Lidköpings kommun

RUTIN

Rutiner för säkerhetsskydd

Lidköpings kommuns samlade rutiner för säkerhetsskydd

Antagen av: Säkerhetsskyddschef

Datum: 2026-11-19

Dokumentinformation

Fastställt av:	Säkerhetsskyddschef
Diarienummer:	KS 2026/719
Fastställt, datum:	2026-11-19
Dokumentsansvarig:	Säkerhetssamordnare
Gäller för:	Lidköpings kommun
Gäller till, datum:	Tills vidare
Revideras datum:	Klicka eller tryck här för att ange text.

Innehållsförteckning

1. Inledning 5

1.1. Syfte 5

1.2. Målgrupp 5

1.3. Avgränsning 5

1.4. Koppling till andra styrdokument 5

1.5. Regelverk och grundläggande begrepp 6

1.6. Säkerhetskänslig verksamhet 6

1.7. Uppföljning och efterlevnad 7

1.8. Organisation och ansvar 9

2. Processer inom säkerhetsskydd 10

2.1. Säkerhetsskyddsanalys och säkerhetsskyddsplan 10

2.2. Säkerhetsskyddsavtal och säkerhetsskyddsöverenskommelse 11

2.3. Särskild säkerhetsskyddsbedömning (SSB) 12

2.4. Samråd och anmälan till tillsynsmyndighet 13

2.5. Upphandling – särskilda moment 14

2.6. Uppföljning och kontroll under avtalstiden 15

2.7. Avslut av säkerhetsskyddsavtal och leverantör/underleverantör 16

3. Rutiner för säkerhetsskydd 17

3.1. Informationssäkerhet 17

3.2. Hantering av säkerhetsskyddsklassificerade handlingar 21

3.3. Personalsäkerhet 25

3.4. Fysisk säkerhet 30

3.5. Informationssystem för hantering av säkerhetsskyddsklassificerad information 31

3.6. Säkerhetshotande händelser 35

4. Utbildning 39

5. Bilagor 40

Bilaga 1 – Samförvaringsbeslut 41

Bilaga 2 – Delgivning och kvittering 43

Bilaga 3 – Beslut om medförande 44

Bilaga 4 – Diarieföring av säkerhetsskyddsklassificerad handling 45

Bilaga 5 – Förstöringsliggare 48

Bilaga 6 – Checklista och mallar för säkerhetsprövning 49
Bilaga 7 – Förteckning över kort, taggar, koder och nycklar 50
Bilaga 8 – Sambruksavtal sekretessdator.....52
Bilaga 9 – Behörighet att hantera säkerhetsskyddsklassificerad information53
Bilaga 10 – Inventering av säkerhetsskyddsklassificerade handlingar.....54
Bilaga 11 – Internkontroll säkerhetsskydd.....56
6. Referenslista.....61

1. Inledning

1.1. Syfte

Syftet med detta dokument är att säkerställa att Lidköpings kommun bedriver ett systematiskt och ändamålsenligt säkerhetsskyddsarbete i enlighet med gällande lagstiftning samt att förebygga att säkerhetskänslig verksamhet utsätts för säkerhetshot. Dokumentet ska:

- säkerställa att kommunen uppfyller krav i lag, förordning och föreskrifter.
- tydliggöra ansvar, roller och arbetsprocesser.
- ge stöd i genomförandet av säkerhetsskyddsarbetet.
- bidra till ett enhetligt, systematiskt och förebyggande arbetssätt.

Rutinen ska utgöra ett stöd i det dagliga arbetet, integreras i kommunens styrning och följas upp samt revideras vid behov, exempelvis vid förändringar i skyddsvärden eller hotbild.

1.2. Målgrupp

Dokumentet riktar sig till samtliga medarbetare, chefer och uppdragstagare som arbetar i eller kommer i kontakt med säkerhetskänslig verksamhet inom Lidköpings kommun, samt i tillämpliga delar till externa aktörer som deltar i denna verksamhet.

1.3. Avgränsning

Rutinen omfattar all verksamhet inom kommunen som bedöms vara säkerhetskänslig enligt säkerhetsskyddslagstiftningen. Rutinen omfattar främst de skyddsvärden och den högsta konsekvensnivå som identifierats i kommunens säkerhetsskyddsanalys.

1.4. Koppling till andra styrdokument

Dokumentet kompletterar kommunens säkerhetsskyddsanalys, säkerhetsskyddsplan, befattningsanalys, riktlinje för säkerhetsskydd samt styrdokument inom signalskydd, informationssäkerhet, civil beredskap och intern kontroll.

1.5. Regelverk och grundläggande begrepp

Lidköpings kommun ska bedriva ett systematiskt och riskbaserat säkerhetsskyddsarbete i enlighet med:

- Offentlighets- och sekretesslag (2009:400)
- Säkerhetsskyddslagen (2018:585)
- Säkerhetsskyddsförordningen (2021:955)
- Säkerhetspolisens föreskrifter om säkerhetsskydd (konsoliderad PMFS 2022:1 med ändringar enligt PMFS 2026:8) samt tillhörande vägledningar

Säkerhetsskydd omfattar skydd av säkerhetskänslig verksamhet och säkerhetsskyddsklassificerade uppgifter. Säkerhetsskydd delas in i informationssäkerhet, fysisk säkerhet och personalsäkerhet.

Med **Sveriges säkerhet** avses Sveriges självständighet och suveränitet, okränkta landsgränser, det svenska självstyret, det demokratiska statsskicket och nationens grundläggande funktionalitet.

En **handling** är en framställning i skrift eller bild samt upptagningar som endast med tekniska hjälpmedel kan läsas eller avlyssnas.

1.6. Säkerhetskänslig verksamhet

Säkerhetskänslig verksamhet är verksamhet som till någon del är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Den verksamheten innehåller alltid ett eller flera skyddsvärden, som identifieras utifrån följande tre kategorier:

- säkerhetsskyddsklassificerade uppgifter
- anläggningar, objekt, system, egendom och andra tillgångar som är av betydelse för Sveriges säkerhet
- internationellt åtagande om säkerhetsskydd.

Verksamhetsutövare som bedriver säkerhetskänslig verksamhet ska identifiera de delar av verksamheten som är av betydelse för Sveriges säkerhet. Dessa delar ska skyddas mot spionerі, sabotage, terroristbrott och andra hot.

Det är kommunens ansvar att utreda behovet av säkerhetsskydd och säkerställa att identifierade skyddsvärden skyddas genom praktiska och organisatoriska åtgärder.

1.7. Uppföljning och efterlevnad

Enligt säkerhetsskyddslagen (2018:585) ska verksamhetsutövare som bedriver säkerhetskänslig verksamhet arbeta systematiskt med säkerhetsskydd. Säkerhetsskyddsåtgärderna ska anpassas utifrån verksamhetens art och omfattning, förekomsten av säkerhetsskyddsklassificerade uppgifter samt andra relevanta förutsättningar.

Ett systematiskt säkerhetsskyddsarbete innebär bland annat att säkerhetsskyddet regelbundet följs upp och kontrolleras, att säkerhetshotande händelser rapporteras och utreds samt att nödvändiga förbättringsåtgärder genomförs.

För att säkerställa att ett systematiskt säkerhetsskyddsarbete bedrivs i Lidköpings kommun används *Årshjul säkerhetsskyddsarbete Lidköpings kommun*. Årshjulet är uppdelat i fyra kvartal och innehåller de aktiviteter som ska genomföras under året. Uppgifter som inte slutförs inom aktuellt kvartal flyttas till nästa. Vid årets slut signeras årshjulet av säkerhetsskyddschefen och arkiveras för att säkerställa spårbarhet och dokumentation.

För att säkerställa att kommunens säkerhetsskydd är aktuellt, ändamålsenligt och effektivt genomförs följande uppföljnings- och kontrollaktiviteter:

- **Periodiska kontroller:** säkerhetsskyddschefen, eller annan utsedd kontrollansvarig, genomför regelbundna kontroller av säkerhetsskyddet. Kontrollerna omfattar bland annat fysiska och tekniska skyddsåtgärder såsom lås- och passersystem (*Bilaga 7 – Förteckning över kort, taggar, koder och nycklar)*, behörighetsadministration samt hantering av säkerhetskänslig information (*Bilaga 1 – Samförvaringsbeslut, Bilaga 8 – Sambruksavtal sekretessdator, Bilaga 9 – Behörighet att hantera säkerhetsskyddsklassificerad information*).
- **Översyn av säkerhetsskyddet:** säkerhetsskyddsanalysen och tillhörande åtgärdsplaner ska ses över minst vartannat år eller tidigare om verksamheten, organisationen, informationshanteringen eller hotbilden förändras på ett sätt som kan påverka säkerhetsskyddet.

- **Avvikelserapportering och incidenthantering:** alla brister, avvikelser och säkerhetshotande händelser ska rapporteras enligt kommunens rutiner för incidenthantering. Varje rapporterad händelse ska utredas för att identifiera orsaker, bedöma konsekvenser och vidta åtgärder som minskar risken för att händelsen upprepas.
- **Internkontroll och självutvärdering:** verksamhetsansvariga ansvarar för att löpande följa upp att fastställda rutiner och säkerhetsskyddsåtgärder efterlevs i den dagliga verksamheten (*Bilaga 11 – Internkontroll säkerhetsskydd*).
- **Extern tillsyn:** kommunens säkerhetsskyddsarbete omfattas även av tillsyn från ansvarig tillsynsmyndighet. Tillsynen syftar till att säkerställa att kommunen uppfyller kraven i säkerhetsskyddslagstiftningen och att beslutade säkerhetsskyddsåtgärder tillämpas i praktiken. Kommunen ska lämna den information och dokumentation som behövs för tillsynen.
- **Ansvar för efterlevnad:** ett väl fungerande säkerhetsskydd bygger på att samtliga medarbetare, uppdragstagare och konsulter som deltar i säkerhetskänslig verksamhet känner till och följer gällande regler, rutiner och säkerhetsföreskrifter. Var och en ansvarar för att omedelbart rapportera upptäckta brister eller avvikelser som kan påverka säkerhetsskyddet.

1.7.1. Konsekvenser vid bristande efterlevnad

- **Myndighetsåtgärder:** om tillsynsmyndigheten konstaterar brister i kommunens säkerhetsskydd kan kommunen föreläggas att vidta rättelse. Allvarliga eller kvarstående brister kan medföra vite eller sanktionsavgifter enligt gällande lagstiftning.
- **Korrigerande åtgärder:** vid konstaterade brister ska i första hand korrigerande åtgärder vidtas. Dessa kan exempelvis bestå av kompletterande utbildning, information, handledning eller förändrade arbetssätt för att säkerställa efterlevnad.
- **Personalärenden och rättsliga åtgärder:** allvarliga eller upprepade överträdelser av säkerhetsskyddsregler, eller medvetet åsidosättande av säkerhetsföreskrifter, hanteras som personalärenden. Beroende på överträdelsens art och allvarlighetsgrad kan arbetsrättsliga åtgärder bli aktuella i enlighet med gällande lagstiftning och kollektivavtal. Om det finns misstanke om brott mot säkerhetsskyddslagen eller annan lagstiftning ska händelsen anmälas till

Polismyndigheten.

