2025-08-27 – ÄRENDE 09

BESLUT

Diarienr
LOC 2025-1807
Informationssäkerhetsklass: K1

Styrelsen för Locum AB

Yttrande över Riktlinje för informationssäkerhet och dataskydd

Ärendet

Regionstyrelsen, rotel I har remitterat förslag till Riktlinje för informationssäkerhet samt dataskydd, RS 2025-0418. Locum har beretts möjlighet att yttra sig över förslaget.

Beslutsunderlag

1. Remissbrev 2025-05-30
2. PM 2025-05-30
3. Riktlinje för informationssäkerhet samt dataskydd
4. Ändringsbilaga 2025-04-14

Förslag till beslut

Styrelsen för Locum AB föreslås besluta

att uppdra åt verkställande direktör att avge yttrande över förslag till Riktlinje för informationssäkerhet och dataskydd (RS 2025-0418) enligt förslag.

Victoria Hörnedal
Verkställande direktör

YTTRANDE

Diarienr
LOC 2025-1807
Informationssäkerhetsklass: K1

Styrelsen för Locum AB

Yttrande över Riktlinje för informationssäkerhet och dataskydd

Ärendet

Regionstyrelsen, rotel I har remitterat förslag till Riktlinje för informationssäkerhet samt dataskydd, RS 2025-0418. Locum har beretts möjlighet att yttra sig över förslaget.

Sammanfattning

Ny lagstiftning genom EU:s direktiv om åtgärder för en hög gemensam säkerhetsnivå i hela unionen i kombination med regeringens utredning om implementation i svensk lag där regionen i egenskap av juridisk person ses som verksamhetsutövare, föranleder en översyn av regionens styrande dokument inom informationssäkerhet och dataskydd.

Locum ställer sig positiv till förändringarna som föreslås. Verksamheten föreslår ett kort tillägg till riktlinjen rörande Operational Technology (OT) samt efterlyser en samlad vägledning till alla regionens styrdokument som berör information och hur de förhåller sig till varandra, för ökad tydlighet för regionens verksamheter.

Därutöver föreslås några smärre språkliga/innehållsmässiga förändringar i formuleringar som redovisas i punktnotationsordning.

Bakgrund

Den 18 oktober 2024 trädde EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) i kraft. NIS2-direktivet ställer krav på åtgärder för att undanröja hinder som påverkar cyberresiliensen och minska sårbarheten för cyberhot. Regeringen tillsatte en utredning kring Sveriges implementering av NIS2-direktivet. Ett delbetänkande överlämnades till regeringen den 5 mars 2024 som föreslår att direktivet implementeras i en ny lag som ska kallas lag om cybersäkerhet. En proposition är planerad till i maj i år. Enligt skrivningar i utredningen (s. 135-136) ska regionen i egenskap av juridisk person ses som verksamhetsutövare enligt denna lag och inte enskilda nämnder.

Regionfullmäktige har också i samband med budget 2025 beslutat inrätta ett antal gemensamma tjänster. Tillsammans med förändringar i policy för styrning och ledning samt att ha en ”*effektiv och samordnad organisation som ser till helheten*” samt en ”*systematisk ledningsprocess*” gör att regionledningskontoret ser behov av att se över Riktlinjer för informationssäkerhet.

Förslaget baseras på ISO 27000-serien.

YTTRANDE

Diarienr
LOC 2025-1807
Informationssäkerhetsklass: K1

Styrelsen för Locum AB

Överväganden

Locum ställer sig positiv till förändringarna som föreslås. Locum föreslår ett kort tillägg till riktlinjen och efterlyser en samlad vägledning till samtliga regionens styrdokument som berör information och hur de förhåller sig till varandra.

Därutöver föreslås några smärre språkliga/innehållsmässiga förändringar i formuleringar som redovisas i punktnotationsordning.

Förslag på tillägg: Operational Technology (OT)
Locum ansvarar för förvaltningen av regionens vårdfastigheter och ska säkerställa driftsäkerheten för dessa. Operational Technology (OT), det vill säga hårdvara och mjukvara som används för att övervaka och styra tekniska system som ventilation, kyla, el, larm, passagesystem med mera är en central del av driften. Dessa system är avgörande för att vårdverksamheten ska fungera säkert och utan avbrott (tillgänglighetsaspekten).

Det danska Datatilsynet har under senare tid sett ett antal intrång relaterade till IoT (Internet of Things), där till exempel programvara i övervakningskameror inte verkar ha hanterats med samma uppmärksamhet på IT-säkerhet som annan IT-utrustning, trots att denna utrustning kan ge en enkel åtkomstväg till det interna nätverket.

Eftersom hackning av programvara i OT och IoT kan leda till åtkomst till andra delar av interna nätverk som innehåller information är det viktigt att riktlinjen även omfattar och uppmärksammar OT som ett prioriterat område inom informationssäkerhet och dataskydd.

En helhetssyn på informationstillgångar
Information omfattas av ett flertal regleringar på olika områden. Den stundande implementeringen i Region Stockholm av ett systemstöd (Iris) som ska kunna hantera dessa olika områden är ett steg mot en helhetssyn på information under hela dess livscykel. De områden som ska inkluderas är delar av arkivredovisningen, informationssäkerhet och dataskydd.

Regionarkivet är den verksamhet som utfärdar anvisningar rörande information i regionen, till exempel vad gäller kravställning på IT-system eller gallring och bevarande. Identifiering av informationsmängder och handlingstyper faller ofta inom deras professionella ramar och deras tillsynsansvar. Då identifiering och värdering av informationsmängder ligger till grund för skyddsåtgärder, samt att verkställd gallring faktiskt kan utgöra en sådan åtgärd, anser Locum att informationsmängderna bör ägnas mer uppmärksamhet i den föreslagna riktlinjen för informationssäkerhet. Alternativt att hänvisningar till andra styrande dokument rörande information infogas. Risk för såväl överskydd som underskydd av information kan annars bli följden, med både ekonomiska och säkerhetsmässiga konsekvenser.

För att få till stånd en effektiv, samordnad och säker hantering av information i Region Stockholm ser Locum, att en sammanhållen vägledning mellan regionens olika

styrdokument som berör information, informationsmängder och informationstillgångar inklusive personuppgifter, är önskvärd.

Synpunkter på förändringar
Önskade tillägg visas med understrykning.

1.3 Styrning
”Ansvaret för informationssäkerhet samt dataskydd är kopplat till verksamhetsansvaret i alla led. Det betyder att varje nämnd eller bolag och varje medarbetare som är ansvarig för en verksamhet också har att ansvara för informationssäkerheten och personuppgiftsbehandlingarna i denna verksamhet.”

4.3 ”Utbildning och fortbildning i Informationssäkerhet och dataskydd”

6.2 Åtkomstkontroll till informationstillgångar
”Behörighet till informationstillgångar ska baseras på användarens aktuella arbetsuppgifter och/eller organisatoriska tillhörighet för att endast ge åtkomst till de informationstillgångar som behövs för att lösa arbetet.”

9.3 Systemdokumentation
”Ägaren av it-system ska säkerställa att användarna får kunskap om vilken typ av information och vilka format som får hanteras i ett it-system och eventuella regler kring denna hantering.”

9.7 Styrning av ändringar i it-system
”Det ska finnas tillämpade rutiner för ändringshantering och testning av it-system.”

12.1 Kravställning
”Innan anskaffning ska analys ske av vilka krav avseende informationssäkerhet, dataskydd, arkivering och gallring som ska ställas.”

Miljömässiga konsekvenser

Beslutet medför oförändrade miljömässiga konsekvenser.

Ekonomiska konsekvenser

Införandet av en roll som dataskyddssamordnare, med den kompetens som erfordras för de ansvarsområden och de arbetsuppgifter som ska utföras enligt den föreslagna riktlinjen, innebär närmast en heltidstjänst. Locum ser svårigheter att kombinera detta med en roll som informationssäkerhetssamordnare, såväl på grund av förväntad arbetsbörda som de skilda kompetenser som behövs för respektive roll.

