



Riktlinje

För signal- och säkerhetsskydd



Herrljunga
kommun

Dokumentinformation

Diarienummer:	KS-2025-00305
Fastställt:	Kommunstyrelsen 2023-04-24 § 74
Senast reviderad:	Kommunstyrelsen 2025-10-16 § 184
Giltig till:	Tills vidare
Dokumentansvarig:	Säkerhets- och beredskapsenheten

Innehållsförteckning

1. Allmänt.....	4
1.1 Syfte	4
1.2 Mål	4
1.3 Berörda lagar och andra regelverk	4
2. Ansvarsfördelning.....	4
2.1 Signalskyddsorganisation	6
3. Säkerhetsskyddsanalys och säkerhetskyddsplan	6
4. Informationssäkerhet.....	6
5. Fysisk säkerhet.....	7
6. Personalsäkerhet.....	7
7. Säkerhetsskyddsavtal/överenskommelse	9
8. Incidenthantering	10
9. Internkontroll.....	10
10. Tillsyn, viten och sanktionsavgift	10

1. Allmänt

Riktlinjen är underställd kommunens säkerhetspolicy och gäller för alla verksamheter i Herrljunga kommun, exklusive de kommunala bolagen, och fastställs av kommunstyrelsen. Utifrån riktlinjen finns framtagna rutiner som ger mer detaljerad information och som fastställs av säkerhetsskyddschef respektive signalskyddschef alternativt kommundirektör. Rutinerna omfattas i vissa fall av sekretess enligt offentlighets- och sekretesslagen (OSL 2009:400).

Säkerhetsskydd avser arbetet med att skydda information och verksamheter som har betydelse för Sveriges säkerhet eller som Sverige har förbundit sig att skydda genom internationella åtagande, mot antagonistiska hot såsom spioneri, sabotage och terroristbrott. När säkerhetsskyddsklassificerad information ska kommuniceras digitalt krävs att informationen krypteras med ett system som har godkänts av Försvarmakten, så kallat signalskydd.

1.1 Syfte

Syftet med riktlinjen är konkretisera säkerhetspolicy avseende signal- och säkerhetsskydd. Riktlinjen och dess underliggande rutiner redovisar Herrljunga kommuns reglering och organisation av signal- och säkerhetsskyddsarbetet och därmed hur gällande lagar och vägledningar ska uppfyllas.

1.2 Mål

Kommunens mål med signal- och säkerhetsskyddsarbetet är att:

- Säkerställa att kommunens information och verksamhet som berörs av säkerhetsskydd identifieras och analyseras.
- Skydda kommunens säkerhetsskyddsklassificerade information och verksamhet så att den inte kommer obehöriga till del, förvanskas eller blir otillgänglig/förstörd.

1.3 Berörda lagar och andra regelverk

Följande regelverk utgör grunden för denna riktlinje och underliggande rutiner:

- Säkerhetsskyddslag (2018:585)
- Säkerhetsskyddsförordning (2021:955)
- Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)
- Säkerhetspolisens vägledningar
- Försvarmaktens föreskrifter om signalskyddstjänsten (FFS 2021:1)
- Försvarmaktens interna bestämmelser (FIB 2008:3)
- Handbok TST Grunder 2007
- Säkerhetsmässiga krav för signalskyddsnycklar 2010

2. Ansvarsfördelning

Ansvaret för säkerhetsskyddsarbetet (inkl. signalskyddsarbetet) följer övergripande samma ansvarsstruktur som redovisas i säkerhetspolicyn. Regelverken inom säkerhetsskyddsområdet kräver dock några ytterligare specifika roller vilka redovisas nedan tillsammans med några förtydliganden (en person kan inneha flera roller):

Säkerhetsskyddschef

Säkerhetsskyddschefen ska leda och samordna säkerhetsskyddsarbetet samt kontrollera att verksamheten bedrivs enligt berörda lagar och föreskrifter, detta ansvar kan inte delegeras. Säkerhetsskyddschef är direkt underställd kommundirektör.

