Region Stockholm

Diarienummer
RS 2021-0106

Riktlinjer

Säkerhetsskydd och signalskydd

Gäller för Region Stockholm

Dokumenttyp	Fastställd	Giltig till och med
Dokumentnummer	Fastställd av	Upprättad av
Informationssäkerhetsklass		

Innehållsförteckning

1. Inledning 3
1.1 Syfte och omfattning....3
1.2 Region Stockholms styrande dokument för säkerhetsskydd och signalskydd 3

2. Organisation av säkerhetsskyddet....3
2.1 Roller och ansvar 3
2.1.1 Regionfullmäktige 3
2.1.2 Regionstyrelsen 3
2.1.3 Regiondirektören.... 4
2.1.4 Förvaltningschef och vd 4
2.1.5 Säkerhetskyddschefen 4
2.1.6 Säkerhetsskyddsamordnare 4
2.1.7 Signalskyddschef 5
2.1.8 Upphandlande enheter eller funktioner....5

3. Medarbetare och säkerhetsskydd....5
3.1 Rekrytering och anställning 5
3.1.1 Sekretess/tystnadsplikt 6
3.2 Utbildning.... 6
3.3 Avslutande av anställning 6
3.4 Uppföljning....7
3.4.1 Rapportering 7

4. Särskilda krav på skyddsåtgärder....7
4.1 Säkerhetsskydd....7
4.1.1 Säkerhetsskyddsanalys.... 8
4.1.2 Behörig att delta i säkerhetskänslig verksamhet.... 8
4.1.3 Säkerhetsskyddsavtal 8
4.1.4 Anmälan vid säkerhetshotande händelse.... 9
4.2 Signalskydd.... 9
4.2.1 Signalskyddsinstruktion....10

1. Inledning

1.1 Syfte och omfattning

Dessa riktlinjer konkretiserar Region Stockholms verksamhetsskyddspolicy, RS 2020-0147, och är styrande för arbetet med säkerhetsskydd och signalskydd vid Region Stockholms samtliga nämnder och bolag.

Riktlinjerna ska även följas inom ramen för program och projekt som bedrivs i Region Stockholms regi.

1.2 Region Stockholms styrande dokument för säkerhetsskydd och signalskydd

Varje nämnd och bolag ska, inom ramen för Region Stockholms riktlinjer för säkerhetsskydd och signalskydd samt säkerhetsskyddschefens instruktioner och beslut, ansvara för arbetet inom sitt verksamhetsområde. De lagar, förordningar och andra föreskrifter som är tillämpliga, ska följas. Hit hör bland annat säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2018:658), Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2) och lagen (1992:1403) om totalförsvar och höjd beredskap.

Styrdokumenten på regionövergripande nivå består av Region Stockholms verksamhetsskyddspolicy med tillhörande riktlinjer för säkerhetsskydd och signalskydd.

2. Organisation av säkerhetsskyddet

För att styra arbetet med säkerhetsskydd och signalskydd inom nämnder och bolag i Region Stockholm är det viktigt att roller och ansvar fördelas. Föreliggande riktlinjer är obligatoriska och ska efterlevas av samtliga nämnder och bolag inom Region Stockholm.

2.1 Roller och ansvar

2.1.1 Regionfullmäktige

Regionfullmäktige fastställer den verksamhetsskyddspolicy som gäller för samtliga nämnder och bolag samt riktlinjer för säkerhetsskydd och signalskydd.

2.1.2 Regionstyrelsen

Regionstyrelsen ansvarar för att ta fram förslag till riktlinjer för säkerhetsskydd och signalskydd och att dessa revideras vid behov.

2.1.3 Regiondirektören

Regiondirektören är chef för den verksamhet som Region Stockholms nämnder med tillhörande förvaltningar utför vad gäller säkerhetsskydd. I detta ligger bland annat att ta framkompletterande anvisningar som förtydligar hur det praktiska arbetet med att följa riktlinjerna ska gå till.

2.1.4 Förvaltningschef och vd

Förvaltningschefen eller vd ansvarar inför nämnden eller styrelsen för arbetet med säkerhetsskydd och signalskydd samt att föreliggande riktlinjer följs.

Vd vid de av Region Stockholm helägda aktiebolagen är chef för verksamhetsutövarens verksamhet vad gäller säkerhetsskydd.

2.1.5 Säkerhetskyddschefen

Regiondirektören ska utse en säkerhetsskyddschef som leder, samordnar och utövar kontrollen av säkerhetsskyddet för Region Stockholms nämnder. Säkerhetsskyddschefen ska, i säkerhetsskyddsfrågor, vara direkt underställd regiondirektören.

