Region Stockholm

40

Yttrande över remiss Riktlinjer för informationssäkerhet

HSN 2020-0586

Hälso- och sjukvårdsnämnden
Hälso- och sjukvårdsförvaltningen
Konsulter Strategisk informationshantering
Leif Augustsson

TJÄNSTEUTLÅTANDE
2020-11-26

HSN 2020-0586

Hälso- och
sjukvårdsnämnden

Yttrande över remiss Riktlinjer för informationssäkerhet

Ärendebeskrivning

Ärendet innehåller förslag till yttrande över remitterat förslag till riktlinjer för informationssäkerhet.

Beslutsunderlag

Hälso- och sjukvårdsdirektörens tjänsteutlåtande

Remiss Riktlinjer för informationssäkerhet
Remiss PM Riktlinjer för informationssäkerhet

Förslag till beslut

Hälso- och sjukvårdsnämnden beslutar följande:

Hälso- och sjukvårdsnämnden antar hälso- och sjukvårdsdirektörens tjänsteutlåtande som nämndens yttrande och överlämnar det till regionstyrelsen.

Förvaltningens motivering till förslaget

Bakgrund

Rotel II har den 2 april remitterat förslag till Riktlinjer för informationssäkerhet för Region Stockholm. I remissen ligger att Rotel II vill ha synpunkter på förslaget. Med anledning av pandemin har den ursprungliga remisstiden förlängts till och med den 20 december 2020.

Överväganden

Hälso- och sjukvårdsförvaltningen ser positivt på förslaget. Förutom behovet av förtydliganden/uppdateringar av riktlinjerna bidrar översynen till att riktlinjerna synliggörs inom berörda nämnder och förvaltningar.

Förvaltningen har några övergripande synpunkter som följer efter nästa rubrik. Därutöver finns ett antal förslag och frågor som tas upp i tur och ordning utifrån uppställningen i förslaget.

Övergripande
Över lag är förvaltningen positiv till de nya riktlinjerna då de verkar för större möjlighet till samarbete inom regionen och mellan förvaltningarna.

Förvaltningen har inte sett några skrivningar som förvaltningen tolkar som direkt fördyrande administration. Däremot finns en oro kring formuleringar som idag ger en osäkerhet i vad effekten blir, när hänvisning finns till ännu ej publicerade men kompletterande styrande dokument, vissa fortfarande på remiss.

Avsnitt 1.1 i remissen Syfte och omfattning
1.1.1 Dessa riktlinjer konkretiserar Region Stockholms verksamhetsskyddspolicy och är styrande för informationshanteringen vid Region Stockholms samtliga nämnder och bolag.

Synpunkt:
Det är svårt att nu bedöma hur väl riktlinjerna konkretiserar en verksamhetsskyddspolicy som inte är beslutad, och även hur de senare påverkar tillämpningen av riktlinjer inom förvaltningen är därför oklart idag

Avsnitt 5.3 i remissen Hantering av informationstillgångar vid lagring och överföring
5.3.1 Informationstillgångar, som är skyddsvärda ur perspektivet konfidentialitet, ska skyddas mot obehörig åtkomst vid lagring och överföring.
5.3.2 Informationstillgångar, som kan leda till kritisk skada ur perspektivet riktighet, ska förses med skydd för att upptäcka olovlig förändring av data vid lagring och överföring.

Synpunkt:
Tillgänglighetsaspekten saknas i denna punkt (5.3) men ingår som en av informationssäkerhetens tre grundstenar.
Därför bör för tydlighetens skull en ny punkt (5.3.3) beskriva riktlinje för hur information i vila (lagring) hålls tillgänglig utifrån verksamhetskrav i teknik och genom avtal. Även hur information under transport (överföring) hanteras ska säkerställas ur tillgänglighetskrav som t.ex. acceptabel transporttid, tid till uppdatering mellan källa och mål.

Förvaltningens reflektion utifrån remissens PM där följande bedöms otydligt:

I avsnitt 1.1 Sammanfattning står:
Remissen behandlar förslag på nya riktlinjer för informationssäkerhet att ersätta nuvarande riktlinjer för informationssäkerhet. Förslaget till riktlinjer är utformade så att de till utformning och innehåll harmonierar med beslutad inriktning för integrerad ledning och styrning i Region Stockholm budget. Remissen är ett led i beredningen av ärendet om riktlinjer för informationssäkerhet inom Region Stockholm, avsett att beslutas om i regionfullmäktige den 17–18 november 2020.

Synpunkt:
Oklart på vilket vis beslutad inritning i budget påverkat utformningen av riktlinjerna. Huruvida den nu mer harmonierade integrerade ledningen påverkar tillämpningen av riktlinjerna går inte att urskilja. Påverkas budget eller mandat inom förvaltningen av detta så bör det tydligt framgå. Det bör även tydliggöras om ett större engagemang i gemensamma frågor finns att vänta från regionledningen framåt.

