklassificerade handlingar och lagringsmedier som medförs från myndigheten ska vara under kontroll eller förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av handlingarna respektive lagringsmedierna inom myndighetens lokaler. En säkerhetsskyddsklassificerad handling eller ett säkerhetsskyddsklassificerat lagringsmedium som har medförts utanför myndighetens lokaler eller områden ska snarast möjligt återföras eller överlämnas till den som ska förvara handlingen eller lagringsmediet.

Utlämnande av säkerhetsskyddsklassificerade uppgifter (allmän hemlig handling)

Om en säkerhetsskyddsklassificerad uppgift begärs ut är det säkerhetsskyddschefen som alltid, oavsett säkerhetsklass, i samråd med handläggare som prövar om en handling och vad inom en handling som får lämnas ut.

Röjande av säkerhetsskyddsklassificerade uppgifter

Om säkerhetsskyddsklassificerade uppgifter (hemlig handling) försvinner eller om det befaras att säkerhetsskyddsklassificerade uppgifter har röjts ska detta med omedelbar verkan anmälas till kommunens säkerhetsskyddschef.

Utlämnande av säkerhetsskyddsklassificerade uppgifter

- Registrator ska innan överlämnande av säkerhetsskyddsklassificerade uppgifter till handläggare, säkerställa handläggarens behörighet mot distributionslistan över säkerhetsklassad handläggare/personal och tillse att de får ta del av säkerhetsskyddsklassificerade uppgifter.
- Kontrollera att handläggaren har behörighet att ta del av verksamhetsområdet som det gäller. Behörighet kan för handläggare gälla endast vissa typer av handlingar för att de ska kunna utföra sitt arbete.
- Det innebär att de inte får ta del av övriga säkerhetsskyddsklassificerade uppgifter inom andra verksamhetsområden än de är behöriga till.

Kopiering av säkerhetsskyddsklassificerade uppgifter

- I normalfallet är det originalet av den säkerhetsskyddsklassificerade uppgiften som lånas ut till behörig handläggare. Används den inte ska den vara inlåst i säkerhetsskåpet.
- Om handlingen behöver kopieras ansvarar registrator för att detta görs. Registratorn ska även säkerställa att exemplarhanteringen dokumenteras i kvittenslistan.
- Om man inte registrerar varje kopia i kvittenslistan så blir det en svartkopia, vilket innebär att myndigheten inte har kontroll över handlingarna. Svartkopior minskar skyddseffekten av att hanteringen av övriga exemplar är spårbar. En förlust av en svartkopia kan inte uppmärksammas i en inventering av säkerhetsskyddsklassificerade uppgifter då uppgift om kopian (exemplaret) saknas i registret över myndighetens säkerhetsklassificerade uppgifter.

Förvaring av säkerhetsklassificerade uppgifter

- En säkerhetsskyddsklassificerad uppgift ska vara under kontroll eller förvaras i ett förvaringsutrymme som verksamhetsutövaren har godkänt enligt 5 kap. 10 § PMFS 2022:1. Kraven gäller inte om handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.
- Arbetar man inte aktivt med en säkerhetsskyddsklassificerad uppgift ska den vara inlåst.
- Den som ansvarar för en säkerhetsskyddsklassificerad handling måste hela tiden ha uppsyn över den om den inte förvaras enligt de säkerhetsregler som finns.

Förvaringsutrymmen

Enligt 5 kap. 10 § PMFS 2022:1 ska verksamhetsutövaren besluta om vilka förvaringsutrymmen som är godkända för förvaring av säkerhetsskyddsklassificerade uppgifter samt kort, nycklar och anteckningar med uppgift om kod, som var för sig ger åtkomst till områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Ett förvaringsutrymme får godkännas endast om det är försett med eller omges av åtgärder för att upptäcka, försvåra och hantera obehörigt tillträde utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan.

Beslut att godkänna ett förvaringsutrymme avsett för förvaring av säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska fattas av verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

Vid problem

Om registratören får problem när det gäller distributionen av säkerhetsskyddsklassificerade uppgifter, det kan gälla handläggare eller chefer som inte följer de rutiner som finns, så ska detta anmälas direkt till säkerhetsskyddschefen.

2.5 Kvittering

Roller

Registrator:

Ansvarar för att kvitteringslista finns fäst ovanpå den säkerhetsskyddsklassificerade uppgiften (handlingen). Säkerställa att mottagande och ansvarig handläggare kvitterar handlingen.

Handläggare: Ansvar för att kvittera kvitteringslistan. Handläggaren ansvarar även från och med kvitteringen för handlingen och säkerställer att den förvaras rätt.

Instruktion

Säkerhetsskyddsklassificerade uppgifter, det vill säga hemliga handlingar, ska kvitteras av mottagande handläggare. Till det används en kvitteringslista som medföljer den säkerhetsskyddsklassificerade uppgiften. Kvitteringslistan ska häftas fast vid den säkerhetsskyddsklassificerade uppgiften.

Handläggaren som hämtar ut den säkerhetsskyddsklassificerade uppgiften kvitterar på kvitteringslistan genom att signera och skriva namnförtydligande samt det datum som handlingen hämtas ut.