Dataskyddssamordnarens arbete kommer också att involvera andra delar av verksamheten, som kommer behöva omfördela tid till detta.

YTTRANDE

Diarienr
LOC 2025-1807
Informationssäkerhetsklass: K1

Styrelsen för Locum AB

Victoria Hörnedal
Verkställande direktör

Regionstyrelsen
Rotel I

REMISS
2025-05-30

Diarienummer
RS 2025-0418

Enligt sändlista

Riktlinje för informationssäkerhet samt dataskydd

Rotel I remitterar för yttrande bilagt förslag till Riktlinje för informationssäkerhet samt dataskydd.

I remissen ligger att roteln vill ha remissinstansernas synpunkter på förslaget. I remissvaren bör framgå vilka eventuella ekonomiska konsekvenser som det förslaget kan komma att medföra för verksamheten och varför.

Remissen är ett led i beredningen av ett ärende avsett att beslutas vid regionfullmäktiges sammanträde den 9 december 2025.
Mer information om förslaget finns i bilagd promemoria från regionledningskontoret daterad den 2025-05-05.

Remisstiden sträcker sig till den 29 augusti 2025.
Yttranden ska skickas till regionledningskontorets registrator, e-post: registrator.rlk@regionstockholm.se. Ange diarienummer RS 2025-0418

Frågor kring remissen skickas i första hand till funktionsbrevlådan: informationssakerhet@regionstockholm.se
Det går även bra att ta kontakt med ansvarig handläggare vid enheten informationssäkerhet:
Henrik Brodin, henrik.brodin@regionstockholm.se, 08-123 177 95

Rozgar Watmani
Kanslichef

REMISS
2025-05-30

Diarienummer
RS 2025-0418

Sändlista

Samtliga nämnder och helägda bolag i Region Stockholm
Regionrevisorerna

Regionledningskontoret
Henrik Brodin

PM
2025-05-05

Diarienummer
RS 2025-0418

Riktlinje för informationssäkerhet samt dataskydd

Förslag

Regionledningskontoret föreslår att regionstyrelsen föreslår att regionfullmäktige, vid sitt sammanträde den 9 december, fastställer Riktlinje för informationssäkerhet (RS 2025-0418). Som en följd av detta föreslås nu gällande Riktlinjer för informationssäkerhet (RS 2020-0148) upphöra att gälla från och med den 1 januari 2026.

Bakgrund

Regionledningskontoret ser behov av att se över Riktlinjer för informationssäkerhet. Översynen ska göra att arbetet med informationssäkerhet förändras för att skapa bättre förutsättningar för den juridiska personen Region Stockholm att få en bättre överblick över de nätverks- och informationssystem som användas samt de risker som är förknippade med dessa.

Regionfullmäktige har i samband med budget för 2025 beslutat att inrätta ett antal gemensamma tjänster. Dessutom innehåller budgeten initiativ som ska skapa bättre förutsättningar för Region Stockholm att fungera som en arbetsgivare.

Den 18 oktober 2024 trädde EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) i kraft. NIS2-direktivet ställer krav på åtgärder för att undanröja hinder som påverkar cyberresiliensen och minska sårbarheten för cyberhot. Regeringen tillsatte en utredning kring Sveriges implementering av NIS2-direktivet. Ett delbetänkande överlämnades till regeringen den 5 mars 2024[1] som föreslår att direktivet implementeras i en ny lag som ska kallas lag om cybersäkerhet. En proposition är planerad till i maj i år. Enligt skrivningar i utredningen (s. 135-136) ska regionen i egenskap av juridisk person ses som verksamhetsutövare enligt denna lag och inte enskilda nämnder.

Dessa förändringar samt inriktningarna i policy för styrning och ledning att ha en ”effektiv och samordnad organisation som ser till helheten” samt en

[1] https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2024/03/sou-202418/

”systematisk ledningsprocess” gör att regionledningskontoret ser behov av att se över Riktlinjer för informationssäkerhet.

Sammanfattning av föreslagna förändringar
För att åstadkomma bättre kontroll av den juridiska personen Region Stockholm föreslås ett antal koncerngemensamma processer som ska implementeras i det nya systemstöd för hantering av informationstillgångar som är under implementation[2]. Processerna rör förteckning, riskhantering, kontroll av regelefterlevnad samt hantering och rapportering av incidenter. I och med införandet av gemensam process för hantering av incidenter tas bestämmelse incidentrapportering bort och arbetas in i processen. Dessutom föreslås att kravet tas bort på att nämnder och bolag att ha en lokal handlingsplan och ersätts av att en strategisk inriktning ska upprättas för Region Stockholms arbete med informationssäkerhet. I linje med detta förtydligas även att det ingår i regionstyrelsens ansvar att ha kontroll på de största riskerna kring koncernens informationstillgångar.

Dessutom anpassas riktlinjerna till att även omfatta dataskydd i linje med att standarderna kring ledningssystem för informationssäkerhet numera även omfattar dataskydd. Riktlinjerna föreslås därför byta namn till ”Riktlinje för informationssäkerhet samt dataskydd”. I samband med denna ändring introduceras även rollen dataskyddssamordnare. Dataskydds-samordnare skulle kunna vara samma person som informations-säkerhetssamordnare utifrån storlek på nämnd/bolag. Däremot bör varken rollen som informationssäkerhetssamordnare eller dataskyddssamordnare delas med rollen dataskyddsombud i enlighet med EU:s dataskydds-förordning som säger att dataskyddsombud inte ska ha en intressekonflikt genom att t.ex. delta i utformningen av dataskyddsåtgärder.

För att skapa tydligare förutsättningar för informationssäkerheten vid de förtroendevaldas arbete förslås ett centralt ansvar hos regionlednings-kontoret för att samordna detta.

En bestämmelse som funnits kring informationssäkerhet vid rekrytering och anställning tas bort då detta regleras i riktlinjerna för säkerhet och därmed anses överflödigt. Däremot tillförs en bestämmelse som kravställer att medarbetare och förtroendevalda ska underteckna en ansvars-förbindelse innan de erhåller tillgång till regionens it-miljö för att säkerställa att de förstår förutsättningarna för detta.

[2] https://diarium.intranat.regionstockholm.se/Details/Case/17957408

En avgränsning läggs till för att förtydliga att informationssäkerhet i enlighet med säkerhetsskyddslagen hanteras i riktlinjerna för säkerhetsskydd.

För att ensa utseendet med övriga riktlinjer inom Region Stockholm tas numrering i respektive avsnitt bort.

Regleringen av att obligatorisk grundläggande utbildning inom informationssäkerhet ska utgöras av DISA tas bort, då obligatoriska utbildningar inte brukar regleras i riktlinjer.

Skrivningen om nämnder och bolags övergripande riskanalys har justerats för att tydliggöra att detta ska ske inom ramen för arbetet med intern styrning och kontroll.

För att inte hamna i konflikt med skrivningar i avsnitt 2.6 i Riktlinje för intern kontroll tas skrivningar om informationssäkerhetchefens och informationssäkerhetssamordnarens rapportering av större avvikelser bort.

Arbetsprocess och förankring
I utarbetandet av förslaget har regionledningskontoret tagit intryck av synpunkter från nämnder och bolag som har lämnats bland annat inom ramen för arbetet vid Region Stockholms informationssäkerhetsråd. Dessutom har erfarenheter från Region Stockholm CERT:s[3] arbete med incidenter arbetats in i förlaget.

Vid utformningen av riktlinje för informationssäkerhet samt dataskydd har följande principer varit styrande i utformningen:

- Riktlinjerna ska inte återupprepa sådant som redan är reglerat i lag. Information om sådant som regleras i lag tas i stället med i vägledningar och metodstöd.
- Riktlinjernas utformning ska bidra till att minska den administrativa bördan i kärnverksamheten. Det innebär att vi ska undvika att reglera lokalt dubbelarbete. Inriktning är även att alla medarbetare inte ska behöva läsa allt i riktlinjerna.