1.8. Organisation och ansvar

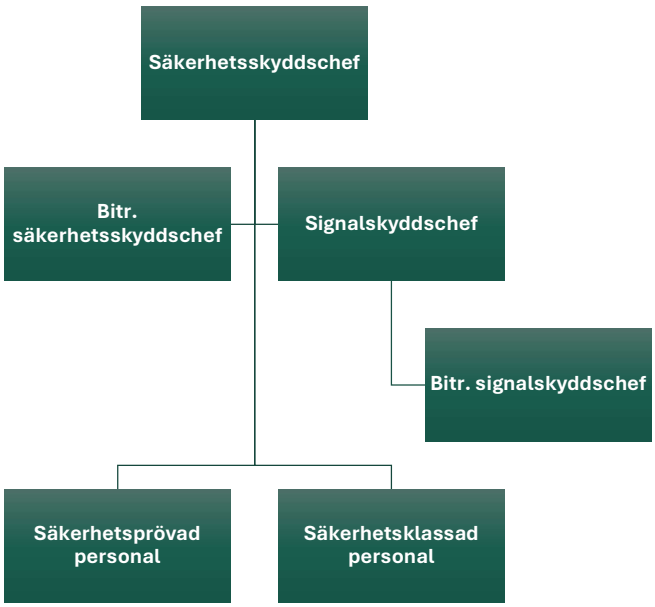
1.8.1. Ledning och övergripande ansvar

Kommundirektören har det yttersta ansvaret för kommunens säkerhetskyddsarbete. Säkerhetsskyddschefen leder arbetet och är direkt underställd kommundirektören.

Alla medarbetare i Lidköpings kommun som deltar i säkerhetskänslig verksamhet eller hanterar säkerhetsskyddsklassificerad information har skyldighet att följa detta dokument samt gällande lagar och föreskrifter kopplat till säkerhetsskydd.

1.8.2. Säkerhetsskyddsorganisationen

Säkerhetsskyddsorganisationen består av säkerhetsskyddschef, biträdande säkerhetsskyddschef, signalskyddschef, biträdande signalskyddschef, säkerhetsprövad personal (inklusive personal inom ramen för säkerhetsskyddsöverenskommelser och avtal).



Säkerhetsskyddsorganisationen i Lidköpings kommun

2. Processer inom säkerhetsskydd

2.1. Säkerhetsskyddsanalys och säkerhetsskyddsplan

Säkerhetsskyddsanalysen utgör grunden för hela säkerhetsskyddsarbetet och fastställer vilka skyddsvärden, hotbilder och säkerhetsskyddsåtgärder som ska tillämpas. Analysen ska ge svar på vad som ska skyddas, mot vad och på vilket sätt. Säkerhetsskyddsanalysen ska följa 2 kap. 1–9 §§ konsoliderad PMFS 2022:1 med ändringar enligt PMFS 2026:8 och ska innehålla:

- en övergripande verksamhetsbeskrivning,
- vilka delar som är av betydelse för Sveriges säkerhet utifrån
  - Sveriges yttre säkerhet
  - Sveriges inre säkerhet
  - nationell samhällsviktig verksamhet
  - verksamhet av betydelse för Sveriges ekonomi
  - verksamhet som kan generera skada på annan säkerhetskänslig verksamhet
- identifierade skyddsvärden
- bedömning ur perspektiven konfidentialitet, riktighet, tillgänglighet
- konsekvensnivå (A-D) för respektive skyddsvärde
- säkerhetshot
- en beskrivning av dimensionerad antagonistiska förmågor
- sårbarheter
- nödvändiga skyddsåtgärder

Säkerhetsskyddsanalysen fastställs av kommundirektören och ska uppdateras vid behov, dock minst vartannat år.

Till säkerhetsskyddsanalysen upprättas en tillhörande befattningsanalys. Befattningsanalysen redovisar vilka befattningar i verksamheten som har tillgång till säkerhetskänslig verksamhet och som därmed kräver placering i säkerhetsklass eller säkerhetsprövning utan inplacering i säkerhetsklass.

Som ett resultat av säkerhetsskyddsanalysen upprättas en säkerhetsskyddsplan och åtgärdsplan som redovisar vilka avvikelser som finns, vilka åtgärder som behövs, vilken funktion som ansvarar för genomförandet och när det ska ske.

Säkerhetsskyddsplanen och åtgärdsplanen fastställs av säkerhetsskyddschefen, uppdateras löpande och följs upp årligen utifrån identifierade avvikelser, förändringar i verksamheten, hotbilden och säkerhetsskyddsåtgärdernas effekt.

2.2. Säkerhetsskyddsavtal och säkerhetsskyddsöverenskommelse

Lidköpings kommun ska ingå säkerhetsskyddsavtal när en extern part, till exempel en leverantör, kan få tillgång till säkerhetsskyddsklassificerade uppgifter i klassen konfidentiell eller högre. Detsamma gäller annan säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet. Syftet är att skyddet ska vara lika starkt hos den externa parten som hos oss.

Avtalet ska ingås innan den externa parten får tillgång. Det kan därför behövas redan under upphandlingen, till exempel om leverantörer måste ta del av uppgifterna för att lämna anbud. Kravet gäller även underleverantörer i alla led.

Avtalsnivåer:

- nivå 1 – när den externa parten kan få tillgång till, eller möjlighet att förvara, säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller tillgång till säkerhetskänslig verksamhet där åtkomst kan medföra en inte obetydlig skada för Sveriges säkerhet, utanför verksamhetsutövarens områden, lokaler eller utrymmen.
- nivå 2 – motsvarande tillgång, men inom verksamhetsutövarens områden, lokaler eller utrymmen.
- nivå 3 – när den externa parten kan, men har inget konstaterat behov av att, få tillgång till konfidentiell eller högre information eller motsvarande verksamhet inom verksamhetsutövarens områden.

Vid avrop från ramavtal ska varje avrop bedömas för sig. Om uppdraget kräver en annan nivå än under anbudsskedet avslutas det tidigare avtalet och ersätts av ett nytt avtal i rätt nivå. Vid samverkan mellan flera aktörer kan avtalet ingås mellan fler än två parter, på den högsta nivå som hade gällt vid bilaterala avtal.

Vad avtalet ska innehålla är reglerat i säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2021:955) och Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1). Säkerhetsskyddet får inte göras mindre omfattande i avtalet än vad lagstiftningen kräver. Avtalet ska bland annat reglera:

- krav på leverantörens säkerhetsskydd
- hur Lidköpings kommun kontrollerar leverantören och underleverantörer
- säkerhetsskyddsutbildning av leverantörens personal och ansvaret för den
- tystnadsplikt, även efter att uppdrages
- återlämning eller förstöring av säkerhetsskyddsklassificerade uppgifter när avtalet upphör.

Vid nivå 1 ska leverantören dessutom upprätta en säkerhetsskyddsinstruktion som dokumenterar hur kraven uppfylls. Instruktionen ska granskas och godkännas av verksamhetsutövaren.

Om den externa parten endast kan få tillgång till uppgifter i klassen begränsat hemlig, eller motsvarande verksamhet, ska skyddet i stället regleras genom en säkerhetsskyddsöverenskommelse. Utformningen avgörs av verksamhetsutövaren, men inför överenskommelsen måste följande genomföras:

- identifiering av vilka uppgifter eller vilken verksamhet som exponeras
- bedömning hot och sårbarheter
- beslut om vilka skyddsåtgärder som behövs
- prövning om förfarandet är lämpligt ur säkerhetsskyddssynpunkt.

Säkerhetsskyddschefen ansvarar för upprättande, uppföljning och avslut av säkerhetsskyddsavtal och säkerhetsskyddsöverenskommelse.

2.3. Särskild säkerhetsskyddsbedömning (SSB)

En särskild säkerhetsskyddsbedömning (SSB) är en fördjupad analys som ska göras vid förfaranden och förändringar som kan påverka Sveriges säkerhet. Exempelvis vid:

- upphandling/avtal
- samverkan/samarbete
- införande/driftsättning av informationssystem (inklusive dokumentation av tester)
- väsentliga systemförändringar
- överlåtelse av verksamhet/egendom.

SSB ska göras innan förfarandet inleds och innan säkerhetsskyddsavtal ingås. Den ska beskriva:

- berörda skyddsvärden och hur de påverkas (konsekvensanalys)
- hot, till exempel spionage, sabotage, terrorism
- sårbarheter och hur de påverkas
- nödvändiga skyddsåtgärder.

Bedömningen ska uppdateras med avvikelser och kompensatoriska åtgärder. Vid upphandling ska den resultera i en plan för hur säkerhetsskyddet regleras i uppdraget, och vid behov revideras kommunens säkerhetsskyddsplanering. Analys och plan ska dokumenteras.

I samband med SSB ska det prövas om förfarandet är lämpligt med den tänkta motparten. Det kan vara olämpligt om:

- personalen hos motparten inte kan säkerhetsprövas
- uppgifterna är så känsliga att aldrig bör förvaras utanför våra lokaler
- motparten inte uppfyller tillförlitlighetskraven, till exempel på grund av ägarförhållanden.

Bedömning och beslut ska dokumenteras.

2.4. Samråd och anmälan till tillsynsmyndighet

Samråd med tillsynsmyndigheten ska ske innan förfarandet inleds om motparten kan få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller högre, eller motsvarande säkerhetskänslig verksamhet, och i övriga fall där regelverket kräver det. Kontrollera alltid aktuella krav hos vår tillsynsmyndighet.

Underlag till samrådet är bland annat beskrivning av verksamheten, identifierade skyddsvärden och konsekvensanalys, lämplighetsprövning, hot- och sårbarhetsbedömning, plan för säkerhetsskyddet samt utkast till säkerhetsskyddsavtal och säkerhetsskyddskrav i upphandlingsdokumenten.

Leverantören och underleverantörer får inte tillgång till verksamheten förrän tillsynsmyndigheten har avslutat samrådet utan krav på åtgärder.

Avsikt att ingå säkerhetsskyddsavtal, ingångna avtal och upphörda avtal ska anmälas på tillsynsmyndighetens blanketter. Säkerhetsskyddschefen ansvarar för att samråd och anmälningar görs och dokumenteras.

2.5. Upphandling – särskilda moment

- Säkerhetsskyddsavtalet ska vara ett separat avtal i upphandlingsunderlaget. Säkerhetsskyddskrav ska anges och att avtalets giltighet förutsätter att leverantören bedömts tillräckligt tillförlitlig och att samrådet avslutats utan förbud.
- Säkerhetsskyddsavtal ingås med de som får tillgång till uppgifterna. Om endast vinnande leverantör behöver tillgång, ingås avtal med den. Om alla anbudsgivare behöver tillgång för att kunna lämna anbud, ingås avtal med alla. Då kan ett tvåstegsförfarande vara lämpligt, så att känslig information lämnas först efter kvalificering.
- Separata säkerhetsskyddsavtal ska ingås med underleverantörer, även i senare led, som kan få tillgång till uppgifter eller verksamhet på avtalspliktig nivå.
- Säkerhetsprövning med registerkontroll ska göras av leverantörens ledning (eller berörda delar av den) och övrig personal som ska delta i den säkerhetskänsliga verksamheten. Man kan avtala att leverantören gör grundutredningen, men godkännande efter registerkontroll sker hos Lidköpings kommun.
- Säkerhetsprövning med registerkontroll får inte göras enbart med stöd av en säkerhetsskyddsöverenskommelse, säkerhetsprövning med grundutredning är dock möjlig.
- Leverantörens personal ska ha relevant kunskap om säkerhetsskydd och känna till de skyddsvärden som berör arbetet.
- Berörda hos leverantören ska underteckna erinran om tystnadsplikt.
- Före säkerhetsskyddsavtal i nivå 1 ska leverantörens säkerhetsskydd kontrolleras på plats och kontrollen dokumenteras.
- Säkerhetsskyddsavtal med leverantörer som inte tilldelats ska avslutas och tystnadsplikt erinras.