Biträdande säkerhetsskyddschef

Säkerhetsskyddschef kan utse en eller flera biträdande säkerhetsskyddschefer som stöttar säkerhetsskyddschefen i dess arbete och kan ersätta säkerhetsskyddschef vid längre sjukdom, ledighet m.m.

Anställda som skapar/hanterar säkerhetsskyddsklassificerad information

Den som skapar/hanterar en handling som innehåller säkerhetsskyddsklassificerad information ska vara behörig och ansvarar för att handlingen hanteras enligt denna riktlinje och underliggande rutin.

Signalskyddschef

Signalskyddschef ansvarar för att leda och samordna signalskyddet i kommunen. För att inneha rollen ska en signalskyddschefsutbildning genomförts med godkänt resultat hos Totalförsvarets signalskyddsskola eller annan behörig utbildare.

Biträdande signalskyddschef

Signalskyddschef ska utse minst en biträdande signalskyddschef som stöttar signalskyddschefen i dess arbete att hantera ledning och samordning av signalskyddstjänsten. Biträdande signalskyddschef ska ha genomgått användar- och administratörsutbildning på Signe kryptodator, operatörsutbildning på filkrypto/PGBI och därutöver fått anpassad information/utbildning av signalskyddschefen.

Minst en biträdande signalskyddschef ska dessutom vara utbildad signalskyddschef för att skapa en robust organisation vid personalomsättning, längre sjukdomsfrånvaro osv eftersom det finns ett krav att det alltid ska finnas en signalskyddschef i tjänst så länge signalskyddssystem och nycklar hanteras i organisationen.

Systemoperatör/lokal administratör

Ansvarar för att skapa och hantera användarkonton, genomföra uppdateringar och exportera loggfiler i signalskyddssystemet. För att inneha rollen ska personen ha genomgått användar- och administratörsutbildning på Signe kryptodator samt operatörsutbildning på filkrypto/PGBI.

Nyckeladministratör

Administrerar kommunens tilldelade signalskyddsnycklar och utbildas av signalskyddschefen.

Användare av signalskyddssystem

Anställda som använder signalskyddssystemet för att kryptera/dekryptera information. Ska ha genomgått användarutbildning på Signe kryptodator och filkrypto/PGBI.

2.1 Signalskyddsorganisation

I Herrljunga kommuns signalskyddsorganisation ingår rollerna signalskyddschef, biträdande signalskyddschef, systemoperatör/lokal administratör samt nyckeladministratör (en person kan inneha mer än en roll). Organisationen gäller såväl i fredstid som vid höjd beredskap.

3. Säkerhetsskyddsanalys och säkerhetsskyddsplan

Kommunen ska minst vartannat år göra en säkerhetsskyddsanalys, i enlighet med säkerhetspolisens föreskrifter. Kortfattat kan analysen beskrivas som att den ska svara på tre frågor:

- Vad ska skyddas?
- Mot vad ska det skyddas?
- Hur ska det skyddas?

Förvaltningschefer och andra berörda befattningar ska bistå säkerhetsskyddschefen i analysarbetet. De behov av åtgärder som framkommer vid analysen sammanställs till en säkerhetsskyddsplan som tydligt anger vem som ansvarar för att åtgärden genomförs samt en tidsplan för genomförandet. I samband med säkerhetsskyddsanalysen ska även en befattningsanalys göras som visar vilka befattningar som kommer i kontakt med den säkerhetskänsliga informationen/verksamheten. De personer som innehar dessa befattningar ska säkerhetsprövas (undantag är politiker i kommunfullmäktige som inte får säkerhetsprövas).