[3] Regionens gemensamma funktion för att förebygga och hantera it- och cybersäkerhetsincidenter.

- Riktlinjerna ska skapa en gemensam lägsta nivå för arbetet med informationssäkerhet samt dataskydd som fungerar för alla verksamhetsområden i Region Stockholm.

I samband med revideringen har individuella dialoger genomförts med informationssäkerhetssamordnare vid nämnder och bolag för att fånga upp synpunkter. Dessutom har intern dialog skett på regionledningskontoret med avdelningarna Ekonomi och finans, Strategisk HR, Strategisk Juridik samt Säkerhet och beredskap.

I utarbetandet av det slutliga förslaget kommer regionledningskontoret att ta hänsyn till de synpunkter som lämnas inom ramen för föreliggande remittering.

Ekonomiska konsekvenser
Beslut i enlighet med förslaget bedöms inte i sig innebära ekonomiska konsekvenser. Regionledningskontoret bedömer dock att förslaget kommer att ge tydligare och mer samordnade arbetssätt inom Region Stockholm, vilket förväntas underlätta för nämnder och bolag att begränsa kostnads- och utvecklingstakten. Förslagets tonvikt på enhetliga processer bedöms också kunna bidra till minskade administrativa kostnader.

Region Stockholm

Diarienummer
RS 2025-0418

Riktlinje

Riktlinje för informationssäkerhet samt dataskydd

Beslutad av regionfullmäktige den X

Gäller tills vidare

Gäller för Region Stockholm

INNEHÅLLSFÖRTECKNING

1. Styrning och planering

1.1 Syfte och omfattning

Dessa riktlinjer konkretiserar Region Stockholms policy för verksamhetsskydd och är styrande för skyddet av informationstillgångar som hanteras vid Region Stockholms samtliga nämnder och bolag.

För att underlätta tillämpning av regelverket kommer det att finnas vägledningar och råd som förtydligar hur det praktiska arbetet med att följa riktlinjerna kan gå till.

Riktlinjerna utgår från internationell standard avseende systematiskt arbetssätt för cyber- och informationssäkerhet samt dataskydd (ISO 27000-serien).

För informationstillgångar som omfattas av säkerhetsskydd regleras arbetet med informationssäkerhet i Riktlinje för säkerhetsskydd och signalskydd.

1.2 Region Stockholms styrande dokument för informationssäkerhet

Varje nämnd och bolag ska, inom ramen för Region Stockholms övergripande ledningssystem för informationssäkerhet, styra och leda sitt informationssäkerhetsarbete i ett ledningssystem inom sitt verksamhetsområde. Det lokala ledningssystemet ska säkra ett systematiskt informationssäkerhetsarbete och en riskavvägd skyddsnivå i verksamheten, och det ska vara en integrerad del i nämndens eller bolagets ordinarie ledningsarbete.

De styrande dokumenten på lokal nivå består av Region Stockholms policy för verksamhetsskydd, Region Stockholms riktlinje för informationssäkerhet samt dataskydd, eventuella kompletterande lokala riktlinjer och anvisningar för informationssäkerhet samt dataskydd.

1.3 Styrning

Riktlinjerna är bindande och ska efterlevas av samtliga nämnder och bolag inom Region Stockholm.

Ansvaret för informationssäkerhet samt dataskydd är kopplat till verksamhetsansvaret i alla led. Det betyder att varje nämnd eller bolag och varje medarbetare som är ansvarig för en verksamhet också har att ansvara för informationssäkerheten i denna verksamhet.

I de fall nämnder och bolag uppdrar åt andra att hantera information ska avtalet om denna hantering omfatta sådana krav att informationen hanteras i enlighet med dessa riktlinjer. Den nämnd eller det bolag som avtalar med annan om hantering av information ansvarar också för en

uppföljning av utförandet och de avtal som ligger till grund för utförandet, så att informationen ges ett avtalsenligt skydd.

Utformning av skyddsåtgärder i enlighet med dessa riktlinjer ska anpassas utifrån organisation, uppdrag, hotbild och sårbarheter.

1.4 Planering

Inom Region Stockholms nämnder och bolag ska ett systematiskt och långsiktigt arbete bedrivas med att skydda informationstillgångar.

Region Stockholm ska ha en strategisk inriktning för arbetet med informationssäkerhet samt dataskydd. Inriktningen ska innehålla mål för arbetet samt prioriterade initiativ. Den strategiska inriktningen ska tas fram av Region Stockholms informationssäkerhetschef i samverkan med funktioner för informationssäkerhet samt dataskydd i nämnder och bolag. Inriktningens prioriterade initiativ för området ska fastställas av regionfullmäktige i samband med budget.

2. Bedömning och hantering av risker

Region Stockholms informationstillgångar ska skyddas oavsett vilken form de har. Om det visar sig att skyddet kan kringgås är det viktigt att verksamheten har en förmåga att upptäcka detta. Därför ska medarbetare i Region Stockholms nämnder och bolag ha den kunskap som behövs om hur de kan agera för att förebygga och hantera risker i den dagliga verksamheten. Denna kunskap uppnås bland annat genom ett systematiskt arbete med riskanalyser.

2.1 Riskbedömning och riskhantering

Nämnder och bolag ansvarar för att analyser genomförs för verksamheter samt it-system avseende vilka risker som kan påverka deras informationstillgångar. Med utgångspunkt i denna bedömning ska beslutas hur riskerna ska hanteras och nödvändiga åtgärder ska vidtas för att upprätthålla rätt skyddsnivå för informationen.

Riskbedömning och riskhantering ska vara en kontinuerlig process och stödja arbetet med informationssäkerhet samt dataskydd. Riskbedömningar ska revideras när förutsättningarna väsentligen förändras.

Riskbedömning och riskhantering ska genomföras i enlighet med vad som anges i Region Stockholms riktlinje för intern kontroll.

Varje nämnd och bolag ska minst årligen genomföra en riskanalys för att identifiera de största riskerna mot de informationstillgångar som hanteras. Denna analys ska dokumenteras inom ramen för intern styrning och kontroll.

Regionstyrelsen ska även genomföra en riskanalys kring de största riskerna mot de informationstillgångar som hanteras i koncernen Region Stockholm. Denna riskanalys ska kunna användas som ett delunderlag i den risk- och sårbarhetsanalys som Region Stockholm ska genomföra enligt lag om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

3. Organisation av informationssäkerheten

För att styra informationssäkerhetsarbetet inom nämnder och bolag i Region Stockholm är det viktigt att roller och ansvar fördelas.

3.1 Roller och ansvar på övergripande nivå i Region Stockholm

Regionövergripande ledning, samordning, uppföljning och analys

Regionstyrelsen ansvarar för uppsikt över nämndernas och bolagens arbete med informationssäkerhet samt för analys, ledning och samordning inom området.

Regionstyrelsen har mandat att fatta beslut om åtgärder för att skydda regionens informationstillgångar vid misstanke om eller vid informationssäkerhetsincident som bedöms kunna leda till allvarlig skada.

Under regionstyrelsen ska det finnas en informationssäkerhetschef för Region Stockholm som samordnar och följer upp regionens informationssäkerhetsarbete. Informationssäkerhetschefen svarar för utbildning och stöd till informationssäkerhetssamordnare.

Informationssäkerhetschefen ansvarar för att säkerställa att de förtroendevalda får stöd i att deras arbete har möjlighet att genomföras med god informationssäkerhet.

3.2 Roller och ansvar i nämnder och bolag

Lokal ledning av informationssäkerhetsarbetet

Förvaltningschefen eller bolagschefen (VD) ansvarar inför nämnden eller styrelsen för arbetet med informationssäkerhet samt dataskydd.