2.6. Uppföljning och kontroll under avtalstiden

- Leverantören och eventuella underleverantörer ska kontrolleras under hela avtalstiden. Säkerhetsskyddschefen ansvarar för att uppföljningen planeras, genomförs och dokumenteras.
- En kontrollplan med frekvens, omfattning, ansvarig och metod ska upprättas för varje avtal. Kontrollerna ska vara regelbundna och anpassade efter avtalets nivå och risk.
- Vid säkerhetsskyddsavtal i nivå 1 ska säkerhetsskydd regelbundet kontrolleras på plats. Kontrollera bland annat att:
  - säkerhetsskyddsinstruktion följs och är aktuell
  - säkerhetsprövning och registerkontroll är genomförda och aktuella för all berörd personal
  - personalförteckningen är aktuell och personalförändringar är rapporterade
  - utbildning och erinran om tystnadsplikt är genomförda
  - hantering, förvaring och spridning av klassificerade uppgifter och informationssystem uppfyller kraven
  - underleverantörer omfattas av avtal och uppfyller samma krav.
- Vid samverkan kan avtalet reglera att varje part följer upp sin egen verksamhet. Lidköpings kommun ska då kontrollera att motparten har gjort det.
- Brister ska dokumenteras och åtgärdas av leverantören inom angiven tid. Kompensatoriska åtgärder ska bedömas och SSB ska uppdateras. Säkerhetshotande händelser hanteras och anmäls enligt rutinen för incidenthantering och gällande föreskrifter.
- Avtalet ska löpande bedömas för revidering, till exempel vid ändrat uppdrag, ny hotbild, ändrad avtalsnivå, ändrade ägarförhållanden eller ändrade skyddsvärden. Vid väsentliga förändringar ska SSB uppdateras och, vid behov, även samråd och anmälan.
- Kontrollresultat, avvikelser, åtgärder och beslut ska dokumenteras och sparas i avtalsakten.

2.7. Avslut av säkerhetsskyddsavtal och leverantör/underleverantör

- Hur avslut av säkerhetsskyddsavtal ska genomföras ska planers redan när avtalet ingås. Säkerhetsskyddschefen ansvarar för att avslutet genomförs.
- Leverantören och underleverantörer ska återlämna eller förstöra alla säkerhetsskyddsklassificerade handlingar enligt Lidköpings kommuns anvisningar, detta ska bekräftas skriftligt och dokumenteras.
- Behörigheter, passerkort, nycklar, systemåtkomst och utlånad utrustning ska avslutas och återlämnas.
- Uppgifter i leverantörens och underleverantörens system ska raderas eller returneras, hur det har gjorts ska dokumenteras.
- Berörd personal ska påminnas om att tystnadsplikten gäller även efter att uppdragets slut. Erinran kan undertecknas på nytt.
- När säkerhetsskyddsavtalet upphört ska avtalet och tillhörande registerkontroller skyndsamt avanmälas till tillsynsmyndigheten. Registerkontroll avanmäls även för personal som lämnar uppdraget under avtalstiden.
- En slutkontroll ska göras där avvikelser och lärdomar dokumenteras, och SSB, säkerhetsskyddsplan och leverantörsregister uppdateras.
- Om uppdraget går över till annan leverantör eller ska tas över i egen regi ska säkerhetsskyddet vara oavbrutet. Nytt avtal eller ny överenskommelse ska vara på plats innan den nya parten får tillgång.
- Avtal, SSB, kontrollrapporter, avanmälningar och beslut ska arkiveras enligt gällande arkivregler och sekretess.

3. Rutiner för säkerhetsskydd

3.1. Informationssäkerhet

Uppgifter (information) är av avgörande betydelse i alla typer av verksamheter. För säkerhetskänslig verksamhet är tillgång till tillförlitliga uppgifter avgörande för att verksamheten ska fungera. Det är viktigt att identifiera vilka uppgifter den säkerhetskänsliga verksamheten på olika sätt är beroende av. För att förhindra skada på såväl verksamheten som Sveriges säkerhet behöver verksamheten även identifiera vilka uppgifter som är säkerhetsskyddsklassificerade med anledning av konsekvenser förknippade med uppgifternas röjande.

Informationssäkerhet inom säkerhetsskydd syftar till:

- att förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och
- att förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.

3.1.1. Klassificering och säkerhetsskyddsklassificering

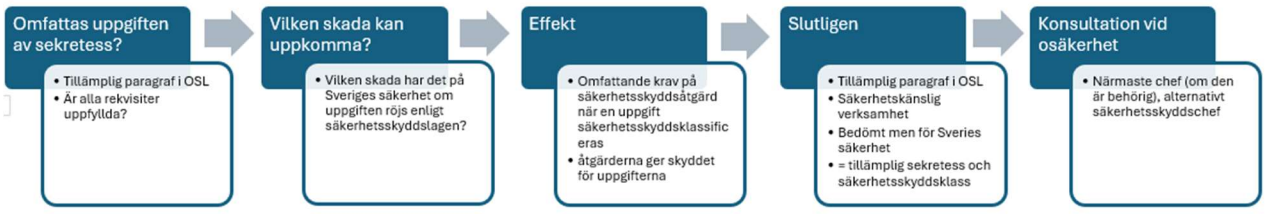
Informationssäkerhet syftar till att förhindra att säkerhetsskyddsklassificerade uppgifter röjs, förändras, förstörs eller blir otillgängliga. Skyddet vilar på tre pelare:

- konfidentialitet: förhindra att obehöriga får tillgång till information.
- riktighet: säkerställa att informationen är korrekt och inte manipulerad.
- tillgänglighet: säkerställa att informationen finns tillgänglig när den behövs.

Säkerhetsskyddsklassificerade uppgifter är uppgifter som rör säkerhetskänslig verksamhet och som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), eller som skulle ha omfattats av sekretess om lagen hade varit tillämplig. Uppgifterna ska, utifrån den skada ett röjande kan medföra, placeras i någon av säkerhetsskyddsklasserna kvalificerat hemlig, hemlig, konfidentiell eller begränsat hemlig.

Säkerhets-skyddsklass	Den skada som ett röjande av uppgifterna kan medföra	Typiska konsekvenser
Kvalificerat hemlig	Synnerligen allvarlig skada	Mycket omfattande och långvariga konsekvenser för nationell säkerhet. Direkt hot mot nationell förmåga. Mycket svårt att återställa.
Hemlig	Allvarlig skada	Omfattande konsekvenser för nationell säkerhet. Betydande påverkan på viktiga funktioner. Svårt att återställa.
Konfidentiell	Inte obetydlig skada	Märkbar påverkan på nationell förmåga. Kan underlätta för en antagonist eller orsaka större störningar i begränsad omfattning.
Begränsat hemlig	Ringa skada	Begränsad påverkan på nationell förmåga. Kan orsaka mindre störningar eller ge viss fördel för en antagonist.

Om en uppgift omfattas av sekretess prövas den i regel först i samband med en begäran om utlämnande av allmän handling från kommunen, eller när kommunen har behov av att dela med sig av uppgifter till exempelvis annan aktör. Här finns det tydliga skillnader mellan offentlighets- och sekretesslagen (2009:400) och säkerhetsskyddslagstiftningen. Alla inom kommunen som bedriver säkerhetskänslig verksamhet ska göra denna bedömning redan när uppgiften skapas eller på annat sätt först hanteras då syftet med säkerhetsskyddsklassificeringen är att kunna vidta rätt säkerhetskyddsåtgärder från början. Om uppgiften i ett senare skede avses lämnas ut eller inte, eller om handlingen som innehåller uppgiften anses upprättad eller inte, saknar betydelse. Kravet gäller alltså även minnesanteckningar, arbetsmaterial och liknande handlingar.



En säkerhetsskyddsklassificerad handling är en handling som innehåller säkerhetsskyddsklassificerade uppgifter.

Exempel på säkerhetsskyddsklassificerade uppgifter:

- uppgifter om för Sverige kritisk infrastruktur (till exempel vatten, el, IT-system)
- säkerhetsskyddsanalys
- uppgifter om skyddsvärda anläggningar
- kryptografiska funktioner och signalskydd
- uppgifter om personal i säkerhetsklassade befattningar.

3.1.2. Märkning av handlingar

En säkerhetsskyddsklassificerad handling ska förses med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har, i syfte att klargöra vilka hanteringsregler som gäller för handlingen. Kravet på anteckning gäller för fysiska och elektroniska handlingar som innehåller säkerhetsskyddsklassificerade uppgifter, likaså arbetshandlingar. Anteckningen ska även innehålla hänvisning till tillämplig sekretessbestämmelse i offentlighets- och sekretesslagen (2009:400), datum då anteckningen gjordes samt vilken verksamhetsutövare som har gjort anteckningen. För fysiska handlingar med säkerhetsskyddsklass konfidentiell eller högre ska även handlingens beteckning, antal sidor samt uppgift om bilagor och exemplarnummer anges. Fysiska stämplar för märkning av handling finns hos säkerhetsenheten.







BEGRÄNSAT HEMLIG

SÄKERHETSSKYDDSKLASSIFICERAD

Sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400)

Datum_____

..... kommun

KONFIDENTIELL

SÄKERHETSSKYDDSKLASSIFICERAD

Sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400)

Datum_____

..... kommun

HEMLIG

SÄKERHETSSKYDDSKLASSIFICERAD

Sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400)

Datum_____

.....kommun

BEGRÄNSAT HEMLIG
SÄKERHETSSKYDDSKLASSIFICERAD
Se sida 1.

KONFIDENTIELL
SÄKERHETSSKYDDSKLASSIFICERAD
Se sida 1.

HEMLIG
SÄKERHETSSKYDDSKLASSIFICERAD
Se sida 1.

KVALIFICERAT HEMLIG

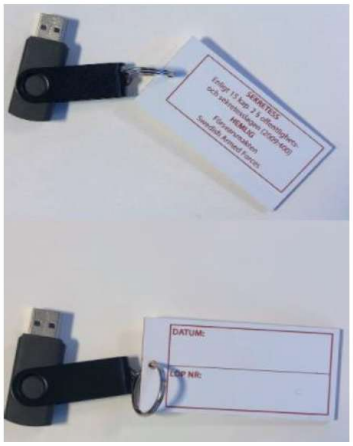
SÄKERHETSSKYDDSKLASSIFICERAD

Sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400)

Datum_____

.....kommun

KVALIFICERAT HEMLIG
SÄKERHETSSKYDDSKLASSIFICERAD
Se sida 1.

