

Riktlinjer

Riktlinjer för informationssäkerhet

Beslutad av regionfullmäktige, den 17 november 2021

Gäller för Region Stockholm

Gäller tills vidare

INNEHÅLLSFÖRTECKNING

1.	Styrning och planering.....	3
2.	Bedömning och hantering av risker.....	5
3.	Organisation av informationssäkerheten	6
4.	Medarbetare och informationssäkerhet	8
5.	Hantering av informationstillgångar	9
6.	Åtkomst till informationstillgångar	11
7.	Kryptering	13
8.	Fysisk och miljörelaterad säkerhet	14
9.	Driftsäkerhet	15
10.	Kommunikationssäkerhet.....	17
11.	Utveckling, anskaffning och underhåll av it-system.....	18
12.	Leverantörsrelationer	19
13.	Hantering av händelser som rör informationssäkerhet	20
14.	Kontinuitetshantering.....	21
15.	Uppföljning	22
16.	Begrepp	23

1. Styrning och planering

1.1 Syfte och omfattning

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

1.1.2 För att underlätta tillämpning av regelverket ska regionstyrelsen ge ut vägledningar och råd som förtydligar hur det praktiska arbetet med att följa riktlinjerna kan gå till.

1.1.3 Riktlinjerna utgår från internationell standard avseende styrning och implementering av informationssäkerhet (ISO 27000-serien).

1.2 Region Stockholms styrande dokument för informationssäkerhet

1.2.1 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.

1.2.2 Styrdokumenten på lokal nivå består av Region Stockholms policy för verksamhetsskydd, Region Stockholms riktlinjer för informationssäkerhet, eventuella kompletterande lokala riktlinjer och anvisningar för informationssäkerhet.

1.3 Styrning

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

1.3.2 Ansvar för informationssäkerheten 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.

1.3.3 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.

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).

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

1.4 Planering

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

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.

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

2.1.1 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.

2.1.2 Riskbedömning och riskhantering ska vara en kontinuerlig process och stödja informationssäkerhetsarbetet. Riskbedömningar ska revideras när förutsättningarna väsentligen förändras.

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

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.

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

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

3.1.2 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.

3.1.3 Under regionstyrelsen ska det finnas en informationssäkerhetschef för Region Stockholm som samordnar och följer upp regionens informationssäkerhetsarbete. Informationssäkerhetschefen ska ha möjlighet att rapportera större avvikelser i arbetet med informationssäkerhet till regionstyrelsen. Informationssäkerhetschefen svarar för utbildning och stöd till informationssäkerhetssamordnare.

3.2 Roller och ansvar i nämnder och bolag

Informationssäkerhetssamordnare

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

3.2.2 Informationssäkerhetssamordnaren ska ha möjlighet att rapportera större avvikelser i arbetet med informationssäkerhet till högsta ledningen i nämnden eller bolaget.

Ägare av it-system

3.2.3 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.

3.2.4 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.

3.2.5 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.

3.2.6 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

3.3.1 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 informationssäkerhetssamordnare från varje nämnd och bolag.

3.3.2 Rådets uppgift ska vara stödjande till Region Stockholms informationssäkerhetschef. 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.

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 Sekretess

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

4.3 Utbildning och fortbildning i informationssäkerhet

4.3.1 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.

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

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.

4.4 Avslutande av anställning eller uppdrag

4.4.1 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

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

5.1.2 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

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

5.3 Hantering av informationstillgångar vid lagring och överföring

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

5.3.2 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

5.4.1 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

5.5.1 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

5.6.1 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)

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

6.1.2 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.

6.1.3 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

6.2.1 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.

6.2.2 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.

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

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

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

6.2.6 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

6.3.1 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

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

6.4.2 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, eller på uppdrag av, ägaren av det regionala nätverket. 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

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

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

7.1.3 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

8.1.1 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

8.2.1 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

8.3.1 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

9.1.1 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.

9.1.2 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

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

9.2.2 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/öppetid för att proaktivt upptäcka och åtgärda fel, minimera avbrott och förebygga andra it-incidenter.

9.3 Systemdokumentation

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

9.3.2 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

9.4.1 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.

9.4.2 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.

9.4.3 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.

9.4.4 It-system ska ha korrekt tidsangivelse.

9.4.5 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

9.5.1 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.