Varje nämnd och bolag ska utse en informationssäkerhetssamordnare som har i uppgift att samordna och följa upp arbetet med informationssäkerhet inom den egna organisationen.

Varje nämnd och bolag ska utse en dataskyddssamordnare som har i uppgift att samordna och följa upp arbetet med dataskydd inom den egna organisationen.

Ägare av it-system

När en nämnd eller ett bolag tar ett system eller nätverk i bruk ansvarar nämnden eller bolaget för att kontrollera att det finns ett definierat ägarskap för det aktuella systemet, eller att etablera ett sådant. Ägaren av

it-system ska informera alla nämnder och bolag som använder systemet om vilken information som får bearbetas där.

Ägaren av ett it-system ska ansvara för att en definierad skyddsnivå finns i förhållande till vilken information som får användas i systemet. I ägarens uppdrag ingår också att tillse att systemet har en aktiv förvaltning och övervakning av it-systemet samt livscykelhantering för systemet.

Att ett system som nyttjas av en nämnd eller ett bolag ägs av en annan nämnd eller ett annat bolag fritar inte den nyttjande nämnden eller bolaget från ansvar för att följa upp att ägaren skyddar systemet. Det är den nyttjande nämnden eller bolaget som ansvarar för att information som förs in i systemet inte har en högre skyddsnivå än vad it-systemet är utformat för.

Ägarskap av it-system eller nätverk kan inte delas mellan nämnder och bolag, men en nämnd eller ett bolag kan ges i uppdrag att utöva ägarskap för en tjänst som nyttjas av flera nämnder och bolag. Den nämnd eller det bolag som ges ett sådant uppdrag har fullt mandat att besluta om tjänstens utformning inom ramen för uppdraget. Ägarskap ska dock utövas med utgångspunkt i Region Stockholms samlade behov och krav på tjänsten och med respekt för samtliga nämnder och bolags behov.

3.3 Informationssäkerhetsråd

För att samordning och uppföljning av informationssäkerhetsarbetet ska kunna bedrivas effektivt ska det finnas ett informationssäkerhetsråd inom Region Stockholm. Rådet leds av informationssäkerhetschefen för Region Stockholm. Utöver denne ska rådet bestå av informationssäkerhets-samordnare från varje nämnd och bolag.

Rådets uppgift ska vara stödjande till Region Stockholms informations-säkerhetschef. Rådet ska främja erfarenhets- och kunskapsutbyte, bevaka vilket behov av stöd som finns i verksamheterna och föreslå förbättringar samt förankra och samordna informationssäkerhetsaktiviteter.

4. Medarbetare och informationssäkerhet

Alla som arbetar eller på annat sätt deltar i Region Stockholms verksamhet måste förstå sitt ansvar för och bidra till att hantera och skydda Region Stockholms informationstillgångar. Läs även bestämmelser kring medarbetare och informationssäkerhet i Riktlinjer för säkerhet.

4.1 Sekretess

Tystnadsplikt ska regleras i avtal i de fall då personer deltar i verksamheten och inte är bundna av tystnadsplikt enligt lag.

4.2 Regler för användning av it-utrustning

Innan medarbetare och förtroendevalda får tillgång till it-utrustning eller erhåller inloggningsuppgifter ska de ha skrivit under ansvarsförbindelse. Regionstyrelsen ansvarar för fastställandet av denna ansvarsförbindelse och rutiner för detta.

4.3 Utbildning och fortbildning i informationssäkerhet

Nämnder och bolag ansvarar för att medarbetare får den utbildning i informationssäkerhet som behövs för att säkerställa säker hantering av de informationstillgångar som medarbetaren kan komma att ta del av. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen.

Nämnder och bolag ska säkerställa att lämplig kunskapsnivå bibehålls under medarbetarens hela anställnings- eller uppdragstid.

Medarbetare vid samtliga nämnder och bolag ska minst ha genomgått en grundläggande utbildning inom informationssäkerhet och behandling av personuppgifter.

4.4 Avslutande av anställning eller uppdrag

Nämnder och bolag ska i rutin för avslut av anställning eller uppdrag inkludera informationssäkerhetsperspektivet som säkrar återlämnande av informationstillgångar samt medvetenhet om fortsatt tystnadsplikt.

5. Hantering av informationstillgångar

Detta kapitel handlar om hur informationstillgångar ska hanteras. Sekretessbelagda uppgifter och personuppgifter är exempel på känslig information som behöver extra skyddsåtgärder.

5.1 Värdering och skydd av information

Nämnder och bolag ansvarar för att informationstillgångar identifieras och värderas utifrån sitt skyddsbehov (vilken skada som kan uppstå).

Förteckning, riskhantering och kontroll av regelefterlevnad för it-system samt personuppgiftsbehandling hos nämnder och bolag ska följa Region Stockholms gemensamma processer. Regionstyrelsen ansvarar för fastställande av dessa processer.

Nämnders och bolags informationstillgångar ska ges skydd med utgångspunkt i att de ska finnas tillgängliga när de behövs (tillgänglighet), att de är skyddade mot obehörig förändring (riktighet) och att obehöriga inte kan få tillgång till dem (konfidentialitet). Skyddet av informationstillgångarna ska utformas så att efterlevnad av styrande regelverk uppnås samt med hänsyn till nämnders och bolags riskacceptans.

5.2 Information om skyddsvärde

Innan informationstillgångar överlämnas till behörig ska mottagaren informeras om informationens skyddsvärde avseende konfidentialitet.

5.3 Hantering av informationstillgångar vid lagring och överföring

Informationstillgångar, där förlust av konfidentialitet kan leda till en skada som är större än försumbar, ska skyddas mot obehörig åtkomst vid lagring och överföring.

Informationstillgångar, där förlust av riktighet kan leda till allvarlig skada, ska förses med skydd för att upptäcka olovlig förändring av data vid lagring och överföring.

5.4 Inventering av it-utrustning

Nämnder och bolag ansvarar för att det finns uppdaterad inventarieförteckning över all it-utrustning som har möjlighet att kommunicera över nätverk.

5.5 Hantering av lagringsmedier

Lagringsmedier som inte längre ska användas för sitt ändamål ska förstöras alternativt raderas på ett sådant sätt att uppgifterna inte kan återskapas. Nämnder och bolag ansvarar för att det finns rutiner för detta.

5.6 Hantering av informationstillgångar utanför verksamhetens lokaler

Nämnder och bolag ansvarar för att det finns regler och säkerhetsåtgärder för att skydda information som nås, bearbetas eller lagras vid arbete utanför verksamhetens lokaler.

6. Åtkomst till informationstillgångar

Här finns bestämmelser för hur åtkomsten till informationstillgångar administreras och kontrolleras så att endast behöriga personer och resurser kommer åt information.

6.1 Autentisering (identifiering av personer och system)

Alla utställda identiteter i ett it-system ska vara unika över tid. Åtkomsten ska vara spårbar till en fysisk person eller ett system.

Ägare av it-system ansvarar för att system, som hanterar information som vid förlust av konfidentialitet, riktighet eller tillgänglighet kan leda till allvarlig skada, har åtkomstkontroll som baseras på autentisering med minst tillitsnivå 3 i enlighet med tillitsramverket för svensk e-legitimation.

All distansanslutning till it-miljöer som är anslutna till Region Stockholms regionala nätverk ska ske genom en lösning som den regionala nätägaren tillhandahåller eller godkänner. Autentisering vid sådan anslutning ska ske med minst tillitsnivå 2 i enlighet med tillitsramverket för svensk e-legitimation.

6.2 Åtkomstkontroll till informationstillgångar

Behörighet till informationstillgångar ska baseras på användarens aktuella arbetsuppgifter och organisatoriska tillhörighet för att endast ge åtkomst till de informationstillgångar som behövs för att lösa arbetet.

Ägare av it-system ansvarar för att det finns tillämpade rutiner för beställning, registrering, ändring och avregistrering av behörighet i it-system. Rutinerna ska även omfatta administratörsbehörigheter.