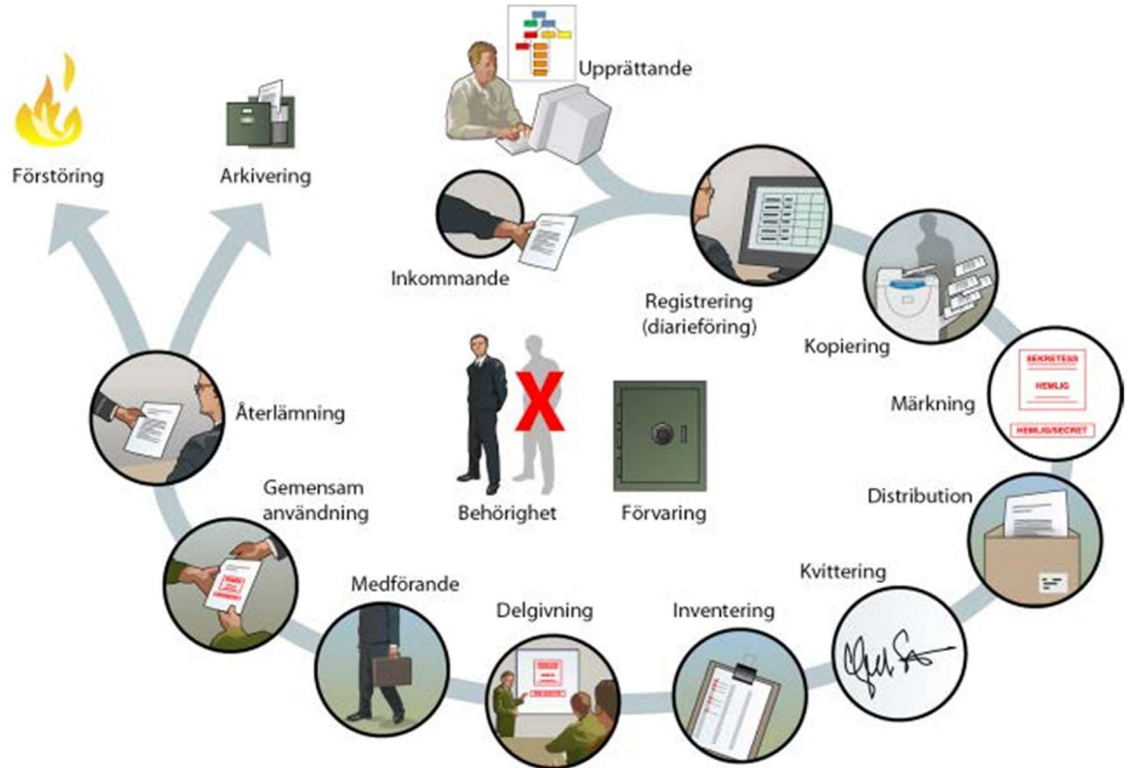




Exempel på märkning av USB-minne och CD-skiva. Bild lånad från mcf.se respektive "Handbok informationssäkerhet", Försvarsmakten.

3.2. Hantering av säkerhetsskyddsklassificerade handlingar

3.2.1. Livscykel för handlingar



Livscykel för handlingar. Bild lånad från ”Handbok, dokument- och ärendehantering”, 2026, Försvarsmakten.

Inkommen handling

Den som hanterar den säkerhetskyddsklassificerade handlingen ansvarar för att den hanteras korrekt från mottagandet från Kontaktcenter, postutlämningsställe eller via krypterad fil i epostsystemet under handlingens livscykel. Post som innehåller säkerhetsskyddsklassificerad information hanteras enligt rutin *Hantering av post med särskilda skyddskrav*.

Upprättande av handling

Säkerhetsskyddsklassificerade handlingar får inte upprättas i kommunens ordinarie verksamhetssystem. Innan färdigställande ska handlingen klassificeras och därefter förvaras i ett, för den aktuella säkerhetsskyddsklassen, godkänt informationssystem. För förvaring av fysiska handlingar, se kapitel 3.2.2 Förvaring.

Diarieföring

Säkerhetsskyddsklassificerade handlingar ska diarieföras i kommunens ordinarie diarieföringssystem Evolution, men tillvägagångssättet skiljer sig mot diarieföring av

öppna handlingar (*Bilaga 4 – Diarieföring av säkerhetsskyddsklassificerad handling*). Handlingarna uppförs även i en samlad registerförteckning i det hemliga diariet (H-diariet) i sekretessdatorn.

Kopiering och utskrift

Kopiering och utskrift sker **endast** på godkända kopiatorer/skrivare på säkerhetsenheten. Se anvisning vid kopiator/skrivare för handhavande.

Distribution, kvittering och medförande

Distribution kan ske på två sätt:

- digitalt – via kryptografiska funktioner. Se *Signalskyddsinstruktion Lidköpings kommun*.
- post – som rekommenderat brev i säkerhetspåse. Se rutin *Hantering av post med särskilda skyddskrav* som finns publicerad på Lidköpings kommuns intranät.

För handlingar i säkerhetsskyddsklass konfidentiell eller högre ska en delgivningslista användas för kvittering av mottagande (*Bilaga 2 – Delgivning och kvittering*).

En säkerhetsskyddsklassificerad handling som medförs utanför verksamhetsutövarens lokaler ska vara under kontroll eller förvaras i ett förvaringsutrymme som verksamhetsutövaren har godkänt. En säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen konfidentiell eller högre får medföras från verksamhetsutövarens lokaler efter beslut från säkerhetsskyddschef, ett sådant beslut ska dokumenteras (*Bilaga 3 – Beslut om medförande*).

Inventering

Handlingar och lagringsmedier med säkerhetsskyddsklass konfidentiellt eller högre ska inventeras minst en gång per år, se *Årshjul säkerhetsskyddsarbete Lidköpings kommun* för när på året inventeringen ska genomföras. Inventering av säkerhetsskyddsklassificerade handlingar får endast genomföras av behöriga medarbetare. Säkerhetsskyddschefen ansvarar för att inventering sker och att det dokumenteras (*Bilaga 10 – Inventering av säkerhetsskyddsklassificerade handlingar*).

Arkivering och förstöring

Arkivering sker på säkerhetsenheten. Förstöring sker med godkänd dokumentförstörare placerad på säkerhetsenheten. Lagringsmedier som ska förstöras lämnas till säkerhetsskyddschefen som tillser att förstöring sker på godkänt sätt.

Vid förstöring av handlingar eller lagringsmedier med säkerhetsskyddsklass konfidentiell eller högre ska förstöringen dokumenteras för spårbarhet (*Bilaga 5 – Förstöringsliggare*).

3.2.2. Förvaring

Godkända förvaringsutrymmen krävs för säkerhetsskyddsklassificerade handlingar (om dessa inte skyddas av godkända kryptografiska funktioner) samt anteckningar med uppgift om lösenord och koder som ger tillgång till informationssystem som är av betydelse för säkerhetskänslig verksamhet.

Förvaringsutrymmen får endast godkännas om de är försedda med, eller omges av, åtgärder för att upptäcka, försvåra och hantera obehörigt tillträde. Åtgärderna dimensioneras utifrån identifierade säkerhetshot och dimensionerande antagonistiska förmågor, DAF. DAF tillhandahålls av Säkerhetspolisen. Åtgärderna innefattar bland annat:

- behörighetsstyrt tillträde.
- larm och kontroll av loggar.
- fastställda rutiner för byte av lösenord och koder till både utrymmen och system.

Kravet på skyddsnivå för förvaringsutrymmet styrs av:

- den högsta säkerhetsskyddsklassen på informationen som förvaras.
- om informationen är **ackumulerad** (ökad volym av samma typ av uppgifter) eller **aggregerad** (olika typer av uppgifter som tillsammans skapar ett nytt, högre skyddsvärde).

Om ett förvaringsutrymme används av flera personer ska säkerhetsskyddschefen fastställa ett samförvaringsbeslut (*Bilaga 1 – Samförvaringsbeslut)*. Beslutet ska tydligt ange vilka personer som har tillgång till utrymmet, hållas uppdaterat och vara

fäst på insidan av utrymmet (till exempel på insidan av dörren till säkerhetsskåpet). Om personer med tillträde till utrymmet inte är behöriga att se alla handlingar som förvaras där, ska utrymmet vara utrustat med låsbara innerfack. Varje person tilldelas då ett personellt innerfack, om fler personer delar på ett innerfack ska ett samförvaringsbeslut vara anslaget på insidan.

3.2.3. Begäran om utlämnande

Vid begäran om utlämnande av en säkerhetsskyddsklassificerad handling ska en förnyad sekretessprövning av handlingen alltid genomföras. Prövningen ska avse huruvida handlingen omfattas av sekretess helt, delvis eller inte alls i enlighet med offentlighets- och sekretesslagen (2009:400). För arbetsgång vid utlämnande av handling, se *Utlämnande av allmän handling och sekretessprövning – en handbok* som finns publicerad på Lidköpings kommuns intranät.

3.2.4. Ändring av säkerhetsskyddsklassificering av handling

Säkerhetsskyddsklassificering av handlingar ska spegla uppgiftens faktiska skyddsvärde. Om förutsättningarna förändras ska en ny bedömning göras av om klassificeringen ska höjas, sänkas eller upphävas i enlighet med säkerhetsskyddslagstiftningen.

Vid Lidköpings kommun ska följande tillämpas:

- ansvarig handläggare ska initiera en ny säkerhetsskyddsbedömning när det finns indikationer på att en handlings skyddsvärde har förändrats. Bedömningen ska utgå från vilka konsekvenser ett röjande av uppgiften kan medföra för Sveriges säkerhet, med beaktande av aktuell verksamhet, hotbild och uppgiftens betydelse.
- beslut om ändring av säkerhetsskyddsklassificering ska fattas av säkerhetsskyddschef.
- vid höjning av säkerhetsskyddsklassificering ska handlingens märkning, förvaringskrav, åtkomstbegränsningar och hanteringsrutiner omedelbart anpassas till den nya skyddsnivån.

- vid sänkning eller upphävande av säkerhetsskyddsklassificering ska särskild restriktivitet iakttas. En sådan ändring får endast ske efter noggrann prövning och dokumenterad motivering.
- samtliga beslut om ändring av säkerhetsskyddsklassificering ska dokumenteras. Dokumentationen ska innehålla beslutsfattare, datum, motivering samt hänvisning till genomförd bedömning.
- handlingens märkning ska uppdateras i enlighet med beslutad klassificering. Tidigare versioner ska hanteras så att obehörig åtkomst inte kan ske.
- åtkomsträttigheter ska ses över och vid behov justeras så att endast behöriga personer ges tillgång till handlingen.
- tillse att säkerhetsskyddsklassificering på handlingen ändras även i diarieföringssystemet.



Exempel på sänkning av säkerhetsskyddsklassificering.

3.3. Personalsäkerhet

3.3.1. Syfte och omfattning

Personalsäkerhet är en grundsten i verksamhetens totala säkerhetsskydd. Syftet är att förebygga att personer som inte är pålitliga ur ett säkerhetsperspektiv får tillgång till säkerhetsskyddsklassificerade uppgifter eller deltar i säkerhetskänslig verksamhet. Genom ett systematiskt personalsäkerhetsarbete säkerställs att samtliga medverkande besitter den kompetens och medvetenhet som krävs för att motverka säkerhetsrisker.