Bolag ska utse en säkerhetsskyddschef som leder, samordnar och utövar kontrollen över säkerhetsskyddet i det egna bolaget, givet att verksamhetsutövaren i sin säkerhetsskyddsanalys har bedömt att det behöver finnas en säkerhetsskyddschef. Säkerhetsskyddschefen ska, i säkerhetsskyddsfrågor, vara direkt underställd vd.

Säkerhetsskyddschefen ansvarar för att säkerhetsskyddet är väl anpassat till verksamhetens behov samt för att kontrollera att verksamheten bedrivs i enlighet med säkerhetsskyddslagen, säkerhetsskyddsförordningen samt myndighets- och verkställighetsföreskrifter. Säkerhetsskyddschefens ansvar att leda och samordna säkerhetsskyddsarbetet samt utöva kontrollen över att verksamheten bedrivs enligt lagen och de föreskrifter som har meddelats i anslutning till lagen får inte delegeras.

Säkerhetsskyddschefer vid bolag ska anmälas till Region Stockholms säkerhetskyddschef.

2.1.6 Säkerhetsskyddsamordnare

Varje förvaltningschef ska i samråd med säkerhetskyddschefen utse en säkerhetskyddsamordnare som har i uppgift att samordna och följa upp arbetet med säkerhetsskydd inom den egna förvaltningen och rapportera till säkerhetskyddschefen enligt dennes instruktion.

Säkerhetsskyddssamordnare ska anmälas till säkerhetskyddschefen.

2.1.7 Signalskyddschef

Om nämnd eller bolag innehar signalskyddssystem, utser förvaltningschef eller vd en signalskyddschef vilken har till uppgift att ansvara för ledning och samordning av signalskyddstjänsten.

Om nämnd eller bolag bedömer att det finns särskilda skäl kan signalskyddschef vid regionledningskontoret utses till signalskyddschef hos en enskild nämnd eller bolag. Beslutet ska dokumenteras. Om sådant beslut fattas ska berörd nämnd och bolag utse biträdande signalskyddschef.[1]

2.1.8 Upphandlande enheter eller funktioner

I de fall Region Stockholms verksamhet utförs av privata, eller andra för regionen utomstående aktörer, ska upphandlande enhet säkerställa att leverantören följer Region Stockholms riktlinjer för säkerhetsskydd och signalskydd i tillämpliga delar. Detta gäller om utomstående aktör kommer att delta i säkerhetskänslig verksamhet eller få kännedom om säkerhetskyddsklassificerade uppgifter. . Detta ska regleras i avtal samt gå att följa upp av avtalsansvarig.

Upphandlade aktörer som ingått säkerhetsskyddsavtal med Region Stockholm ska följa de krav som ställs i aktuellt avtal, se vidare avsnitt 4.1.3 om säkerhetsskyddsavtal.

3. Medarbetare och säkerhetsskydd

Anställda eller individer som på annat sätt deltar i Region Stockholms verksamhet ska förstå sitt ansvar för och bidra till att upprätthålla verksamhetens säkerhetsskydd.

3.1 Rekrytering och anställning

Innan anställning eller annat deltagande i verksamheten som har betydelse för Sveriges säkerhet ska individens lämplighet prövas genom så kallad säkerhetsprövning. I förekommande fall ska individen inplaceras i säkerhetsklass. Beslut om inplacering i säkerhetsklass 2 och 3 för såväl Region Stockholms nämnder som för dess helägda bolag fattas av Region Stockholms säkerhetsskyddschef.[2] Region Stockholms säkerhetsskyddschef beslutar också om placering i säkerhetsklass 2 och 3 i fråga om anställning eller uppdrag hos en leverantör som Region Stockholm har ingått ett

[1] 1 kap. 8 § FFS 2021:1

[2] 5 kap. 7-8 §§ säkerhetsskyddsförordningen
Regioner beslutar även om placering i säkerhetsklass 2 och 3 i fråga om anställning eller annat deltagande hos enskilda verksamhetsutövare som de utövar ett rättsligt bestämmande inflytande över enligt 2 kap. 3 § offentlighets- och sekretesslagen (2009:400). Förordning (2019:1179).

säkerhetsskyddsavtal med. Regeringen fattar beslut om placering i säkerhetsklass 1.

Efter godkänd säkerhetsprövning samt eventuell inplacering i säkerhetsklass kan anställning eller annat deltagande i säkerhetskänslig verksamhet påbörjas.