Konton som ger systemadministrativ behörighet får endast användas för systemadministration och ska tilldelas restriktivt.

Den som är inloggad i ett it-system ansvarar för vem som tar del av information via den inloggningen.

Tilldelning av behörighet i it-system ska dokumenteras och regelbundet följas upp. Uppföljningen ska minst ske en gång per år.

Det ska finnas en funktion som säkerställer automatisk utloggning ur it-system eller aktivering av låst skärm efter en viss tids inaktivitet som bedöms rimlig ur risksynpunkt för tänkt användningsområde för it-systemet.

6.3 Styrning av åtkomst till icke digital information

När icke-digitala informationstillgångar överförs ska den som förmedlar informationen förvissa sig om att mottagaren är den avsedda och att lämpliga skyddsåtgärder vidtagits för att säkerställa detta.

6.4 Avstängning av åtkomst

Medarbetares tillgång till it-system får stängas av då användningen utgör en hög risk för regionens it-miljö och/eller informationstillgångar.

Anslutning till Region Stockholms regionala nätverk får stängas av då anslutningen utgör hög risk mot regionens it-miljö och/eller informationstillgångar. Beslut om sådan avstängning ska fattas av ägaren av det regionala nätverket, eller person med delegation därifrån. Innan beslut om avstängning fattas ska riskerna med avstängningen ha analyserats.

7. Kryptering

Kryptering kan användas för att skydda information från att kunna läsas då den kommer i orätta händer. Kryptering kan också användas för att skydda information från obehörig förändring.

7.1 Kryptografiska säkerhetsåtgärder

Vid kryptering av information ska etablerade och pålitliga algoritmer samt nyckellängder användas.

Vid kryptering vid informationsöverföring ska etablerade kryptografiska protokoll användas och konfigureras enligt god standard.

Vid kryptering ska det finnas administrativa och tekniska skyddsåtgärder som säkerställer att krypteringsnyckeln hanteras säkert över sin livscykel.

8. Fysisk och miljörelaterad säkerhet

Tillträdeskontroll, skalskydd och brandskydd handlar om hur informationstillgångar (inkl. it-system) ska skyddas, både i egna lokaler och vid inhyrning i andras.

8.1 Generellt om fysisk och miljörelaterad säkerhet

Utrymmen som innehåller informationstillgångar ska ha ett fysiskt skydd som utformas och dimensioneras utifrån tillgångarnas värde, identifierade risker och styrande regelverk.

8.2 Skalskydd och tillträdeskontroll

Utrymmen som innehåller informationstillgångar ska skyddas genom åtgärder som säkerställer att endast behöriga får tillträde till tillgångarna.

8.3 Skydd mot angrepp, olyckor och naturkatastrofer

Utrymmen som innehåller informationstillgångar (och informationsbehandlingsresurser) ska ha ett fysiskt skydd mot naturkatastrofer, illvilliga angrepp eller olyckor som är anpassat till tillgångarnas värde.

9. Driftsäkerhet

För att undvika störningar och driftstopp i Region Stockholms it-system krävs en förvaltning och drift med etablerade rutiner för till exempel driftsättning, säkerhetskopiering och loggning.

9.1 Test, utveckling och utbildning i it-miljön

Om informationstillgångar, som vid förlust av konfidentialitet kan leda till en skada som är större än försumbar, hanteras i miljöer för utveckling, test eller utbildning ska samma skydd uppnås som i produktionsmiljö.

Tester av it-miljön ska riskhanteras och ska inte introducera risker som kan medföra allvarlig skada i produktionsmiljön.

9.2 Rutiner för drift och förvaltning

Ägare av it-system och nätverk ansvarar för att administration, drift och underhåll av it-system sker på ett strukturerat och spårbart sätt.

Ägare av it-system som innehåller information där förlust av konfidentialitet, riktighet eller tillgänglighet med allvarlig skada ska tillse att det finns en kontinuerlig övervakning under systemets drifttid/öppettid för att proaktivt upptäcka och åtgärda fel, minimera avbrott och förebygga andra it-incidenter.

9.3 Systemdokumentation

Ägaren av it-system ansvarar för att it-systemet är dokumenterat. Dokumentationen ska ge tillräckligt stöd för strukturerad och säker drift och förvaltning.

Ägaren av it-system ska säkerställa att användarna får kunskap om vilken typ av information som får hanteras i ett it-system och eventuella regler kring denna hantering.

9.4 Säkerhetsloggning

Ägaren av it-system ansvarar för att händelser som kan ha betydelse för säkerheten i it-systemet eller it-miljön i Region Stockholm loggas. Av denna säkerhetslogg ska tidpunkt och annan för händelsen relevant information framgå.

Ägaren av it-system ansvarar för att det finns rutiner för hantering av systemets loggar och händelser som kan påverka säkerheten i it-systemet. Rutinerna ska omfatta hur systemförvaltningen ska kunna upptäcka obehörig åtkomst eller annan skadlig påverkan. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser.

Ägare av it-system ska, då regionstyrelsen efterfrågar detta, tillgängliggöra sådana säkerhetsloggar som behövs för att kunna upptäcka och utreda hot mot och sårbarheter i skyddet av Region Stockholms regionala it-infrastruktur.

It-system ska ha korrekt tidsangivelse.

Nämnder och bolag ska informera medarbetare om att användning av it-system loggas och att loggarna kan granskas för att undersöka it- och cybersäkerhetsrelaterade sårbarheter och hot riktade mot Region Stockholms informationstillgångar och it-miljö.

9.5 Säkerhetsuppdateringar och versionshantering

Ägaren av it-system ska säkerställa att endast it-system används där alla delkomponenter fortfarande supporteras av respektive leverantör. Om detta inte är möjligt ska riskerna reduceras till en acceptabel nivå.

Leverantörs säkerhetsuppdateringar ska installeras skyndsamt i it-system.

9.6 Skydd mot skadlig kod

Ägaren av it-system ska säkerställa att behovet av skydd mot skadlig kod i it-systemet är analyserat.

I de fall behov av skydd mot skadlig kod finns ska ägaren av it-systemet säkerställa att sådant skydd implementeras.

9.7 Styrning av ändringar i it-system

Det ska finnas rutiner för ändringshantering och testning av it-system.

9.8 Säkerhetskopiering och återläsning av data

Säkerhetskopiering av informationstillgångar (inklusive programvara) ska utföras regelbundet, med frekvens och omfattning anpassad till verksamhetskrav respektive legala krav, enligt fastställd instruktion. För information, som behövs för organisationens förmåga att utföra sitt uppdrag, ska säkerhetskopiering ske minst en gång per dygn.

Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras. För information, som behövs för nämnden eller bolagets förmåga att utföra sitt uppdrag, ska kontroll ske minst en gång per år att uppgifterna på säkerhetskopiorna går att återskapa inom den tidsrymd som nämndens eller bolagets kontinuitetsplanering kräver.

Säkerhetskopior och original ska förvaras fysiskt åtskilda i enlighet med informationens skyddsvärde.

10. Kommunikationssäkerhet

En viktig förutsättning för att skydda Region Stockholms it-system är att det finns bra skyddsåtgärder i nätverken samt kontroll på vilken kommunikation som sker i nätverken.

10.1 Generella skyddsåtgärder i nätverk

Ägaren av nätverk ansvarar för att nätverk förses med skyddsåtgärder för att motverka obehörig åtkomst.

Ägaren av nätverk ansvarar för att nätverk delas upp genom fysisk eller logisk separation. Avgränsningen ska vara tydlig och dokumenterad.

Användare med it-utrustning som inte är kontrollerad eller godkänd av Region Stockholm får endast anslutas till för detta avsedda gästnätverk.

Om ägare av nätverk som är anslutna till Region Stockholms regionala nätverk vill ha egna anslutningar till andra nätverk fordras att risk- och konsekvensanalys utförs och att särskild överenskommelse tecknas med ägaren av det regionala nätverket som reglerar det gemensamma nättrafikskyddet.