4. Informationssäkerhet

Informationssäkerhetsarbetet omfattar all information oavsett i vilken form den är (fysisk på papper, muntlig eller digital) och ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs. Arbetet ska också förebygga skadlig inverkan i övrigt på uppgifter och informationssystem i säkerhetskänslig verksamhet. Grunden för detta arbete är kommunens ordinarie arbete med informationssäkerhet i enlighet med riktlinjen för informationssäkerhet men ytterligare krav enligt nedan tillkommer.

Säkerhetsskyddsklasser

Information som berörs av säkerhetsskyddslagen omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och ska delas in i olika säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan ge för Sveriges säkerhet:

- Kvalificerat hemlig = Synnerligen allvarlig skada

- Hemlig = Allvarlig skada
- Konfidentiell = En inte obetydlig skada
- Begränsat hemlig = Ringa skada

Säkerhetskrav vid hantering

En säkerhetsskyddsklassificerad handling ska alltid vara under kontroll (det vill säga i behörig persons omedelbara närhet och uppsikt) eller inlåst i ett godkänt förvaringsutrymme.

Elektronisk hanteringen av säkerhetsklassificerad information ska hålla en hög säkerhet i enlighet med säkerhetspolisens föreskrifter, vilket till exempel innebär att säkerhetsskyddsklassificerad information bara får hanteras och förvaras elektroniskt i en fristående dator med hög säkerhet. Informationen får alltså inte hanteras i kommunanställdas ordinarie datorer.

Detaljerad information om hur säkerhetsskyddsklassificerade handlingar ska hanteras tex. hur de ska märkas, förvaras, skickas och förstöras finns i en underliggande rutin till denna riktlinje.

Kryptodator Signe

För att skydda säkerhetskänslig information vid digital överföring ska kryptografiska funktioner som godkänts av Försvarmakten användas. Signe kryptodator som Länsstyrelsen tilldelat kommunen innehåller signalskyddssystemet filkrypto/PGBI och är godkänd att användas för information i säkerhetsskyddsklass begränsat hemlig. Länsstyrelsen kräver som en följd av detta att Herrljunga kommun följer FFS 2021:1 samt de övriga säkerhetsmässiga krav som Försvarmaktens högkvarter meddelar avseende signalskyddssystemen och dess ingående delar.

Detaljerad information som tydliggör hur signalskyddssystem och säkerhetsskyddsklassificerade informationssystem ska konfigureras och administreras finns i underliggande rutiner till denna riktlinje.

5. Fysisk säkerhet

För att säkerställa att endast behöriga personer får tillgång till säkerhetsklassificerad information och verksamhet ska berörda områden/byggnader/rum skyddas fysiskt i enlighet med det skyddsbehov som framkommer i säkerhetsskyddsanalysen. Det kan tex. handla om passersystem, larm och inbrottsskydd.

6. Personalsäkerhet

Endast personer som bedöms vara lojala och pålitliga ur säkerhetssynpunkt ska ha tillgång till säkerhetsskyddsklassificerad information och verksamhet. Därför ska personer som innehar de befattningar som pekats ut i befattningsanalysen säkerhetsprövas.

Säkerhetsklass

Utifrån hur säkerhetskänslig information/verksamhet som en befattning kommer hantera placeras den i olika säkerhetsklasser.

Säkerhetsklass 1:

Tar del av kvalificerat hemliga uppgifter i en omfattning som inte är ringa eller kan orsaka synnerligen allvarlig skada för Sveriges säkerhet.

Säkerhetsklass 2:

Tar del av hemliga uppgifter i en omfattning som inte är ringa eller i ringa omfattning kvalificerat hemlig alternativt kan orsaka allvarlig skada för Sveriges säkerhet.

Säkerhetsklass 3:

Tar del av konfidentiella uppgifter eller i ringa omfattning hemliga uppgifter alternativt kan orsaka en inte obetydlig skada för Sveriges säkerhet.

Den som bara hanterar uppgifter i säkerhetsskyddsklassen begränsat hemlig och endast kan orsaka ringa skada ska också säkerhetsprövas men inte placeras i säkerhetsklass och det görs då inte heller någon registerkontroll.