Vilka som tagit del av uppgifter ur en säkerhetsskyddsklassificerad uppgift ska vara dokumenterade i kvitteringslistan. Andra handläggare som tar del av handlingen ska kvittera på kvitteringslistan och det är den ansvarige handläggaren som ansvarar för att andra handläggare är behöriga att ta del av säkerhetsskyddsklassificerade uppgifter. Innan man låter en annan person ta del av en säkerhetsskyddsklassificerad uppgift ska man alltså tillse att den personen är behörig att göra detta.

Tänk på att kvittering också kan ske genom muntlig överföring av uppgifter och visning av uppgifter i mötessammanhang. Vid dragningar av ärende där säkerhetsskyddsklassificerade uppgifter föredras muntligt eller via presentation ska alltså samtliga deltagande åhörare kvittera att de tagit del av uppgifter ur handlingen.

Om inte kvittering sker har verksamheten tappat kontrollen över handlingen och det ska anmälas till säkerhetsskyddschef.

2.6 Inventering

Roller

Registrator: Leder inventeringen av säkerhetsskyddsklassificerade uppgifter.

Ej registrator/säkerhetsklassad person dock inte säkerhetsskyddschef:
Övervakar inventering.

Handläggare: Uppvisar säkerhetsskyddsklassificerade uppgifter.

Instruktion

Årlig inventering av säkerhetsskyddsklassificerade uppgifter som inte förvaras i diarium eller arkiv.

Kontroll av:

- Rätt skydd av uppgift/handling
- Uppvisa samtliga säkerhetsskyddsklassificerade uppgifter
- Undersöka förekomst av svartkopia
- Inventera hårddiskar och USB-minnen Inventeringsmall Resultatet rapporteras till säkerhetsskyddschef som utreder eventuella röjda säkerhetsklassificerade uppgifter och vidtar åtgärder.

2.7 Återlämning

Roller

Registrator: Ansvarar för att uppdatera diariet över säkerhetsskyddsklassificerade uppgifter samt låsa in handlingen för förvaring.

Handläggare: Ansvarar för att omgående återlämna säkerhetsskyddsklassificerade uppgifter som inte behövs för handläggning.

Instruktion

När ett ärende är avslutat ska säkerhetsskyddsklassificerade uppgifter överlämnas till registrator. Registratören uppdaterar diariet och låser in den säkerhetsskyddsklassificerade uppgiften för förvaring. Kopior av säkerhetsskyddsklassificerade uppgifter som inte ska bevaras ska rensas. Vid återlämning stryks handlingen i diariet med ett streck så att texten under fortfarande går att läsa som tecken på att handlingen är återlämnad. Datumet då handlingen återlämnats ska även dokumenteras i diariet. Vid en ny utlåning skrivs en ny post i diariet med handlingens exakta handlings-id.

Datum:	Hemligt diarium:	Sid nr:
--------	------------------	---------

Datum:	Dnr nr:	H-löpnr:	Exemplar nr:
Avsändare/Mottagare:	Ansvarig handläggare:		
Ärendemening:	Förvaltning:		
	Datum åter:		

Datum:	Dnr nr:	H-löpnr:	Exemplar nr:
Avsändare/Mottagare:	Ansvarig handläggare:		
Ärendemening:	Förvaltning:		
	Datum åter:		

2.8 Arkivering och gallring (förstöring)

Roller

Registrator: Ansvarar för att säkerhetsskyddsklassificerade uppgifter förvaras på rätt sätt. Ordnar säkerhetsskyddsklassificerade uppgifter i en egen serie. Överlämnar bevarande handlingar till arkivet.

Arkivarie: Mottar arkivboxar på sedvanligt sätt och kvitterar dessa som vanligt. Arkivboxarna ska hållas åtskilda från det vanliga arkivet och skall läsas in i godkända skåp.

Instruktion

Arkivering

Säkerhetsskyddsklassificerade uppgifter ska hållas åtskilda från det vanliga arkivet. Handlingarna skall ordnas i en separat serie. Vanligtvis ”säkerhetsskyddsklassificerade uppgifter ordnade efter diarienummer”. Serien med säkerhetsskyddsklassificerade uppgifter ska förtecknas som en separat serie i arkivförteckningen. Nedan är ett exempel på hur det kan se ut i arkivförteckningen.

F Handlingar ordnade efter nämnd

– F1 Diarieförda Ärenden

– – F1a Diarieförda ärenden.

– – F1b Säkerhetsskyddsklassificerade uppgifter ordnade efter diarienummer.

Arkiveringen av säkerhetsskyddsklassificerade uppgifter ska ske på så sätt att de säkerhetsskyddsklassificerade uppgifterna har högre skydd än det vanliga arkivet. Vanligtvis placeras ett säkerhetsskåp i arkivet för förvaring av säkerhetsskyddsklassificerade uppgifter.

Gallring (förstöring)

Säkerhetskyddsklassificerade uppgifter får inte kastas i sekretesstunna eller pappersåtervinning. De ska alltid förstöras på plats under överseende av säkerhetskyddschefen. Samtlig destruktion av säkerhetskyddsklassificerade uppgifter eller medier ska dokumenteras i en destruktionsloggare.

(Bilagor: 1. Mall för hemligt diarium 2. Distributionslista 3. Mall – Kvitteringslista som ska medfölja hemlig handling när en handläggare övertar ansvaret för den. 4. Mall- Inventeringslista