10.2 Skyddsåtgärder i trådlösa nätverk

Trafik i trådlösa nätverk ska krypteras.

10.3 Specifika skyddsåtgärder i Region Stockholms regionala nätverk

Anslutningar av nätverk till Region Stockholms regionala nätverk får endast ske i enlighet med rutiner som beslutats av ägaren till det regionala nätverket.

Ägaren för Region Stockholms regionala nätverk ansvarar för att alla anslutningar passerar genom perimeterskydd.

Alla perimeterskydd i anslutningar till och från Region Stockholms regionala nätverk ska ha regelverk som bara släpper igenom trafik som har ett verifierat verksamhetsbehov.

10.4 Skyddsåtgärder vid extern informationsöverföring

Överföring av informationstillgångar utanför Region Stockholm ska regleras genom avtal om inte överföringen redan regleras genom författning.

11. Utveckling, anskaffning och underhåll av it-system

Informationssäkerhet ska hanteras under ett it-systems hela livscykel. Därför är det viktigt att dessa frågor hanteras i ett tidigt skede. Hur kravställning och avtalsskrivning ska gå till i samband med upphandling beskrivs i nästa kapitel.

11.1 Anskaffning av IT

När en verksamhet köper IT som tjänst hos extern part eller förlägger drift av it-system hos en sådan, ska minst samma regler för informationssäkerhet samt dataskydd gälla som när driften hanteras i egen regi.

11.2 Systemutvecklingsprojekt

Informationssäkerhet ska hanteras i systemutvecklingsprojekt genom dokumenterade modeller för systemutveckling och projektstyrning.

11.3 Test

Instruktioner för acceptanstest, driftgodkännande och produktionssättning ska finnas och tillämpas vid nämnder och bolag som bedriver drift av it-system.

12. Leverantörsrelationer

Det är viktigt att Region Stockholms informationstillgångar har samma skydd även då de hanteras av en leverantör.

12.1 Kravställning

Innan anskaffning ska analys ske av vilka krav avseende informationssäkerhet samt dataskydd som ska ställas.

Kraven som ställs i samband med anskaffning ska säkerställa skyddet för de informationstillgångar som leverantören eller leverantörens produkter kommer att hantera.

Nämnder och bolag ansvarar för att leverantörer har motsvarande informationssäkerhetskrav på sig som om Region Stockholm hade tillhandahållit tjänsten i egen regi.

12.2 Upprättande och förvaltning av avtal

Vid upprättande av avtal med extern leverantör som ska hantera informationstillgångar åt verksamheten ska kraven på informationssäkerhet regleras.

Avtalet ska specificera hur händelser som rör informationssäkerhet ska hanteras då de uppstår hos leverantören relaterat till de informationstillgångar de hanterar åt nämnden eller bolaget.

Avtalet ska specificera vad som händer om leverantören inte följer de krav som ställts gällande informationssäkerhet.

Avtalet ska specificera att verksamheten har rättighet att genomföra revision av informationssäkerheten.

Nämnder och bolag ansvarar för att uppföljning sker gällande hur leverantörer de har avtal med hanterar informationssäkerheten.

12.3 Riskhantering av leverantörsberoenden

Risker som följer av beroendet av en leverantör ska minimeras och åtgärder vidtas för att hantera konsekvenserna av att leverantören inte kan fullfölja sitt uppdrag.

13. Hantering av händelser som rör informationssäkerhet

När en allvarlig händelse inträffar som påverkar informationssäkerheten är det viktigt att snabbt agera för att begränsa eller avvärja konsekvenserna av händelsen. Störningar kan ha flera orsaker och kan snabbt komma att påverka många delar av verksamheten, men också andra aktörer i samhället.

13.1 Hantering av informationssäkerhetshändelser

Samtliga nämnder och bolag ska följa Region Stockholms process för att hantera händelser som kan utgöra ett hot mot Region Stockholms informationstillgångar inom respektive nämnds och bolags ansvarsområde. Regionstyrelsen ansvarar för fastställande av denna process.

13.2 Analys av it-utrustning

Regionstyrelsen ansvarar för att Region Stockholm har förmåga att genomföra analys av it-utrustning i de fall då utrustningen misstänks utgöra ett hot mot Region Stockholms it-miljö eller informationstillgångar.

Nämnder och bolag ska tillgängliggöra sådan it-utrustning, som misstänks kunna vålla skada på Region Stockholms it-miljö eller informations-tillgångar, för analys om utrustningen utgör ett sådant hot. It-utrustningen ska tillgängliggöras till regionstyrelsen, eller funktion meduppdrag därifrån.

14. Kontinuitetshantering

Verksamheten ska kunna fortsätta även om till exempel it-system slås ut, en strömkabel grävs av eller byggnader brinner ner. Därför är det viktigt att planera för hur verksamheten ska fungera om det händer något.

14.1 Generella regler för kontinuitetsplanering

Informationssäkerhet ska vara en integrerad del av den överordnade processen för verksamhetens kontinuitetsplanering. Processen ska behandla nödvändiga informationssäkerhetskrav som behövs för verksamheten i kontinuitet.

15. Uppföljning

Region Stockholm ska följa upp hur väl ledningssystemet för informationssäkerhet fungerar och utvärdera skyddet av verksamhetens informationstillgångar för att identifiera förbättringsbehov.

15.1 Uppföljning av regelverket

Anpassningar av Region Stockholms styrande dokument för informationssäkerhet samt dataskydd ska ske utifrån förändringar i lagar och föreskrifter, uppdateringar av rekommendationer på området, resultat från analyser av sårbarheter och hotbild samt förändringar i verksamhet och verktyg.

15.2 Uppföljning av efterlevnad

Varje nämnd och bolag ska regelbundet genomföra revision av sin informationssäkerhet samt dataskydd och göra en analys av hur skyddsåtgärder förhåller sig till gällande styrande regelverk samt aktuell hotbild. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas, anpassas och kompletteras.

Varje år ska nämnder och bolag följa upp status på informationssäkerheten samt dataskydd inom det egna ansvarsområdet.

Regionstyrelsen ska årligen utvärdera informationssäkerheten och verkan av det övergripande ledningssystemet för informationssäkerhet inom Region Stockholm.

15.3 Uppföljning av händelser i it-miljön

Användning av Region Stockholms it-system ska följas upp för att upptäcka hot mot informationstillgångar och it-miljö. Vid misstanke om brott mot lag eller Region Stockholms styrande regelverk kan fördjupad uppföljning komma att ske.

Regionstyrelsen ansvarar för att det finns instruktioner för hur kontroll ska genomföras av loggar i central it-infrastruktur i syfte att identifiera hot mot och reducera sårbarheter i Region Stockholms it-miljö eller informationstillgångar.

Nämnder och bolag ska följa Region Stockholms process för kontroll av medarbetares användning av it-utrustning då så är nödvändigt. Regionstyrelsen ansvarar för fastställande av denna process.

16. Begrepp

Nedan följer förklaringar av begrepp som används i detta dokument. Begreppen utgår från ISO-standarder[1] och förskrifter[2] på området.

Begrepp	**Förklaring**
Allvarlig skada	Allvarlig negativ påverkan för Region Stockholm, annan myndighet eller enskilda fysiska eller juridiska personer. (Kan t.ex. handla om att känsliga personuppgifter röjs till obehörig; att ett sjukhus inte kan leverera en viss typ av vård eller att en tunnelbanelinje har stora störningar.) Motsvarar konsekvensnivå 4 i Region Stockholms riskmodell.
Autentisering	Kontroll av uppgiven identitet.
Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.
Dataskydd	Skydd av den personliga integriteten enligt de regelverk som ska tillämpas vid behandling av personuppgifter.
Fysisk säkerhet	Tekniska säkerhetsåtgärder relaterade till skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten.
Försumbar skada	Försumbar negativ påverkan på Region Stockholm, annan myndighet eller enskilda fysiska eller juridiska personer. Motsvarar konsekvensnivå 1 i Region Stockholms riskmodell.
Hot	Möjlig orsak till en oönskad händelse som kan medföra negativa konsekvenser för verksamheten.
Informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.