Säkerhetsskyddslagens krav på säkerhetsprövning omfattar inte enbart anställda, utan även alla andra som på annat sätt deltar i den säkerhetskänsliga verksamheten, exempelvis uppdragstagare eller personer i plikttjänstgöring enligt lagen (1994:1809)

om totalförsvarsplikt.

3.3.2. Grundläggande principer för bedömning

Säkerhetsprövningen syftar till att fastställa om personen kan antas vara lojal mot de intressen som skyddas av säkerhetsskyddslagen, om det finns några sårbarheter som kan används emot personen samt om personen i övrigt kan antas vara pålitlig från säkerhetssynpunkt. Bedömningen vilar på:

- pålitlighetsbedömningen: en analys av om det finns risk för att personen kan göra sig skyldig till exempelvis spionerі, om personen är sårbar för otillbörlig påverkan (till exempel utpressning) eller kan komma att genom oaktsamhet röja sekretessbelagda uppgifter.
- lojalitetsprövningen: en analys av om det finns en risk att personen begår brottsliga handlingar mot Sveriges säkerhet, exempelvis på grund av förbindelser till främmande makt eller terroristorganisationer.

3.3.3. Placering i säkerhetsklass

För varje funktion som ska få tillgång till säkerhetsskyddsklassificerad information eller verksamhet ska det framgå:

- en unik beteckning för funktionen
- vilka arbetsuppgifter som innefattas
- omfattning av tillgång till säkerhetsskyddsklassificerade uppgifter
- vilken säkerhetsklass som befattningen ska placeras i (eller säkerhetsprövning utan klass)
- vilken konsekvensnivå personen kan orsaka

Detta sammanställs i en befattningsanalys som fastställs av säkerhetsskyddschefen.

Kriterier för placering i säkerhetsklass:

- placeringen baseras på den typ av uppgifter personen får tillgång till samt den potentiella skadan för Sveriges säkerhet som ett läckage eller otillbörligt utnyttjande skulle orsaka.

- placering i säkerhetsklass får endast ske om behovet av säkerhetsskydd inte kan tillgodoses på något annat sätt.
- för anställningar i säkerhetsklass 1 och 2 krävs som huvudregel svenskt medborgarskap.

Beslut om placering i säkerhetsklass fattas av säkerhetsskyddschef eller biträdande säkerhetsskyddschef. Kontaktuppgifter till dessa redovisas och uppdateras löpande hos Säkerhetspolisen.

Verksamhetsutövaren ska föra en förteckning över pågående registerkontroller, denna ska innefatta:

- säkerhetspolisens ID
- namn/personnummer
- säkerhetsklass
- kontrollorsak
- uppgifter om make/maka/sambo för klass 1 och 2
- uppgifter om säkerhetsskyddsavtal om relevant
- vem som ha ansökt om registerkontroll.

3.3.4. Organisation och ansvar

Verksamhetsutövaren ansvarar för att säkerhetspröva varje person som ska delta i kommunens säkerhetskänsliga verksamhet. Säkerhetsprövningen ska vara genomförd och ett beslut fattat innan deltagandet påbörjas. Därefter ska prövningen följas upp löpande under hela den tid personen deltar i verksamheten för att säkerställa att förutsättningarna för beslutet fortfarande kvarstår.

- säkerhetsskyddschef: har övergripande ansvar för att säkerhetsprövningar genomförs korrekt, fattar beslut om inplacering och hanterar kontakten med Säkerhetspolisen.
- säkerhetssamordnare: har operativt stöd i genomförandet, administration av ansökningar och löpande uppföljning.
- rekryterande chef/HR: ansvarar för den initiala rekryteringsprocessen, identitetskontroll och att kandidaten informeras om kravet på säkerhetsprövning.

3.3.5. Process för säkerhetsprövning

Säkerhetsprövningen består av en grundutredning och kan, beroende på säkerhetsklass och riskbild, kompletteras med registerkontroll och en särskild personutredning.

Fas 1: Rekrytering och urval	**Annonsering:** vid utlysning av tjänster med placering i säkerhetsklass ska det framgå att tjänsten kräver säkerhetsprövning, men inte vilken nivå det rör sig om, ”Tjänsten innebär att säkerhetsprövning enligt säkerhetsskyddslagen (2018:585) kommer att genomföras vid anställning.”. **Urval och identitetskontroll:** rekryterande chef genomför identitetskontroll genom verifiering av betyg, intyg och referenser. Den slutgiltiga kandidaten ges fördjupad information om prövningens syfte, genomförande och registerkontrollens innebörd.
Fas 2: Genomförande av prövningen	**Administration:** varje ärende hanteras med en checklista (*Bilaga 6 – Checklista och mallar för säkerhetsprövning*) för att säkerställa fullständig dokumentation. **Information och samtycke:** innan prövningen inleds erhåller kandidaten introduktionsmaterial om säkerhetsskyddets principer. Registerkontroll och särskild personutredning får endast genomföras efter ett skriftligt, informerat samtycke, vilket gäller för hela perioden av deltagandet i verksamheten. **Säkerhetsprövningsintervju:** genomförs av säkerhetssamordnare och/eller säkerhetsskyddschef enligt fastställd mall (*Bilaga 6 – Checklista och mallar för säkerhetsprövning)* för att fördjupa personkännedomen. **Underlag:** prövningen baseras på betyg, intyg, referenser, uppgifter från intervjun samt övriga relevanta uppgifter.
Fas 3: Extern prövning och inplacering	**Ansökan till Säkerhetspolisen:** säkerhetsenheten upprättar ansökan om registerkontroll. • kontrollorsak: ansökan ska innehålla en precis beskrivning av den säkerhetskänsliga verksamheten och de skyddsvärden som personen exponeras för.

	• logistik: handlingar skickas via rekommenderad post i grön säkerhetspåse med mottagningsbevis. Dokumentation arkiveras i särskild pärm. Handlingarna kan också skickas digitalt enligt särskild anvisning från Säkerhetspolisen. **Resultathantering:** svar från Säkerhetspolisen och övrigt underlag hanteras som säkerhetsskyddsklassificerade handlingar. Underlaget får uteslutande användas för säkerhetsprövningen.
Fas 4: Kvalificering och kompetensutveckling	**Obligatorisk grundutbildning:** innan tillträde till säkerhetskänslig verksamhet (och helst innan prövningen genomförs) ska följande digitala utbildningar vara genomförda: • grundläggande säkerhetsskyddsutbildning (utbildning från Försvarshögskolan och Myndigheten för civilt försvar) • utbildning om säkerhetsskyddsklassificerade handlingar (utbildning från Myndigheten för civilt försvar). **Specialutbildningar:** beroende på roll kan kompletterande utbildningar krävas, exempelvis för säkerhetsfunktioner, signalskydd (PGBI) via Länsstyrelsen eller specifik utbildning i registrering av klassificerade handlingar.
Fas 5: Förvaltning och kontinuerlig prövning	**Löpande uppföljning:** säkerhetsprövningen är en pågående process. Chefer ska vara uppmärksamma på förändringar hos medarbetarna, kopplat till livssituation, ekonomi eller beteende som kan påverka lämpligheten. • årlig kontroll: en uppföljande säkerhetsprövning genomförs årligen (*Bilaga 6 – Checklista och mallar för säkerhetsprövning*). • rapporteringsskyldighet: förändringar i äktenskap eller samboförhållande ska rapporteras till Säkerhetspolisen enligt gällande rutiner (undantaget säkerhetsklass 3 och säkerhetsprövning utan att vara inplacerad i säkerhetsklass). **Tjänsteförändring:** vid ändring av säkerhetsklass, kontrollorsak, person-/samordningsnummer, vem som beslutar om placering eller äktenskap/samboförhållande för klass 1 och 2 ska Säkerhetspolisen omedelbart meddelas och ny

	ansökan skickas för att säkerställa obruten inplacering.
Fas 6: Avslut och arkivering	**Upphörande:** vid avslut av uppdrag ska säkerhetsskyddschefen informeras av ansvarig chef eller HR om slutdatum i god tid. Vid inplacering i säkerhetsklass ska avslut göras även till Säkerhetspolisen. Behörigheter i system ska avslutas, nycklar och taggar ska återlämnas, koder till skåp ska ändras och samtliga behörighetslistor ska uppdateras (*Bilaga 6 – Checklista och mallar för säkerhetsprövning)*. **Avslutande samtal:** ett formellt avslutande säkerhetssamtal genomförs och dokumenteras för att påminna om det fortlöpande sekretessansvaret (*Bilaga 6 – Checklista och mallar för säkerhetsprövning).* **Arkivering:** ärenden avslutas i ordinarie system. Det fysiska, klassificerade underlaget arkiveras på säkerhetsenheten.

3.4. Fysisk säkerhet

Fysisk säkerhet ska förhindra obehörigt tillträde och skadlig påverkan (sabotage, våld, insyn, avlyssning) på platser där säkerhetskänslig verksamhet bedrivs.

Skyddet byggs upp genom:

- personal och rutiner: behörig och utbildad personal, bevakning och besökshantering.
- tekniska lösningar: larm, fysiska barriärer och tillträdeskontroll.
- hantering: planerade insatser för att upptäcka och hantera antagonistiska handlingar samt minska konsekvenser vid angrepp.

Säkerhetsskyddschefen beslutar om vilka utrymmen som är godkända för regelbunden behandling av säkerhetsskyddsklassificerade uppgifter och regelbundna samtal där konfidentiell eller högre information får behandlas.

Tillträde till säkerhetskänsliga utrymmen ges endast till behöriga och inte i större utsträckning än vad som är nödvändigt. Tillträde samt tillgång till kort, taggar och koder beslutas av säkerhetsskyddschefen och dokumenteras (*Bilaga 7 – Förteckning*

över kort, taggar, koder och nycklar). Ifylld förteckning förses med lämplig säkerhetsskyddsklass och förvaras därefter.

3.4.1. Rutin vid larm säkerhetsrum

Vid larm i säkerhetskänsligt utrymme utförs åtgärder enligt *Rutin vid larm säkerhetsrum*. Rutinen är sekretessklassificerad enligt 18 kap. 8 § offentlighets- och sekretesslagen (2009:400) och är endast tillgänglig för behöriga på säkerhetsenheten.

3.5. Informationssystem för hantering av säkerhetsskyddsklassificerad information

Informationssystem som har betydelse för säkerhetskänslig verksamhet ska ges ett säkerhetsskydd som är anpassat till verksamhetens skyddsvärden, identifierade säkerhetshot, sårbarheter och dimensionerande antagonistiska förmågor. Kraven omfattar både informationssystem som behandlar säkerhetsskyddsklassificerade uppgifter och andra informationssystem som har betydelse för säkerhetskänslig verksamhet.

Säkerhetsskyddsklassificerade uppgifter får endast behandlas i informationssystem eller på lagringsmedium som kommunen har godkänt för lägst den säkerhetsskyddsklass som uppgifterna har. När en säkerhetsskyddsklassificerad uppgift överlämnas ska mottagaren uppmärksammas på vilken säkerhetsskyddsklass uppgiften har.