Alla som ingår i signalskyddsorganisationen ska minst vara placerade i säkerhetsklass 3.

Säkerhetsprövning

Närmsta chef ansvarar för att säkerställa att person som ska inneha en befattning som kräver säkerhetsprövning, prövas innan personen påbörjar sin anställning alternativt får tillgång till säkerhetsskyddsklassificerad information eller verksamhet. Gäller det en nyanställning bör det redan vid rekryteringen framgå för den sökande att tjänsten kräver en säkerhetsprövning. Säkerhetsskyddschef ansvarar för att säkerhetsprövningen av berörda personer genomförs efter att det efterfrågats av berörd chef.

Säkerhetsprövningen omfattar flera steg:

- Grundutredning av berörd persons personliga förhållanden vilket bland annat innefattar kontroll av betyg, referenser samt relevanta öppna källor såsom sociala medier. Genomförs av säkerhetsskyddschef eller av denne utsedd person.
- Säkerhetsprövningsintervju där lojalitet, pålitlighet och sårbarhet bedöms. Genomförs av säkerhetsskyddschef eller av denne utsedd person.
- Registerkontroll i bland annat belastnings- och misstankeregistret. För placering i säkerhetsklass 1 och 2 omfattar kontrollen även make/maka/sambo. Genomförs av Säkerhetspolisen och fortgår under hela den tid personen är säkerhetsklassad.
- Särskild personutredning som bland annat innebär att personens ekonomiska förhållanden kontrolleras. Denna utredning sker bara vid placering i säkerhetsklass 1 och 2, då det även krävs att personen är svensk medborgare. Genomförs av Säkerhetspolisen.
- För placering i säkerhetsklass 1 ska en begäran först skickas till regeringen.

Innan registerkontroll och i förekommande fall särskild personutredning genomförs ska berörd person ge sitt skriftliga samtycke. Samtycket gäller för hela den tid personen innehar den säkerhetsklassade befattningen.

Om en persons säkerhetsprövningen inte blir godkänd får personen inte hantera säkerhetsskyddsklassificerad information eller verksamhet vilket kan få konsekvensen att tänkt anställning inte genomförs eller att befintlig anställning/uppdrag behöver anpassas. Resultatet av säkerhetsprövningen delges berörd chef som beslutar om eventuella åtgärder.

Löpande uppföljning

Minst en gång per år, tex. i samband med medarbetarsamtal, ska närmsta chef följa upp om det skett några förändringar eller händelser i den säkerhetsprövades liv (såväl privat som på arbetet) som kan påverka säkerhetsprövningen. Det kan tex. röra sig om ändrat civilstånd, missbruk, ekonomiska svårigheter, brottslighet eller brist på lojalitet mot Sverige. Framkommer sådana uppgifter ska säkerhetsskyddschefen omedelbart informeras. Närmsta chef ska dokumentera att uppföljningen har skett.

Säkerhetsprövad person slutar eller får andra uppgifter

När en säkerhetsprövad anställd slutar eller får en annan befattning ska det omedelbart meddelas säkerhetsskyddschef som ansvarar för att meddela säkerhetspolisen att registerkontroll ska upphöra alternativt förändras. Närmsta chef ansvarar för att ett avslutande säkerhetssamtal genomförs där bland annat tystnadsplikten repeteras. Chef ska dokumentera att avslutningssamtal har hållits.

Utbildning

Personer som deltar i säkerhetskänslig verksamhet ska ha tillräcklig kunskap om säkerhetsskydd. Säkerhetsskyddschef ansvarar för att information/grundutbildning ges efter genomgången säkerhetsprövning. Närmsta chef ansvarar därefter för att säkerställa att kunskapen upprätthålls och vid behov fördjupas. Personer som ingår i signalskyddsorganisationen utbildas av signalskyddschef, biträdande signalskyddschef, Totalförsvarets signalskyddsskola eller annan part i enlighet med gällande regelverk. All utbildning ska dokumenteras i listan över säkerhetsskyddsbehörig personal respektive personal som ingår i signalskyddsorganisationen. Säkerhetsskyddschef respektive signalskyddschef förvaltar dessa listor.