9.5.2 Leverantörs säkerhetsuppdateringar ska installeras skyndsamt i it-system.

9.6 Skydd mot skadlig kod

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

9.6.2 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

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

9.8 Säkerhetskopiering och återläsning av data

9.8.1 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.

9.8.2 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.

9.8.3 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

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

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

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

10.1.4 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

10.2.1 Trafik i trådlösa nätverk ska krypteras.

10.3 Specifika skyddsåtgärder i Region Stockholms regionala nätverk

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

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

10.3.3 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

10.4.1 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

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.

11.2 Systemutvecklingsprojekt

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

11.3 Test

11.3.1 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

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

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

12.1.3 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

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

12.2.2 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.

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

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

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

12.3 Riskhantering av leverantörsberoenden

12.3.1 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

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.

13.2 Analys av it-utrustning

13.2.1 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.

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

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.

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

14.1.1 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

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.

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.

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

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

15.3 Uppföljning av händelser i it-miljön

15.3.1 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.

15.3.2 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.

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.

16. Begrepp

Nedan följer förklaringar av begrepp som används i detta dokument. Begreppen utgår från ISO-standarder¹ och föreskrifter² på området.

Begrepp	Förklaring
<i>Allvarlig skada</i>	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.
<i>Autentisering</i>	Kontroll av uppgiven identitet.
<i>Behörighet</i>	Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.
<i>Fysisk säkerhet</i>	Tekniska säkerhetsåtgärder relaterade till skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten.
<i>Försumbar skada</i>	Försumbar negativ påverkan på Region Stockholm, annan myndighet eller enskilda fysiska eller juridiska personer. Motsvarar konsekvensnivå 1 i Region Stockholms riskmodell.
<i>Hot</i>	Möjlig orsak till en oönskad händelse som kan medföra negativa konsekvenser för verksamheten.
<i>Informationssäkerhet</i>	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
<i>Informationssäkerhets-händelse</i>	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".)

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
<i>Informationssäkerhets-incident</i>	Enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet.
<i>Informationstillgång</i>	Information, och resurser som hanterar den, som är av värde för verksamheten.
<i>It-system</i>	System med teknik som hanterar och utbyter information med omgivningen.
<i>It-utrustning</i>	Fysisk utrustning som hanterar och utbyter information med omgivningen.
<i>Konfidentialitet</i>	Skydd mot obehörig insyn.
<i>Kontinuitetsplanering</i>	Åtgärder för att säkerställa verksamhetens kontinuitet vid olika allvarliga störningar.
<i>Kryptering</i>	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.
<i>Ledningssystem</i>	Uppsättning av samverkande eller varandra påverkande delar av en organisation för att upprätta policyer och mål samt processer för att uppnå dessa mål.
<i>Medarbetare</i>	Alla som arbetar, eller på annat sätt deltar i verksamheten.
<i>Policy för verksamhetsskydd</i>	Dokument innehållande Region Stockholms styrande principer rörande skyddet av verksamheten.
<i>Region Stockholms regionala nätverk</i>	Nätverk som används för att sammankoppla de lokala nätverken vid nämnder och bolag.
<i>Riktighet</i>	Skydd mot oönskad förändring.
<i>Risk</i>	En sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till.
<i>Riskanalys</i>	Process för att förstå riskens natur och för att avgöra risknivån.
<i>Riskbedömning</i>	Övergripande process som innefattar delprocesserna riskidentifiering, riskanalys och riskutvärdering.
<i>Riskhantering</i>	Samordnade aktiviteter för att styra och leda en verksamhet med avseende på risk
<i>Riskidentifiering</i>	Process för att upptäcka, kartlägga och beskriva risker.

Begrepp	Förklaring
<i>Risikutvärdering</i>	Process för att jämföra resultaten från riskanalysen med riskkriterierna för att avgöra om risken och/eller dess storlek är acceptabel eller godtagbar.
<i>Riskägare</i>	Person som ansvarar för och har befogenhet att hantera en risk.
<i>Styrande regelverk</i>	Lagar, förordningar, interna styrande dokument (som t.ex. reglemente och arbetsordning) samt avtal.
<i>Sårbarhet</i>	Brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot.
<i>Säkerhetslogg</i>	Logg över säkerhetskritiska händelser.
<i>Tillgång</i>	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.)
<i>Tillgänglighet</i>	Åtkomst för behörig person vid rätt tillfälle.
<i>Åtkomstkontroll</i>	Funktioner i ett system som syftar till att reglera och kontrollera en användares åtkomst till information och resurser.