Kommunen har med detta dokument fastställda rutiner för hantering av informationssystem under systemets förväntade livstid. Rutinen omfattar bland annat anskaffning och utveckling, driftsättning och förändring, behörighetsadministration, konfiguration och uppdatering, loggning och säkerhetsövervakning, incidenthantering, säkerhetskopiering och återställning samt avveckling och återanvändning av lagringsmedier.

Innan införande av ett informationssystem ska en särskild säkerhetsskyddsbedömning genomföras.

3.5.1. Ansvar

Säkerhetsskyddschefen ansvarar för att informationssystem som har betydelse för säkerhetskänslig verksamhet omfattas av tillräckliga säkerhetsskyddsåtgärder, att system som ska behandla säkerhetsskyddsklassificerade uppgifter är godkända för aktuell säkerhetsskyddsklass samt spårbarhet i systemen. Spårbarheten upprätthålls genom att behöriga användare loggar in med separata konton och att loggarna skyddas och bevaras.

Säkerhetssamordnare och berörda systemägare/systemförvaltare stödjer i genomförande, dokumentation, kontroll och uppföljning.

Enligt säkerhetsskyddslagen ska kommunen ha åtgärder på plats för att skydda information. Målet är att:

- förhindra att säkerhetsskyddsklassificerad information läcker ut, ändras eller förstörs.
- skydda system och uppgifter från annan skadlig påverkan.

För hantering av säkerhetsskyddsklassificerad information upp till säkerhetsskyddsklass begränsat hemlig används signalskyddsmateriel samt en sekretessdator med tillhörande utrustning.

Sekretessdatorn är en helt isolerad enhet, vilket innebär att den saknar koppling till internet, Bluetooth och andra nätverk. Sekretessdatorn används tillsammans med dokumentet *Användarmanual sekretessdator 10* från Göliska IT, manualen förvaras med hårdvaran. För rutin gällande signalskydd, se *Signalskyddsinstruktion Lidköpings kommun.*

3.5.2. Beställning av utrustning

Innan beställning av en sekretessdator görs ska säkerhetsskyddschef eller säkerhetssamordnare säkerställa följande:

1. **behovet är identifierat:** det finns ett faktiskt behov av att hantera och skapa uppgifter upp till nivån Begränsat hemlig.
2. **säkerhetsskyddsbedömning finns:** en särskild säkerhetsskyddsbedömning (SSB) är genomförd och godkänd av säkerhetsskyddschefen.

3. **fysiskt skydd är godkänt:** det finns ett godkänt säkerhetsskåp (klass SSF 3492) och ett säkert utrymme för förvaring.
4. **personal är behörig och utbildad:** personalen som ska använda datorn är säkerhetsprövad och har genomgått grundutbildning i säkerhetsskydd och hantering av säkerhetsskyddsklassificerade handlingar.

Framtagande av sekretessdator med utrustning sker via kommunalförbundet Göliska IT, granskningen görs gemensamt med kommunens säkerhetsenhet.

Leverans av tjänster från Göliska IT

- PC - HP Elitebook 6G1i 16”
- färglaserskrivare - Lexmark XC2326
- USB-minnen 128 GB för backup (max 5st)
- inköpshantering av hårdvara
- hantering av garantiärenden
- utleverans
- säkerhetsklassade skrotningsrutiner
- livscykelhantering
- Microsoft Win11-licens long life
- Microsoft Office Std-licens

3.5.3. Fysisk säkerhet och förvaring

- Dator, strömsladd och krypterade USB-stickor ska alltid förvaras i ett godkänt säkerhetsskåp (SSF 3492) och utrymme.
- Om datorn inte är inlåst måste den vara under konstant uppsikt av behörig personal. Medförande av dator utanför verksamhetsutövarens lokaler ske restriktivt.
- USB-stickor som innehåller säkerhetskopior ska förvaras i en brandbox, inuti säkerhetsskåpet.
- Dator och de USB-stickor som används ska vara tydligt märkta med vilken säkerhetsskyddsklass som högst får behandlas i systemet.

- Varje dator och tillhörande USB-stickor som används diarieförs i Evolution (*Bilaga 4 – Diarieföring av säkerhetsskyddsklassificerad handling*) och i det hemliga diariet (H-diariet) i sekretessdatorn.
- Alla lösenord (PIN-kod, BitLocker) ska förvaras separat från datorn.

3.5.4. Driftsättning och användning

Före driftsättning av ett informationssystem krävs test av skyddsåtgärder (penetrationstest) och att testresultatet är dokumenterat.

Uppstart och inloggning

Se *Användarmanual sekretessdator 10* från Göliska IT.

Vid utelåsning eller glömt lösenord

Se *Användarmanual sekretessdator 10* från Göliska IT.

Hantering av USB-stickor

Se *Användarmanual sekretessdator 10* från Göliska IT. För dataöverföring mellan sekretessdator och signalskyddssystem får endast den röda USB-stickan tillhörande signalskyddssystemet användas.

Innan användning

1. En okulär besiktning av rummet ska göras. Föremål som kan sända eller ta emot signaler (mobiltelefoner, smarta klockor, etcetera) **får inte** tas med in i utrymmet.
2. Endast behörig personal (registrerade i sambruksavtalet, *Bilaga 8 – Sambruksavtal sekretessdator*) får använda datorn.
3. Datorn får **aldrig** lämnas utan uppsikt.
4. Utrustning som inte är godkänd av säkerhetsskyddschef **får inte** kopplas in i datorn.

3.5.5. Skrivare och utskrifter

- För utskrift och kopiering får endast tillhörande godkänd skrivare användas.
- Efter varje användning ska ett svart papper kopieras för att skriva över tidigare spår.

- Töm minnet i skrivaren genom att dra ut strömsladden efter avstängning.

3.5.6. Underhåll och kontinuitet

Backup (säkerhetskopiering)

För att inte förlora viktig information ska backup göras **minst tre gånger per år**, eller vid behov (se *Årshjul säkerhetsskyddsarbete Lidköpings kommun*). För säkerhetskopiering, se *Användarmanual sekretessdator 10* från Göliska IT.

- Spara säkerhetskopian på tillhörande krypterad USB-sticka.
- Kontrollera minst en gång per år att backupen fungerar och att uppgifterna går att återställa.

Service och reparationer

Service och reparation av sekretessdatorn genomförs av Göliska IT på plats på säkerhetsenheten. En behörig person från säkerhetsenheten ska övervaka arbetes gång för att säkerställa att säkerhetsskyddsklassificerad information inte röjs och att datorn inte manipuleras.

3.5.7. Avveckling och förstöring

Säkerhetsskyddschefen tar beslut om avveckling av sekretessdator och lagringsmedium innan hårdvaran därefter får förstöras. Förstöringen ska ske på ett sätt som gör att informationen på den aldrig kan återskapas, det ska även dokumenteras i en förstöringsliggare för spårbarhet (*Bilaga 5 - Förstöringsliggare*). Ärendet avslutas därefter i diariet (både Evolution och H-diariet).

3.6. Säkerhetshotande händelser

En säkerhetshotande händelse är en händelse, incident eller pågående verksamhet som innebär (eller kan innebära) att säkerhetsskyddsåtgärder har kringgåtts, att säkerhetsskyddsklassificerade uppgifter har röjts eller att säkerhetskänslig verksamhet har utsatts för spionerі, sabotage eller terroristbrott.

Lidköpings kommun ska effektivt kunna identifiera, utreda, hantera och rapportera säkerhetshotande händelser eller verksamhet. Detta för att minimera skadeeffekter på Sveriges säkerhet, skydda säkerhetsskyddsklassificerade uppgifter och säkerställa att brister i säkerhetsskyddet åtgärdas för att förhindra upprepning.

3.6.1. Ansvar

Det operativa ansvaret för utredning och ansvaret för rapportering av säkerhetshotande händelser i Lidköpings kommun är enligt följande:

Säkerhetsskyddschef:

- har det övergripande ansvaret för att rutiner kring säkerhetshotande händelser implementeras och efterlevs.
- ansvarar för att utredningar initieras och genomförs med lämpligt säkerhetsskydd.
- beslutar om anmälan till Säkerhetspolisen och andra tillsynsmyndigheter.

Säkerhetssamordnare:

- genomför utredningar på delegation från säkerhetsskyddschefen.
- dokumenterar händelseförloppet och föreslår åtgärder.

Alla medarbetare/konsulter:

- är skyldiga att skyndsamt rapportera varje misstänkt eller konstaterad säkerhetshotande händelse till närmaste chef eller direkt till säkerhetsskyddschefen.

3.6.2. Hanteringsprocess

För stöd och dokumentation, använd *Rapport vid säkerhetshotande händelser och verksamhet* på Säkerhetspolisens hemsida.

Upptäckt och rapportering

Vid upptäckt av en händelse **ska** rimliga åtgärder omedelbart vidtas för att begränsa skadan. Händelsen rapporteras **omedelbart** till säkerhetsskyddschefen eller biträdande säkerhetsskyddschef.

Utredning och omfattning

Utredning och skadebedömning ska påbörjas skyndsamt efter att en säkerhetshotande händelse har inträffat. Säkerhetsskyddschefen eller utsedd säkerhetssamordnare leder utredningen för att fastställa:

- händelseförlopp: vad har hänt, när, hur och av vem (om känt)?
- berörda skyddsvärden: vilka uppgifter eller fysiska tillgångar är påverkade?
- skadebedömning: bedömning av skadan för Sveriges säkerhet baserat på uppgifternas klassificering:
    - kvalificerat hemlig: synnerligen allvarlig skada.
    - hemlig: allvarlig skada.
    - konfidentiell: inte obetydlig skada.
    - begränsat hemlig: ringa skada.

Analys av systemfel

Utredningen ska identifiera om händelsen beror på mänsklig faktor, tekniskt fel eller brister i styrdokumenten. **Viktigt:** utredningen ska analysera om den aktuella risken fanns med i kommunens säkerhetsskyddsanalys. Om inte, ska analysen uppdateras.

Anmälan till Säkerhetspolisen

Om det finns skäl att anta att händelsen påverkar Sveriges säkerhet ska anmälan göras skyndsamt till Säkerhetspolisen och enligt deras mall. Vid osäkerhet om anmälningsplikt ska anmälan göras ändå. Säkerhetspolisen meddelar sedan i sin tur till kommunens tillsynsmyndighet.

Åtgärdsplan och genomförande

En konkret åtgärdsplan upprättas för att:

1. stoppa den pågående händelsen (om tillämpligt).
2. återställa säkerheten.
3. förhindra upprepning (till exempel genom tekniska åtgärder, ändrade rutiner eller utbildning).

Slutrapport och dokumentation

En fullständig rapport sammanställs med utredningens resultat, vidtagna åtgärder och utvärdering. Rapporten arkiveras med lämpligt säkerhetsskydd.

Utvärdering

Händelsen utvärderas i efterhand för att se om rutinen för hantering av händelser fungerat effektivt.

Uppföljning

Processen för hantering av säkerhetshotande händelser revideras årligen eller vid behov efter allvarliga incidenter för att säkerställa att den är anpassad efter aktuella hotbilder och lagkrav.

Utbildning och medvetenhet

All personal med behörighet ska ha god kännedom om hur säkerhetshotande händelser ska rapporteras. Detta upprätthålls genom övning.