Säkerhetsprövning får också göras under pågående anställning eller annat pågående deltagande i verksamheten om tjänsten bedöms beröras av säkerhetsskyddslagen.

Säkerhetsprövning ska fortlöpande följas upp av närmsta chef så länge anställning eller annat deltagande i säkerhetskänslig verksamhet pågår. Närmsta chef ska samråda med Region Stockholms säkerhetskyddschef vid osäkerhet om förfarandet för sådan uppföljning.

3.1.1 Sekretess/tystnadsplikt

Tystnadsplikt för anställda inom Region Stockholm och dess helägda bolag regleras enligt bestämmelserna i offentlighets- och sekretesslagen (2009:400).

En verksamhetsutövare ska upplysa den som tillåts ta del av säkerhetsskyddsklassificerade uppgifter om räckvidden och innebörden av den sekretess och tystnadsplikt som följer av offentlighets- och sekretesslagen (2009:400) respektive 5 kap. 1-2 §§ säkerhetsskyddslagen.

3.2 Utbildning

Nämnder och bolag ansvarar för att anställda får den utbildning som krävs för att de ska kunna tillämpa de regler som finns i föreliggande riktlinjer.

Nämnd eller bolag som bedriver säkerhetskänslig verksamhet ska säkerställa att den som anställs eller på annat sätt deltar i verksamheten får en relevant utbildning i säkerhetsskydd innan personen får åtkomst till verksamheten.

Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Utbildning ska ske fortlöpande.

Utbildning ska dokumenteras på individnivå.

3.3 Avslutande av anställning

Nämnder och bolag ska i rutin för avslut av anställning eller uppdrag säkerställa att berörd individ är medveten om tystnadsplikt även efter avslutad anställning.

Avslutande säkerhetsprövningssamtal ska hållas om detta ej är uppenbart obehövligt.

När person avslutar sitt deltagande i säkerhetskänslig verksamhet vid nämnd eller bolag ska detta skyndsamt meddelas till Region Stockholms säkerhetsskyddschef för vidare avanmälan om registerkontroll vid Säkerhetspolisen.

3.4 Uppföljning

Uppföljning av dessa riktlinjers efterlevnad ska ske enligt regionens ledningsprocess, vilket i huvudsak innebär att den ska följas upp på samma sätt och samtidigt som regionens övriga styrande dokument.

Anpassningar av Region Stockholms riktlinjer för säkerhetsskydd och signalskydd ska ske utifrån förändringar i lagar och föreskrifter, uppdateringar av rekommendationer på området, resultat från analyser av sårbarheter och hotbild samt förändringar i verksamhet.

3.4.1 Rapportering

Nämnder ska utan dröjsmål anmäla händelse eller omständighet som bedöms vara av betydelse för den säkerhetskänsliga verksamheten som till Region Stockholms säkerhetsskyddschef enligt dennes instruktion.

Bolag ska utan dröjsmål anmäla händelse eller omständighet som bedöms vara av väsentlig betydelse för den säkerhetskänsliga verksamheten till Region Stockholms säkerhetsskyddschef enligt dennes instruktion.

4. Särskilda krav på skyddsåtgärder

4.1 Säkerhetsskydd

För att avgöra om det finns behov av ett säkerhetsskydd ska en verksamhetsbeskrivning genomföras av respektive nämnd och bolag. Om bolag eller nämnd med tillhörande förvaltning i sin verksamhetsbeskrivning kommer fram till att verksamheten berörs av säkerhetsskydd ska skyddsbehovet identifieras i en säkerhetsskyddsanalys med tillhörande säkerhetsskyddsplan. Säkerhetsskyddsanalysen och säkerhetsskyddplanen ska efter utlämnandeprövning normalt delges till Region Stockholms säkerhetsskyddschef. De bolag eller nämnd med tillhörande förvaltning som inte berörs av säkerhetsskydd ska anmäla detta till Region Stockholms säkerhetsskyddschef.

Bolag som bedriver säkerhetskänslig verksamhet ska utan dröjsmål anmäla detta till Länsstyrelsen. På samma sätt ska Region Stockholm utan dröjsmål göra en anmälan till Säkerhetspolisen.