[1] Terminologi för informationssäkerhet (SIS-TR 50:2015)
Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Översikt och terminologi (ISO/IEC 27000:2018)
[2] Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2015:4) om landstings risk- och sårbarhetsanalyser

Begrepp	Förklaring
Informationssäkerhets-händelse	Förekomst eller förändring av specifika omständigheter som försämrar skyddet av informationstillgångar. (En händelse kan även bestå av något som inte händer; En händelse kan ibland refereras till som en "incident" eller "olycka”.)
Informationssäkerhets-incident	Enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet.
Informationstillgång	Information, och resurser som hanterar den, som är av värde för verksamheten. (Detta inkluderar även personuppgifter enligt EU:s dataskyddsförordning.)
It-system	System med teknik som hanterar och utbyter information med omgivningen.
It-utrustning	Fysisk utrustning som hanterar och utbyter information med omgivningen.
Konfidentialitet	Skydd mot obehörig insyn.
Kontinuitetsplanering	Åtgärder för att säkerställa verksamhetens kontinuitet vid olika allvarliga störningar.
Kryptering	Omvandling av klartext till kryptotext med hjälp av ett kryptosystem och en krypteringsnyckel eller en publik krypteringsnyckel i syfte att förhindra obehörig åtkomst till information
Ledningssystem	Uppsättning av samverkande eller varandra påverkande delar av en organisation för att upprätta policyer och mål samt processer för att uppnå dessa mål.
Medarbetare	Alla som arbetar, eller på annat sätt deltar i verksamheten.
Policy för verksamhetsskydd	Dokument innehållande Region Stockholms styrande principer rörande skyddet av verksamheten.
Region Stockholms regionala nätverk	Nätverk som används för att sammankoppla de lokala nätverken vid nämnder och bolag.
Riktighet	Skydd mot oönskad förändring.
Risk	En sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till.
Riskanalys	Process för att förstå riskens natur och för att avgöra risknivån.

Begrepp	Förklaring
Riskbedömning	Övergripande process som innefattar delprocesserna riskidentifiering, riskanalys och riskutvärdering.
Riskhantering	Samordnade aktiviteter för att styra och leda en verksamhet med avseende på risk.
Riskidentifiering	Process för att upptäcka, kartlägga och beskriva risker.
Riskutvärdering	Process för att jämföra resultaten från riskanalysen med riskkriterierna för att avgöra om risken och/eller dess storlek är acceptabel eller godtagbar.
Riskägare	Person som ansvarar för och har befogenhet att hantera en risk.
Styrande regelverk	Lagar, förordningar, interna styrande dokument (som t.ex. reglemente och arbetsordning) samt avtal.
Sårbarhet	Brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot.
Säkerhetslogg	Logg över säkerhetskritiska händelser.
Tillgång	Allt som är av värde för verksamheten. (Det kan handla om både materiellt värde och det som har ett immateriellt värde, t.ex. förtroende eller varumärke.)
Tillgänglighet	Åtkomst för behörig person vid rätt tillfälle.
Åtkomstkontroll	Funktioner i ett system som syftar till att reglera och kontrollera en användares åtkomst till information och resurser.

Regionledningskontoret
Strategisk IT
Informationssäkerhet

ÄNDRINGSBILAGA
2025-04-14

RS 2025-0418

Handläggare Henrik Brodin
Telefon 08-123 177 95
E-post henrik.brodin@regionstockholm.se

Ändringsbilaga

Läsanvisning:
~~Genomstryken text~~ som är borttagen eller omformulerad,
ny/omformulerad text *kursiv*.

Ursprunglig text	**Ny text**
1.1 Syfte och omfattning	
~~1.1.3~~ Riktlinjerna utgår från internationell standard avseende ~~styrning och implementering av informationssäkerhet~~ (ISO 27000-serien).	Riktlinjerna utgår från internationell standard avseende *systematiskt arbetssätt för cyber- och informationssäkerhet samt dataskydd* (ISO 27000-serien).
	För informationstillgångar som omfattas av säkerhetsskydd regleras arbetet med informationssäkerhet i Riktlinje för säkerhetsskydd och signalskydd.
1.2 Region Stockholms styrande dokument för informationssäkerhet	
~~1.2.2~~ Styrdokumenten på lokal nivå består av Region Stockholms verksamhetsskyddspolicy, Region Stockholms riktlinjer för informationssäkerhet, eventuella kompletterande lokala riktlinjer och anvisningar för informationssäkerhet.	Styrdokumenten på lokal nivå består av Region Stockholms verksamhetsskyddspolicy, Region Stockholms Riktlinje för informationssäkerhet *samt dataskydd*, eventuella kompletterande lokala riktlinjer och anvisningar för informationssäkerhet *samt dataskydd*.

Ursprunglig text	Ny text
1.3 Styrning	
~~1.3.2~~ Ansvaret för informationssäkerhet~~en~~ är kopplat till verksamhetsansvaret i alla led. Det betyder att varje nämnd eller bolag och varje medarbetare som är ansvarig för en verksamhet också har att ansvara för informationssäkerheten i denna verksamhet.	Ansvaret för informationssäkerhet *samt dataskydd* är kopplat till verksamhetsansvaret i alla led. Det betyder att varje nämnd eller bolag och varje medarbetare som är ansvarig för en verksamhet också har att ansvara för informationssäkerheten i denna verksamhet.
1.4 Planering	
~~1.4.2 En lokal handlingsplan ska finnas vid varje nämnd och vid varje bolag. Av handlingsplanen ska framgå vilka prioriteringar och initiativ som görs avseende informationssäkerhet under innevarande år, med en inriktning för följande tre år. Planen ska årligen uppdateras med utgångspunkt i den systematiska uppföljningen och aktuella hot och sårbarheter.~~	*Region Stockholm ska ha en strategisk inriktning för arbetet med informationssäkerhet samt dataskydd. Inriktningen ska innehålla mål för arbetet samt prioriterade initiativ. Den strategiska inriktningen ska tas fram av Region Stockholms informationssäkerhetschef i samverkan med funktioner för informationssäkerhet samt dataskydd i nämnder och bolag. Inriktningens prioriterade initiativ för området ska fastställas av regionfullmäktige i samband med budget.*
2.1 Riskbedömning och riskhantering	
~~2.1.2~~ Riskbedömning och riskhantering ska vara en kontinuerlig process och stödja ~~informationssäkerhetsarbetet~~. Riskbedömningar ska revideras när förutsättningarna väsentligen förändras.	Riskbedömning och riskhantering ska vara en kontinuerlig process och stödja *arbetet med informationssäkerhet samt dataskydd*. Riskbedömningar ska revideras när förutsättningarna väsentligen förändras.

Ursprunglig text	Ny text
~~2.1.4~~ Varje nämnd och bolag ska minst årligen genomföra en riskanalys för att identifiera de största riskerna mot de informationstillgångar som hanteras. Denna analys ska dokumenteras.	Varje nämnd och bolag ska minst årligen genomföra en riskanalys för att identifiera de största riskerna mot de informationstillgångar som hanteras. Denna analys ska dokumenteras inom ramen för intern styrning och kontroll.
	Regionstyrelsen ska även genomföra en riskanalys kring de största riskerna mot de informationstillgångar som hanteras i koncernen Region Stockholm. Denna riskanalys ska kunna användas som ett delunderlag i den risk- och sårbarhetsanalys som Region Stockholm ska genomföra enligt lag om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.
3.1 Roller och ansvar på övergripande nivå i Region Stockholm	
~~3.1.3~~ Under regionstyrelsen ska det finnas en informations-säkerhetschef för Region Stockholm som samordnar och följer upp regionens informations-säkerhetsarbete. ~~Informations-säkerhetschefen ska ha möjlighet att rapportera större avvikelser i arbetet med informationssäkerhet till regionstyrelsen.~~ Informations-säkerhetschefen svarar för utbildning och stöd till informationssäkerhetssamordnare.	Under regionstyrelsen ska det finnas en informations-säkerhetschef för Region Stockholm som samordnar och följer upp regionens informations-säkerhetsarbete. Informations-säkerhetschefen svarar för utbildning och stöd till informationssäkerhetssamordnare.
	Informationssäkerhetschefen ansvarar för att säkerställa att de förtroendevalda får stöd i att deras arbete har möjlighet att genomföras med god informationssäkerhet.