4. Utbildning

Den som är ansvarig för den säkerhetskänsliga verksamheten ska se till att de medarbetare som ska komma i kontakt med säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd, innan medarbetare får åtkomst till säkerhetsskyddsklassificerad information eller verksamhet. Behovet av utbildning ska också följas upp löpande, utifrån en utbildningsplan. Innan säkerhetsprövning och uppföljande säkerhetsprövning genomförs ska grundläggande säkerhetsskyddsutbildning (digital utbildning från Försvarshögskolan och Myndigheten för civilt försvar) och utbildning om säkerhetsskyddsklassificerade handlingar (digital utbildning från Myndigheten för civilt försvar) genomföras. Intyg från genomförda utbildningar ska arkiveras hos säkerhetsenheten, tillsammans med ett utbildningsregister.

De medarbetare som ska ingå i kommunens signalskyddsorganisation ska genomgå riktade utbildningar inom signalskydd, se *Signalskyddsinstruktion Lidköpings kommun.*

5. Bilagor

Bilaga 1 – Samförvaringsbeslut

Bilaga 2 – Delgivning och kvittering

Bilaga 3 – Beslut om medförande

Bilaga 4 – Diarieföring av säkerhetsskyddsklassificerad handling

Bilaga 5 – Förstöringsliggare

Bilaga 6 – Checklista och mallar för säkerhetsprövning SEKRETESS 35 kap. 1 § Offentlighets- och sekretesslagen (finns förvarad hos säkerhetsenheten)

Bilaga 7 – Förteckning över kort, taggar, koder och nycklar

Bilaga 8 – Sambruksavtal sekretessdator

Bilaga 9 – Behörig att hantera säkerhetsskyddsklassificerad information

Bilaga 10 – Inventering av säkerhetsskyddsklassificerade handlingar

Bilaga 11 – Internkontroll säkerhetsskydd

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 1 – Samförvaringsbeslut

Nedanstående personer är behöriga att använda angivet förvaringsutrymme. Beslut tas av säkerhetsskyddschef. Ifylld mall är säkerhetsskyddsklassificerad. **Kod på förvaringsutrymmet byts när personer tas bort från listan.**

Beteckning på förvaringsutrymme	
Plats för förvaringsutrymme (rum)	
Beslut fattat av:	Datum: Namn, befattning: Signatur:

Namn och verksamhet	Personnummer	Tillträde (datum, sign. beslut)	Avslutat (datum, sign. beslut)

Namn och verksamhet	Personnummer	Tillträde (datum, sign. beslut)	Avslutat (datum, sign. beslut)

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 2 – Delgivning och kvittering

Beslut om delgivning tas av säkerhetsskyddschef. Ifylld mall är säkerhetsskyddsklassificerad. Kvittens ska bevaras i minst 10 år för handlingar i säkerhetsskyddsklass konfidentiellt och hemlig, samt i 25 år för kvalificerat hemlig.

Handling/ärende (namn på dokument eller mötets syfte)	
Klassificeringsnivå	
Ansvarig för delgivning (namn och befattning)	
Datum för delgivning	
Plats/mötesrum	

Markera vilken typ av delgivning som avser denna lista:

☐ **Fysisk handling:** Mottagaren har erhållit/tagit del av ett fysiskt dokument.

☐ **Muntlig information:** Mottagaren har tagit del av informationen under möte/genomgång.

☐ **Digitalt medium:** Mottagaren har fått tillgång till information via krypterat system.

Genom min underskrift bekräftar jag att jag har tagit del av den ovan nämnda informationen. Jag är medveten om informationens säkerhetsskyddsklassificering och förbinder mig att hantera informationen i enlighet med gällande säkerhetsskyddsinstruktioner och sekretessbestämmelser. Jag är införstådd med att obehörigt röjande av informationen kan leda till rättsliga påföljder.

Namn, verksamhet	Personnummer	Tidpunkt	Underskrift

Särskilda villkor *(till exempel om handlingen ska lämnas tillbaka efter mötet, eller om informationen endast fick läsas på plats)*

Signatur, ansvarig för delgivningen: _____
Datum: _____

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 3 – Beslut om medförande

Beslut om medförande tas av säkerhetsskyddschef. Ifylld mall är säkerhetsskyddsklassificerad.

Syfte med transporten	
Godkännande	Datum: Namn, signatur:

Handlingens namn/ID	Antal ex.	Format (papper/USB/hårddisk)	Klassificering

Markera de åtgärder som vidtagits för att säkra handlingarna under transporten:

☐ Dubbelt kuvert
☐ Kryptering
☐ Ständig tillsyn

Utlämning från förvar
Härmed bekräftas att ovan nämnda handlingar har lämnats ut till transportansvarig

Datum/tid: _____

Signatur utlämnare: _____

Transportansvarig
Jag bekräftar att jag tagit emot handlingarna och åtar mig fullt ansvar för deras säkerhet under transporten

Datum/tid: _____

Namn och signatur _____

Mottagande och kvittens
Härmed bekräftas att ovan nämnda handlingar har mottagits i oskadat skick och att förseglingar varit intakta.

Datum/tid: _____

Signatur mottagare: _____

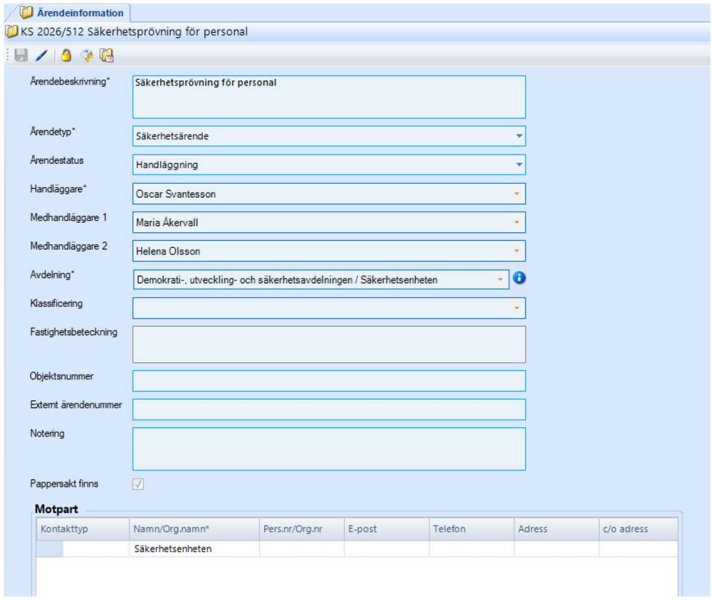
Avvikelser (till exempel brutna förseglingar)

Lidköpings kommun

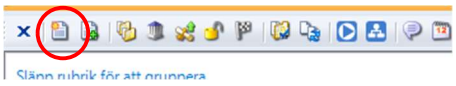
Diarienummer: _____
Handlings-ID: _____

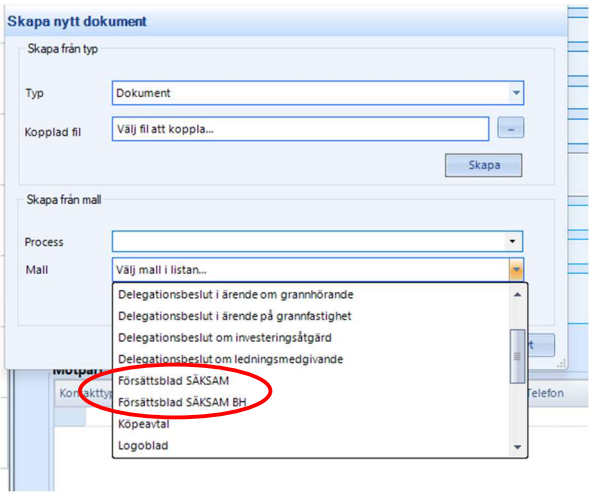
Bilaga 4 – Diarieföring av säkerhetsskyddsklassificerad handling

a) Ett nytt ärende skapas av kanslienheten i Lidköpings kommun. Ärendemeningen ska vara öppen och övergripande utan detaljer kring vad som är säkerhetsskyddsklassificerat (exempel ”Säkerhetsprövning för personal”, det ska inte framgå vem som har säkerhetsprövats eller var i organisationen personen finns). Rutan ”Pappersakt finns” ska bockas i om en sådan finns.

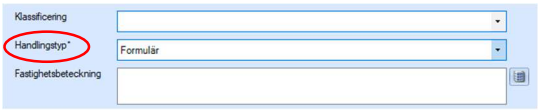


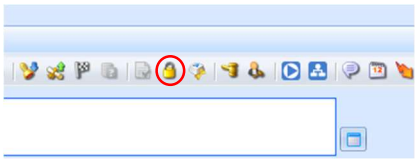
b) Skapa en ny handling och välj mall ”Försättsblad SÄKSAM” om handlingen endast omfattas av sekretess, och mall ”Försättsblad SÄKSAM BH” om handlingen dessutom är säkerhetsskyddsklassificerad.



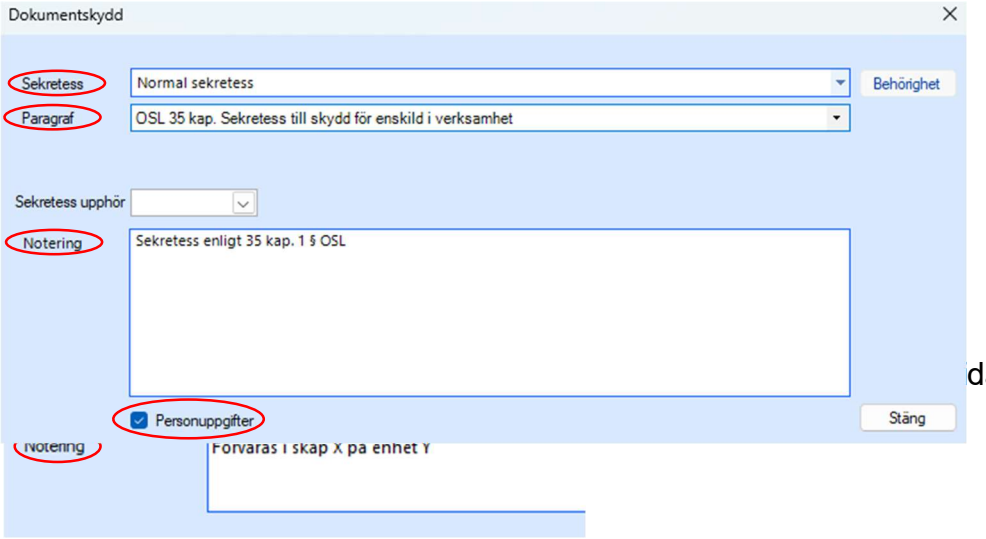


c) Välj passande handlingstyp och tryck sedan på hänglåset för att välja rätt dokumentskydd.



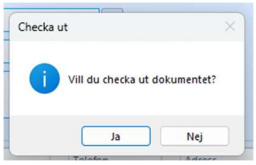


Välj ”Normal sekretess” i listan för ”Sekretess” och sedan rätt kapitel enligt OSL i listan för ”Paragraf”. Skriv även vilken paragraf i kapitlet som handlingen omfattas av, se exempel nedan. Om det finns personuppgifter i handlingen ska rutan ”Personuppgifter” bockas i. Tryck på ”Stäng”.

d) 

dan.