4.1.1 Säkerhetsskyddsanalys

Säkerhetsskyddsanalysen innebär att säkerhetsskyddsklassificerade uppgifter och vad som i övrigt behöver ett säkerhetsskydd identifieras. Vilka delar av verksamheten som är skyddsvärda med hänsyn till Sveriges säkerhet samt vilka hot och sårbarheter som finns kopplade till skyddsvärdet ska också identifieras. Säkerhetsskyddsanalysen ska även innehålla en bedömning av vilka säkerhetsskyddsåtgärder som är nödvändiga (se vidare anvisning för säkerhetsskydd och avsnitten informationssäkerhet, fysisk säkerhet och personalsäkerhet). Dessa ska sedan på ett mer detaljerat sätt redovisas i en säkerhetsskyddsplan.

Nämnder och bolag ska även i bidra med underlag till den koncerngemensamma säkerhetsskyddsanalysen enligt instruktion från Region Stockholms säkerhetsskyddschef.

Säkerhetsskyddsanalys och -plan ska uppdateras vid behov och minst en gång vartannat år.[3]

4.1.2 Behörig att delta i säkerhetskänslig verksamhet

För att ta del av säkerhetsskyddsklassificerade handlingar eller annars delta i säkerhetskänslig verksamhet vid Region Stockholm måste berörd individ vara i behov av uppgiften för att kunna utföra en viss arbetsuppgift. Berörd måste dessutom ha tillräckliga kunskaper i säkerhetsskydd samt ha genomgått säkerhetsprövning.

4.1.3 Säkerhetsskyddsavtal

Inför och vid upphandling, ingående av avtal eller inledande av samverkan eller ett samarbete ska säkerhetsskyddsavtal ingås om det i avtalet ingår säkerhetsskyddsklassificerade handlingar i klassen konfidentiellt eller högre eller om det i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Innan ett förfarande som kräver säkerhetsskyddsavtal enligt ovan påbörjas ska en särskild säkerhetskyddsbedömning genomföras. Med utgångspunkt i säkerhetskyddsbedömningen ska även lämpligheten av det planerade förfarandet prövas.

[3] 2 kap. 10 § PMFS

Innan det planerade förfarandet inleds ska samråd med tillsynsmyndigheten ske om förfarandet innebär att:

1. den andra aktören kan få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller högre, eller
2. annan säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Regionens bolag ska utan dröjsmål anmäla avsikt att ingå säkerhetsskyddsavtal till Länsstyrelsen.[4] Region Stockholms nämnder ska, när säkerhetsskyddsavtal ingåtts med leverantör, göra en anmälan till Säkerhetspolisen.[5]

4.1.4 Anmälan vid säkerhetshotande händelse

Säkerhetsskyddschefen ska utan dröjsmål informeras om verksamheten misstänker något av följande;

1. att en säkerhetsskyddsklassificerad uppgift kan ha röjts
2. att en IT-incident har inträffat i ett informationssystem som bolag eller nämnd är ansvarig för som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet
3. eller fått kännedom om någon annan för denne allvarlig säkerhetshotande verksamhet

Säkerhetsskyddschef ska därefter skyndsamt informera Säkerhetspolisen. Säkerhetskyddschefer vid Region Stockholms bolag ska även skyndsamt informera Region Stockholms säkerhetskyddschef.

4.2 Signalskydd

Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem som finns utom Region Stockholms kontroll ska uppgifterna skyddas med hjälp av kryptografiska funktioner som godkänts av Försvarsmakten.[6]

Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras inom Region Stockholm ska detta ske enligt instruktion från Region Stockholm säkerhetsskyddschef .

[4] 2 kap. 5 § Säkerhetsskyddförordningen (2018:658)
[5] 2 kap. 7 § Säkerhetsskyddförordningen (2018:658)
[6] 3 kap. 5 § 2 st. Säkerhetsskyddsförordningen (2018:658)

4.2.1 Signalskyddsinstruktion

Nämnd och bolag som har ett signalskyddssystem med kryptografiska funktioner ska ha en signalskyddsinstruktion.[7] Signalskyddsinstruktion ska minst innehålla uppgift om;

1. En verksamhetsutövares eller enhets signalskyddsorganisation.
2. Åtgärder som ska vidtas vid krishantering, höjd beredskap och signalskyddsincident.
3. Rutiner för beställning, mottagning, extern och intern distribution, delgivning, kvittens, förvaring, inventering och förstöring av signalskyddsnycklar samt, i förekommande fall, lokal produktion av signalskyddsnycklar.
4. Rutiner för beställning, mottagning, extern och intern försändning, utlämning, kvittens, förvaring, inventering, reparation och återlämning av signalskyddsmateriel.
5. Rutiner för beställning, mottagning, extern och intern försändning, utlämning, förvaring och återsändning av aktiva kort och mjuka certifikat.