Ursprunglig text	Ny text
3.2 Roller och ansvar i nämnder och bolag	
~~1.3.4~~ Förvaltningschefen eller bolagschefen (VD) ansvarar inför nämnden eller styrelsen för arbetet med informationssäkerhet. ~~Det löpande arbetet samordnas och följs upp av informationssäkerhetssamordnare (se 3.2.1)~~.	Förvaltningschefen eller bolagschefen (VD) ansvarar inför nämnden eller styrelsen för arbetet med informationssäkerhet *samt dataskydd*.
~~3.2.2 Informationssäkerhets-samordnaren ska ha möjlighet att rapportera större avvikelser i arbetet med informationssäkerhet till högsta ledningen i nämnden eller bolaget.~~	
	Varje nämnd och bolag ska utse en dataskyddssamordnare som har i uppgift att samordna och följa upp arbetet med dataskydd inom den egna organisationen.
4. Medarbetare och informationssäkerhet	
Alla som arbetar eller på annat sätt deltar i Region Stockholms verksamhet måste förstå sitt ansvar för och bidra till att hantera och skydda Region Stockholms informationstillgångar.	Alla som arbetar eller på annat sätt deltar i Region Stockholms verksamhet måste förstå sitt ansvar för och bidra till att hantera och skydda Region Stockholms informationstillgångar. *Läs även bestämmelser kring medarbetare och informationssäkerhet i Riktlinjer för säkerhet*

Ursprunglig text	Ny text
4.1 Rekrytering och anställning	
~~4.1.1 Innan och under anställning eller annat deltagande i verksamheten ska arbetsgivaren pröva att individen bedöms lämplig, dvs. individens lojalitet och pålitlighet från säkerhetssynpunkt, för att hantera de för tjänsten aktuella informationstillgångarna.~~	
4.2 Regler för användning av it-utrustning	
	Innan medarbetare och förtroendevalda får tillgång till it-utrustning eller erhåller inloggningsuppgifter ska de ha skrivit under ansvarsförbindelse. Regionstyrelsen ansvarar för fastställandet av denna ansvarsförbindelse och rutiner för detta.
4.3 Utbildning och fortbildning i informationssäkerhet	
~~4.3.3~~ Medarbetare vid samtliga nämnder och bolag ska minst ha genomgått en grundläggande utbildning inom informationssäkerhet. ~~Denna utbildning ska bestå av Region Stockholms DISA, Datorstödd informationssäkerhetsutbildning för användare, eller en utbildning som minst förmedlar motsvarande kunskap.~~	Medarbetare vid samtliga nämnder och bolag ska minst ha genomgått en grundläggande utbildning inom informationssäkerhet *och behandling av personuppgifter*.

Ursprunglig text	Ny text
5.1 Värdering och skydd av information	
	Förteckning, riskhantering och kontroll av regelefterlevnad för it-system samt personuppgifts-behandling hos nämnder och bolag ska följa Region Stockholms gemensamma processer. Regionstyrelsen ansvarar för fastställande av dessa processer.
11.1 Anskaffning av IT	
~~11.1.1~~ När en verksamhet köper IT som tjänst hos extern part eller förlägger drift av it-system hos en sådan, ska minst samma regler för informationssäkerhet gälla som när driften hanteras i egen regi.	När en verksamhet köper IT som tjänst hos extern part eller förlägger drift av it-system hos en sådan, ska minst samma regler för informationssäkerhet *samt dataskydd* gälla som när driften hanteras i egen regi.
11.1 Anskaffning av IT	
~~12.1.1~~ Innan anskaffning ska analys ske av vilka krav avseende informationssäkerhet som ska ställas.	Innan anskaffning ska analys ske av vilka krav avseende informationssäkerhet *samt dataskydd* som ska ställas.
13.1 Hantering av informationssäkerhetshändelser	
~~13.1.1~~ Samtliga nämnder och bolag ~~ansvarar för att det finns processer och rutiner~~ för att hantera händelser ~~och sårbarheter~~ som kan utgöra ett hot mot Region Stockholms informationstillgångar inom respektive nämnds och bolags ansvarsområde. ~~Nämnder och bolag ska också medverka i de regionövergripande processer som etablerats i detta syfte.~~	Samtliga nämnder och bolag *ska följa Region Stockholms process* för att hantera händelser som kan utgöra ett hot mot Region Stockholms informationstillgångar inom respektive nämnds och bolags ansvarsområde. *Regionstyrelsen ansvarar för fastställande av denna process.*

Ursprunglig text	Ny text
~~13.3 Incidentrapportering~~	
~~13.3.1 Då nämnder och bolag rapporterar incidenter rörande brister i informationssäkerheten till tillsynsmyndigheter i enlighet med lag ska regionstyrelsen, eller funktion med uppdrag därifrån, få information.~~	
15.1 Uppföljning av regelverket	
~~15.1.1~~ Anpassningar av Region Stockholms styrande dokument för informationssäkerhet ska ske utifrån förändringar i lagar och föreskrifter, uppdateringar av rekommendationer på området, resultat från analyser av sårbarheter och hotbild samt förändringar i verksamhet och verktyg.	Anpassningar av Region Stockholms styrande dokument för informationssäkerhet *samt dataskydd* ska ske utifrån förändringar i lagar och föreskrifter, uppdateringar av rekommendationer på området, resultat från analyser av sårbarheter och hotbild samt förändringar i verksamhet och verktyg.
15.2 Uppföljning av efterlevnad	
~~15.2.1~~ Varje nämnd och bolag ska regelbundet genomföra revision av sin informationssäkerhet och göra en analys av hur skyddsåtgärder förhåller sig till gällande styrande regelverk samt aktuell hotbild. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas, anpassas och kompletteras.	Varje nämnd och bolag ska regelbundet genomföra revision av sin informationssäkerhet *samt dataskydd* och göra en analys av hur skyddsåtgärder förhåller sig till gällande styrande regelverk samt aktuell hotbild. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas, anpassas och kompletteras.
~~15.2.2~~ Varje år ska nämnder och bolag följa upp status på informationssäkerheten inom det egna ansvarsområdet.	Varje år ska nämnder och bolag följa upp status på informationssäkerheten *samt dataskydd* inom det egna ansvarsområdet.

Ursprunglig text	Ny text
15.3 Uppföljning av händelser i it-miljön	
~~15.3.3~~ Nämnder och bolag ~~ska ha dokumenterade rutiner~~ för kontroll av medarbetares användning av it-utrustning då så är nödvändigt. ~~Rutinen ska klargöra vem som fattar beslut om sådan kontroll.~~	Nämnder och bolag *ska följa Region Stockholms process* för kontroll av medarbetares användning av it-utrustning då så är nödvändigt. *Regionstyrelsen ansvarar för fastställande av denna process.*
Begrepp	
	Dataskydd: Skydd av den personliga integriteten enligt de regelverk som ska tillämpas vid behandling av personuppgifter.
Informationstillgång: Information, och resurser som hanterar den, som är av värde för verksamheten.	Informationstillgång: Information, och resurser som hanterar den, som är av värde för verksamheten. *(Detta inkluderar även personuppgifter enligt EU:s dataskyddsförordning.)*