Riktlinje

För signal- och säkerhetsskydd

Herrljunga kommun

Dokumentinformation

Diarienummer:	KS-2024-00438
Fastställd:	Kommunstyrelsen 2023-04-24 § 74
Senast reviderad:	Kommunstyrelsen 2023-04-24 § 74
Giltig till:	Tills vidare
Dokumentansvarig:	Säkerhetschef

Innehållsförteckning

Syfte
Syftet med riktlinjen är konkretisera säkerhetspolicyn avseende signal- och säkerhetsskydd och beskriva hur kommunen ska arbeta för att upprätta god säkerhet inom området med utgångspunkt från gällande lagar och vägledningar.

Till denna riktlinje finns framtagna rutiner som ger mer detaljerad information och som fastställs av kommundirektör, alternativt berörd förvaltning. Rutinerna omfattas i vissa fall av sekretess enligt offentlighets- och sekretesslagen (2009:400).

Riktlinjen är underställd kommunens säkerhetspolicy och gäller för alla verksamheter inom Herrljunga kommun, exklusive de kommunala bolagen. Riktlinjen fastställs av kommunstyrelsen.

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/förstörs.

Berörda lagar och andra regelverk
Följande regelverk utgör grunden för denna riktlinje:
- Säkerhetsskyddslag (2018:585)
- Säkerhetsskyddsförordning (2021:955)
- Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)
- Säkerhetspolisens vägledningar
- Överenskommelse om kommunernas arbete med civilt försvar (mellan SKL och MSB). SKL 18/01807.
- Försvarsmaktens föreskrifter om signalskyddstjänsten (FFS 2021:1)

Säkerhetsskydd
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 spionerі, sabotage och terroristbrott.

Ansvarsfördelning/ Säkerhetsskyddschef
Säkerhetschef är tillika säkerhetsskyddschef och är som sådan direkt underställd kommundirektören. Kommundirektören kan även utse en biträdande säkerhetsskyddschef. Säkerhetskyddschefen ska leda och samordna säkerhetsskyddsarbetet samt kontrollera att verksamheten bedrivs enligt berörd lag och föreskrifter. I övrigt gäller den ansvarsfördelning som framgår i säkerhetspolicyn.

Säkerhetsskyddsanalys och säkerhetskyddsplan
Kommunen ska minst vartannat år göra en säkerhetsskyddsanalys, i enlighet med säkerhetspolisens föreskrifter. Övergripande kan analysen sammanfattas till att den ska svara på tre frågor:
- Vad ska skyddas?
- Mot vad ska det skyddas?
- Hur ska det skyddas?

Förvaltningschefer, i nära samarbete med säkerhetsskyddschef, ansvarar för att analysen genomförs.
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 det analyseras vilka roller som kommer i kontakt med den säkerhetskänsliga informationen/verksamheten. De personer som innehar dessa roller ska säkerhetsprövas (undantagen politiker i kommunfullmäktige och kommunstyrelsen).

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 informationssäkerhetspolicyn samt grundregeln att varje person bara ska ha tillgång till de uppgifter/verksamheter som krävs för att hen ska kunna utföra sitt arbete.

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

För att säkerställa att obehöriga inte kommer över informationen ska utrymmen där säkerhetsskyddsklassificerade uppgifter hanteras insynsskyddas och elektronisk utrustning som kan möjliggöra obehörig avlyssning, tex mobiltelefoner, får inte finnas i närheten när säkerhetsskyddsklassificerade uppgifter diskuteras.

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

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.

Informationssystem

Den hård- och mjukvara som används vid elektronisk hanteringen av säkerhetsklassificerad information ska hålla en hög säkerhet i enlighet med säkerhetspolisens föreskrifter. Det innebär bland annat att system ska granskas för att hitta brister och sårbarheter, testas, ha unika användaridentiteter, spårbarhet över användandet, kommunicera på ett säkert sätt samt vara logiskt eller fysiskt separerat från andra informationssystem som inte håller samma säkerhetsnivå.

Fysisk säkerhet

För att säkerställa att endast behöriga personer får tillgång till säkerhetsklassificerad information/verksamhet ska berörda områden/byggnader/rum skyddas fysiskt. Det kan tex. handla om passersystem, larm och inbrottsskydd.

Personalsäkerhet

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

Säkerhetsklass

Utifrån hur säkerhetskänslig information/verksamhet som en roll 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 behöver inte placeras i säkerhetsklass och det görs då inte heller någon registerkontroll.

Säkerhetsprövning

Närmsta chef ansvarar för att säkerställa att person som ska inneha en roll som kräver säkerhetsprövning, prövas innan personen påbörjar anställning alternativt får tillgång till säkerhetsskyddsklassificerad information/verksamhet.

Gäller det en nyanställning ska det redan vid rekryteringen framgå för den sökande att tjänsten innebär 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.
- Säkerhetsprövningsintervju där lojalitet, pålitlighet och sårbarhet bedöms. Genomförs av säkerhetsskyddschef.
- Registerkontroll i bland annat belastnings- och misstankeregistret. Denna kontroll fortgår under hela den tid personen är säkerhetsklassad. För placering i säkerhetsklass 1 och 2 omfattar kontrollen även make/maka/sambo. Genomförs av Säkerhetspolisen.