För mer stöd se avsnitt 3.4 i Försvarsmaktens handbok för signalskyddstjänst[8].

Signalskyddsincident:

1. När en signalskyddsnyckel saknas eller har, eller kan antas ha, kommit till obehörigs kännedom (nyckelincident).
2. När signalskyddsmateriel saknas eller kan antas ha manipulerats eller utsatts för annan åverkan (materielincident).
3. När ett aktivt kort eller lagringsmedium för mjukt certifikat saknas, kan antas ha manipulerats eller att obehörig kan antas ha haft tillgång till kortet eller det mjuka certifikatet (incident med aktivt kort eller certifikat).

[7] 1 kap. 12 § FFS 2021:1
[8] Handbok totalförsvarets signalskyddstjänst – grundläggande regler för signalskyddstjänst. 2007.

Definitioner

För användningen av dessa riktlinjer gäller följande termer och definitioner:

Signalskydd	Åtgärd som syftar till att förhindra obehörig insyn i och påverkan av telekommunikations- och IT-system med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder.
Signalskyddschef	Funktion inom signalskyddsorganisation som har till uppgift att ansvara för ledning och samordning av signalskyddstjänsten.
Säkerhetsprövning	Klarläggning om personen som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet kan antas vara lojal med de intressen som ska skyddas och i övrigt pålitlig ur säkerhetssynpunkt.
Säkerhetsskydd	Skydd av säkerhetskänslig verksamhet mot spioneri, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.
Säkerhetsskyddsanalys	Analys som utreder behovet av säkerhetsskydd.
Säkerhetsskyddsavtal	Avtal som anger hur kravet på säkerhetsskydd ska tillgodoses om det i upphandling, avtal, samverkan eller samarbete om förfarandet kan ge aktör tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiellt eller högre eller annan säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet
Säkerhetsskyddschef	Funktion inom säkerhetsskyddsorganisationen som ska leda och samordna säkerhetsskyddsarbetet samt kontrollera att verksamheten bedrivs enligt säkerhetsskyddslagen, säkerhetsskyddsförordningen och de föreskrifter som har meddelats i anslutning till lagen.
Säkerhetsklass	Inplacering i säkerhetsklass 1-3 av anställd eller annan som deltar i säkerhetskänslig verksamhet utifrån den omfattning berörd får ta del av säkerhetsskyddsklassificerade uppgifter eller har möjlighet att orsaka skada för Sveriges säkerhet.

Säkerhetsskydds-klassificerad uppgift	Uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.
Säkerhetsskyddsplan	Plan över vilka säkerhetsskyddsåtgärder som behöver vidtas inom områdena fysisk säkerhet, informationssäkerhet och personalsäkerhet för att säkerställa att skyddsvärden som identifierats i säkerhetsskyddsanalys tas tillvara.
Säkerhetskänslig verksamhet	Verksamhet som är av betydelse för Sveriges säkerhet eller som Sverige har förbundit sig att skydda genom internationella åtaganden.

Bilaga - Verksamhetsutövare

Region Stockholm, som juridisk person, är verksamhetsutövare i säkerhetsskyddslagens och -förordningens mening för den verksamhet dess nämnder med tillhörande förvaltningar utför.

Region Stockholms bolag är, i egenskap av juridiska personer, var för sig verksamhetsutövare för den verksamhet som de bedriver.

Regiondirektören respektive VD är den chef för verksamhetsutövarens verksamhet som säkerhetsskyddschefen ska vara direkt underställd.

Verksamhetsutövare: Region Stockholm	**Verksamhetsutövare: enskilda bolag**
Regionstyrelsen	AB Storstockholms Lokaltrafik, SL
Hälso- och sjukvårdsnämnden	AB Stockholms Läns Landstings Internfinans
Trafiknämnden	Ambulanssjukvården i Storstockholm AB, AISAB
Kulturnämnden	Danderyds Sjukhus AB
Patientnämnden	Folktandvården Stockholms Län AB
Revisorskollegiet	Landstingshuset i Stockholm AB
Fastighets- och servicenämnden	Locum AB
Karolinska Universitetssjukhuset	MediCarrier AB
Stockholms läns sjukvårdsområde, SLSO	S:t Eriks Ögonsjukhus AB
Tillväxt- och regionplanenämnden	Stockholm Care AB
Klimat- miljö- och hållbarhetsnämnden	Södersjukhuset AB
Färdtjänstnämnden	Södertälje Sjukhus AB
Vårdens kunskapsstyrningsnämnd	TioHundra AB
	Waxholms Ångfartygs AB, WÅAB