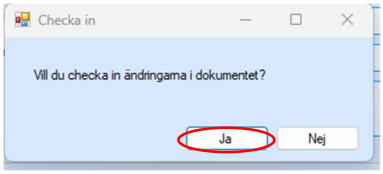
Tryck på spara och välja att checka ut dokumentet.



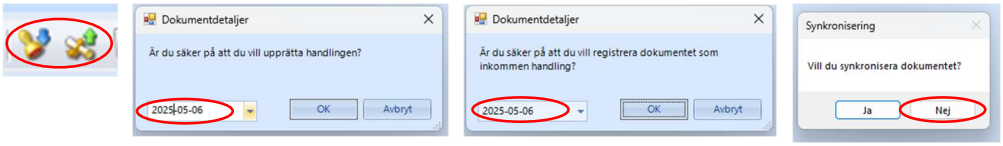
e) Försättsbladet öppnas då upp som ett Word-dokument, färdigställ det (**OBS!** Inga säkerhetsskyddsklassificerade uppgifter!), spara och stäng. Skriv in ”Säkerhetsenheten” i fältet för ”Kopplas in från enhetens beskrivning”. Tillse att datumen överensstämmer.



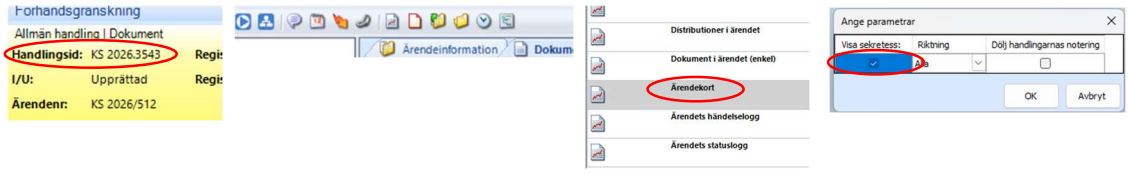
f) Välj att checka in ändringarna.



g) Fastställ dokumentet med rätt datum som upprättat eller inkommet, välj att **inte** synkronisera.



h) Handlingen får ett handlings-ID, detta ska dokumenteras i H-diariet i sekretessdatorn. Skriv ut ärendekort och förvara tillsammans med de fysiska handlingarna.



i) Meddela kansliet när handlingar ska ersättas med nya eller avslutas.

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 5 – Förstöringsliggare

Ifylld mall är säkerhetsskyddsklassificerad. **Dokumentet sparas i minst 10 år.**

Gäller för år: ……

Dokumentbeskrivning/ ärendemening	Diarienr. / handlings-ID	Upprättad/ inkommen datum	Exemplar (original/ kopior)	Arkivmedium (papper/digitalt)	Datum, namn, befattning

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 6 – Checklista och mallar för säkerhetsprövning

Originalhandlingen innehåller sekretessklassificerade uppgifter enligt 35 kap. 1 § Offentlighets- och sekretesslagen (2009:400) och finns förvarad hos säkerhetsenheten.

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 7 – Förteckning över kort, taggar, koder och nycklar

Nedanstående personer är behöriga att använda angivet förvaringsutrymme, beslut tas av säkerhetsskyddschef. Kort, koder, taggar och nycklar ska lämnas in när personer tas bort från listan och kod på förvaringsutrymmet ska bytas. Översyn av listan görs enligt ***Årshjul säkerhetsskyddsarbete Lidköpings kommun***. Ifylld mall är säkerhetsskyddsklassificerad.

Beteckning på förvaringsutrymme	
Plats för förvaringsutrymme (rum)	
Beslut fattat av:	Datum: Namn, befattning: Signatur:

Namn och verksamhet	Personnummer	Materiel och ID	Tillträde (datum, sign. beslut)	Avslutat och lämnat in materiel (datum, sign. beslut)
		Kort ☐ Tagg ☐ Kod ☐ Nyckel ☐		

Namn och verksamhet	Personnummer	Materiel och ID	Tillträde (datum, sign. beslut)	Avslutat och lämnat in materiel (datum, sign. beslut)
		Kort ☐ Tagg ☐ Kod ☐ Nyckel ☐		
		Kort ☐ Tagg ☐ Kod ☐ Nyckel ☐		
		Kort ☐ Tagg ☐ Kod ☐ Nyckel ☐		
		Kort ☐ Tagg ☐ Kod ☐ Nyckel ☐		
		Kort ☐ Tagg ☐ Kod ☐ Nyckel ☐		

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 8 – Sambruksavtal sekretessdator

Nedanstående personer är behöriga att använda angiven sekretessdator för säkerhetsskyddsklassificerade uppgifter. Beslut tas av säkerhetsskyddschef. Ifylld mall är säkerhetsskyddsklassificerad.

Beteckning på dator	
Säkerhetsskyddsklass	

Namn och verksamhet	Personnummer	Tillgång (datum, sign. beslut)	Avslutat (datum, sign. beslut)

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 9 – Behörighet att hantera säkerhetsskyddsklassificerad information

Nedanstående är en förteckning över behöriga att hantera säkerhetsskyddsklassificerad information. Beslutet fattas av säkerhetsskyddschef. Förteckningen uppdateras löpande och ses även över enligt *Årshjul säkerhetsskyddsarbete Lidköpings kommun*.
Ifylld mall är säkerhetsskyddsklassificerad.

Anmärkningar (begränsningar/avsteg kommenteras)

Beslut fattat av:

Namn, befattning: _____

Datum: _____

Namn	Personnummer	Verksamhetsplats	BH	K	H
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 10 – Inventering av säkerhetsskyddsklassificerade handlingar

Inventeringen omfattar säkerhetsskyddsklassificerade handlingar i alla former (pappersformat, lagringsmedier, osv.) i säkerhetsskyddsklass **konfidentiell** eller högre. Ifylld mall är säkerhetsskyddsklassificerad.

Datum för inventering: _____

Handläggare för inventeringen:

Namn, befattning: _____

Namn, befattning: _____

Handlingens beteckning/ ID	Handlingens benämning	Säkerhets-skyddsklass	Antal sidor	Bilagor	Antal exemplar och innehavare av respektive exemplar-nr	Förvaring

Inventeringsresultat:
☐Inga handlingar saknades
☐Handlingar saknades (listas under saknade handlingar)

Saknade handlingar	
Handlingsnummer	Kommentar och vidare åtgärder

Inventering fastställd av (namn, befattning): _____

Datum: _____

Lidköpings kommun

Diarienummer: _____
Handlings-ID: _____

Bilaga 11 – Internkontroll säkerhetsskydd

Syftet med internkontrollen är att säkerställa att kommunen bedriver ett systematiskt och ändamålsenligt säkerhetsskyddsarbete samt uppfyller krav enligt säkerhetsskyddslag (2018:585), säkerhetsskyddsförordning (2021:955) samt tillhörande föreskrifter. Internkontrollen fastställs av säkerhetsskyddschef. Ifylld mall är säkerhetsskyddsklassificerad.

Datum för kontroll: _____

Kontrollansvarig (namn, befattning):

_____

Kontrollområden

A. Styrning och organisation

Kontrollpunkt	Ja	Nej	Delvis	Kommentar
Säkerhetsskyddsansvar är tydligt beslutat				
Säkerhetsskyddschef är utsedd				
Roller och ansvar är dokumenterade				
Presentera status för arbete med säkerhetsskydd och incidentrapporter för kommundirektör				
Rutiner för rapportering av avvikelser finns				

Risknivå: □ låg □ medel □ hög

B. Säkerhetsskyddsanalys, -plan och befattningsanalys

Kontrollpunkt	Ja	Nej	Delvis	Kommentar
Säkerhetsskyddsanalys är genomförd				
Säkerhetsskyddsplan är genomförd				
Åtgärdsplan finns				
Befattningsanalys finns				
Analysen är aktuell (högst 2 år eller vid förändring)				

Risknivå: □ låg □ medel □ hög

C. Personalsäkerhet

Kontrollpunkt	Ja	Nej	Delvis	Kommentar
Rutiner för säkerhetsprövning finns och följs				
Registerkontroller genomförs där krav finns				
Samtliga behörighetslistor är aktuella				
Säkerhetsskyddsavtal och -överenskommelser finns där så krävs				
Rutiner finns för avslut av behörigheter				
Kravställda utbildningar har genomförts				

Risknivå: □ låg □ medel □ hög

D. Informationssäkerhet

Kontrollpunkt	Ja	Nej	Delvis	Kommentar
Informationsklassning är genomförd				
SSB för informationssystem är aktuell				
Säkerhetsskyddsklassificerade uppgifter är identifierade				
Behörighetsstyrning tillämpas enligt behovsprincipen				
Loggning och uppföljning sker (inkl. backup-kontroller USB-stickor)				
Krypteringslösningar används där krav finns				
Rutiner för incidenthantering finns				

Risknivå: □ låg □ medel □ hög

E. Fysisk säkerhet

Kontrollpunkt	Ja	Nej	Delvis	Kommentar
Skyddsvärda lokaler är identifierade				
Passerkontroll finns				
Uppföljning av passageloggar sker				
Nyckel- och taggadministration är aktuell				
Larm finns där behov föreligger				

Rutiner finns för förvaring av skyddsvärd information				

Risknivå: □ låg □ medel □ hög

F. Upphandling och avtal

Kontrollpunkt	Ja	Nej	Delvis	Kommentar
Rutiner finns för bedömning av säkerhetsskydd vid upphandling				
Säkerhetsskyddsbedömning genomförs före upphandling				
Säkerhetsskyddsavtal och -överenskommelser tecknas vid behov				
Leverantörer följs upp och avslutas				
Säkerhetsskyddskrav inkluderas i avtalen				

Risknivå: □ låg □ medel □ hög

G. Incidenter och avvikelser

Kontrollpunkt	Ja	Nej	Delvis	Kommentar
Rutiner för anmälan och rapportering finns				
Incidenter dokumenteras				
Utredningar genomförs				
Korrigerande åtgärder följs upp				
Eventuell rapportering till tillsynsmyndighet sker				

Risknivå: □ låg □ medel □ hög

Sammanfattande riskbedömning

Kontrollområde	Risknivå	Kommentar
Styrning och organisation		
Säkerhetsskyddsanalys		
Personalsäkerhet		
Informationssäkerhet		
Fysisk säkerhet		
Upphandling och avtal		
Incidenthantering		

Övergripande bedömning

☐ Godtagbar nivå
☐ Vissa brister behöver åtgärdas
☐ Allvarliga brister kräver omedelbara åtgärder

Åtgärdsplan

Identifierad brist	Åtgärd och eventuell kostnad	Ansvarig	Klart senast	Status

Beslut

Internkontroll fastställd av (namn, befattning): _____

Datum: _____

6. Referenslista

Säkerhetsskyddslagen (2018:585)

Säkerhetsskyddsförordningen (2021:955)

Säkerhetspolisens föreskrifter om säkerhetsskydd (konsoliderad PMFS 2022:1 med ändringar enligt PMFS 2026:8)

Lidköpings kommuns säkerhetsskyddsanalys (KS 2025/234)

Signalskyddsinstruktion Lidköpings kommun (KS 2024/149)