- Särskild personutredning som bland annat innebär att personens ekonomiska förhållanden kontrolleras. Denna utredning sker bara vid placering i säkerhetsklass 1 och 2, då krävs det även 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 rollen.

Resultatet av säkerhetsprövningen delges berörd chef som beslutar om personen ska anställas alternativt att redan anställd ska ges tillgång till säkerhetsskyddsklassificerad information/ verksamhet eller inte.

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 Herrljunga kommun och Sverige. Framkommer sådana uppgifter ska säkerhetsskyddschefen omedelbart informeras. Närmsta chef ska dokumentera att uppföljningen har skett.

När säkerhetsklassad 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.

Säkerhetsskyddsavtal

Om kommunen tänker genomföra en upphandling, ingå ett avtal eller inleda ett samarbete som innebär att en annan aktör får tillgång till uppgifter i säkerhetsskyddsklass konfidentiell eller högre alternativt får tillgång till säkerhetskänslig verksamhet av samma betydelse för Sveriges säkerhet, ska ett säkerhetskyddsavtal (SUA) tecknas med aktören. Detta krav omfattar även eventuella underleverantörer.

Att kommunen avser att ingå en SUA ska anmälas till tillsynsmyndigheten och när ett avtal väl ingås alternativt upphör ska det också anmälas till Säkerhetspolisen. Kontakterna med myndigheterna ska ske via säkerhetsskyddschefen.

Inför en SUA ska kommunen 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 verksamheten/informationen. I vissa fall ska det även genomföras ett samråd med kommunens tillsynsmyndighet.

En upprättad SUA ska bland annat redogöra för de krav som ställs på aktörens säkerhetsskydd samt hur kommunen ska kontrollera att aktören uppfyller kraven. SUA samt säkerhetsprövning av berörda personer måste vara på plats innan aktören får tillgång till den säkerhetskänsliga verksamheten/uppgifterna.

Säkerhetsskyddsincident

Om det sker en säkerhetsskyddsincident ska omständigheterna kring händelsen utredas, göras en skadebedömning och nödvändiga åtgärder ska vidtas.

En incident ska anmälas till Säkerhetspolisen, via säkerhetsskyddschef, i följande fall:

- om en säkerhetsskyddsklassificerad uppgift kan ha röjts,
- det inträffar en IT-incident i ett informationssystem som verksamheten är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet eller
- verksamheten får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.

Sanktionsavgift

Om kommunen inte uppfyller berörda delar av Säkerhetsskyddslagen har tillsynsmyndigheten 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.

Signalskydd

Ett sätt att skydda säkerhetsskyddsklassificerad information är att kryptera den. Sådana kryptografiska funktioner som har godkänts av Försvarsmakten kallas för signalskydd. Kommunen har genom Länsstyrelsen tillgång till signalskydd i form av en kryptodator som är godkänd att hantera information i säkerhetsskyddsklass begränsad hemlig.

Signalskyddsorganisation

I signalskyddsorganisationen finns olika ansvarsroller enligt nedan, en person kan inneha mer än en roll. Alla som ingår i organisationen måste minst vara placerade i säkerhetsklass 3 och ha fått utbildning om signalskydd.

Signalskyddschef

Signalskyddschefen ansvarar för att leda och samordna signalskyddet. Då det är svårt att upprätthålla den krävda utbildningsnivån för en signalskyddschef inom kommunen eftersträvar Herrljunga kommun att genom överenskommelse överlåta rollen till annan lämplig aktör, såsom Länsstyrelsen.

Biträdande signalskyddschef

Om en extern aktör har tilldelats rollen som signalskyddschef ska kommundirektören utse minst en biträdande signalskyddschef inom kommunen som ansvarar för ledning och samordning lokalt utifrån signalskyddschefens direktiv.

Systemoperatör/lokal administratör

Ansvarar för att skapa användarkonton, genomföra uppdateringar, exportera loggfiler m.m.

Nyckeladministratör
Har huvudansvaret för kommunens signalskyddsnycklar.

Hantering
Kryptodator, signalskyddsnycklar m.m. ska hanteras så att ingen obehörig får del av dem. Det ställer krav på säker förvaring, spårbarhet, säker förstöring m.m. Mer detaljerad information kring säkerhetsbestämmelserna finns i underliggande rutin till denna riktlinje.

Signalskyddsincident
Signalskyddsincidenter ska omedelbart anmälas till signalskyddschef, via biträdande signalskyddschef, samt säkerhetsskyddschef. En incident kan till exempel vara att en signalskyddsnyckel har/misstänks ha blivit röjd, plomberingar har brutits eller säkerhetsskåp lämnats öppna. Misstänker man att det har skett åverkan/manipulation ska berörd utrustning omedelbart tas ur drift.

Mer information om hur incidenter ska hanteras finns i underliggande rutin till denna riktlinje.