Tystnadsplikt

Den som deltar eller har deltagit i säkerhetskänslig verksamhet lyder under sekretess enligt Offentlighets- och sekretesslagen (2009:400). Detsamma gäller den som fått del av uppgifter i samband med säkerhetsprövning.

7. Säkerhetsskyddsavtal/överenskommelse

Om kommunen tänker genomföra en upphandling, ingå ett avtal eller inleda ett samarbete/samverkan som innebär att en annan aktör får tillgång till säkerhetsskyddsklassificerad information eller verksamhet ska ett säkerhetsskyddsavtal alternativt säkerhetsskyddsöverenskommelse tecknas med aktören.

Säkerhetsskyddsöverenskommelse räcker för information och verksamheter i säkerhetsskyddsklass begränsat hemlig, högre klass kräver säkerhetsskyddsavtal. Detta krav omfattar även eventuella underleverantörer.

Säkerhetsskyddschef ska alltid informeras om behov finns att ingå säkerhetsskyddsavtal alternativt överenskommelse. Att kommunen avser att ingå ett säkerhetsskyddsavtal ska anmälas till tillsynsmyndigheten. När avtal väl ingås och senare upphör ska det anmälas till Säkerhetspolisen och tillsynsmyndigheten.

Ett upprättat säkerhetsskyddsavtal alternativt överenskommelse ska bland annat redogöra för de krav som ställs på aktörens säkerhetsskydd samt hur kommunen ska kontrollera att aktören uppfyller kraven. Observera att ansvaret för säkerhetsskyddet ligger kvar hos kommunen även efter att ett säkerhetsskyddsavtal alternativt överenskommelse har tecknats.

Inför ett säkerhetsskyddsavtal ska kommunen i de flesta fall göra en särskild säkerhetsskyddsbedömning och utifrån resultatet av den göra en lämplighetsprövning, dvs analysera om det är lämpligt att en annan aktör får tillgång till den säkerhetsskyddsklassificerade informationen eller verksamheten. I vissa fall ska det även genomföras ett samråd med kommunens tillsynsmyndighet. De roller hos aktören som kommer ta del av den klassificerade informationen eller verksamheten ska säkerhetsprövas av kommunen.

8. Incidenthantering

Alla misstänkta säkerhetsincidenter rörande säkerhetsskyddsklassificerad information och verksamheter och andra misstänkta händelser som kan röra Sveriges skydd mot antagonistiska händelser ska omedelbart rapporteras till säkerhetsskyddschef. Om incidenten berör ett signalskyddssystem ska även signalskyddschef informeras. Mer information om hur incidenter ska hanteras, utredas och rapporteras finns i underliggande rutin till denna riktlinje.

9. Internkontroll

Kommunen ska årligen göra interkontroll av sin säkerhetsskydds- och signalskyddsverksamhet. Dessa genomförs av säkerhetsskyddschef respektive signalskyddschef i samverkan med relevant personal och dokumenteras i avsedd mall.

10. Tillsyn, viten och sanktionsavgift

Länsstyrelsen i Västra Götaland är tillsynsmyndighet för Herrljunga kommun både när det gäller signalskydd och säkerhetsskydd. Tillsynsmyndigheten kan besluta om förelägganden som kan förenas med vite. Om kommunen inte uppfyller vissa delar av säkerhetsskyddslagen har tillsynsmyndigheten dessutom rätt att besluta om en

sanktionsavgift. Summan beror bland annat på vilken skada som har/kunde ha uppstått men får max vara 10 miljoner kronor för en kommun.