I avsnitt 1.2 Bakgrund står:
I samband med att riktlinjerna fastställs kommer regionledningskontoret att tillgängliggöra en vägledning som tydliggöra bakgrund och ger förslag på hantering av punkterna in riktlinjerna.

Synpunkt:
Texten ovan skapar en osäkerhet avseende i vilken omfattning den ej tillgängliga vägledningen kommer påverka lokal tillämpning av riktlinjer och utformning av handlingsplan.
Men precis som PM deklarerar så ser förvaltningen en besparing i att dubbelarbetet med lokalt styrande dokument nu minskar i omfattning.

Ekonomiska konsekvenser
Förslaget i sig innebär inte några ekonomiska konsekvenser men efterlevnad av riktlinjerna leder till delvis ändrade arbetssätt och behöver tas hänsyn till i handlingsplan framåt.

Konsekvenser för patientsäkerhet
Förslaget får möjligen positiva konsekvenser för patientsäkerheten.

Konsekvenser för jämlik och jämställd vård
Förslaget innebär oförändrade konsekvenser för jämlik och jämställd vård.

Miljökonsekvenser
Förslaget innebär oförändrade konsekvenser för miljön.

Administrativa konsekvenser
Förslaget innebär i sig inga administrativa konsekvenser för vårdgivare. Dock innebär de ett visst initialt arbete i omformulering av avtalstexter mm. men det bedöms idag inte som extraordinärt

Björn Eriksson
Hälso- och sjukvårdsdirektör

Johan Bratt
Avdelningschef

Beslutet ska skickas till
Regionstyrelsen

Godkänd av Björn Eriksson, 2020-11-26

Diarienummer
RS 2020-0148

Remiss - Riktlinjer

Riktlinjer för informationssäkerhet

Gäller för Region Stockholm

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

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 18
11. Utveckling, anskaffning och underhåll av it-system 19
12. Leverantörsrelationer 20
13. Hantering av händelser som rör informationssäkerhet 21
14. Kontinuitetshantering 22
15. Uppföljning 23
16. Begrepp 24

1. Styrning och planering

1.1 Syfte och omfattning

1.1.1 Dessa riktlinjer konkretiserar Region Stockholms verksamhetsskyddspolicy och är styrande för informationshanteringen vid Region Stockholms samtliga nämnder och bolag.

1.1.2 För att underlätta tillämpning av regelverket kan 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 verksamhetsskyddspolicy, Region Stockholms riktlinjer för informationssäkerhet, eventuella kompletterande lokala riktlinjer och anvisningar för informationssäkerhet.

1.3 Styrning

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

1.3.2 Ansvaret 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 bedrivas 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. Regionstyrelsen ansvarar för regionövergripande styrande dokument.

3.1.2 Regionstyrelsen har mandat att fatta beslut i frågor som rör regionövergripande informations- och it-säkerhet samt operativa beslut som bedöms nödvändiga för att i akuta situationer skydda regionens informationstillgångar, samt för att utreda incidenter inom området.

3.1.3 Regionstyrelsen ska ha 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.

3.2.3 Informationssäkerhetssamordnare ska lämna sådan information till informationssäkerhetschefen som avses i 3.1.3 då regionstyrelsen efterfrågar detta.

Ägare av it-system

3.2.4 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.

3.2.5 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.

3.2.6 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.

3.2.7 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.

Informationsanvändare

3.2.8 Informationsanvändare är samtliga personer som i sin yrkesutövning hanterar information inom Region Stockholm, vilket inkluderar såväl anställda som andra användare. Informationsanvändarnas medverkan är väsentlig för en effektiv informationssäkerhet. De ska göras medvetna om sin skyldighet att ta del av och följa uppställda informationssäkerhetsregler liksom att rapportera informationssäkerhetshändelser enligt fastställda rutiner.

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 anställning eller annat deltagande i verksamheten påbörjas 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 på ett sådant sätt att offentlighets- och sekretesslagen inte blir tillämplig.

4.3 Utbildning och fortbildning i informationssäkerhet

4.3.1 Nämnder och bolag ansvarar för att medarbetare får den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter och för att säkerställa säker hantering av de informationstillgångar som medarbetaren kommer i kontakt med. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen.

4.3.2 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

I detta kapitel finns det riktlinjer för hur informationstillgångar ska hanteras. Sekretessbelagda uppgifter och personuppgifter är exempel på känslig information som måste hanteras på särskilt sätt.

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 informations-tillgångarna ska utformas så att efterlevnad av styrande regelverk uppnås samt med hänsyn till nämnders och bolags risktolerans.

5.2 Märkning av sekretessbelagd information

5.2.1 Märkning av information som bedöms kunna omfattas av sekretess ska ske vid informationsdelning. Detta ska gälla för information i såväl fysisk som elektronisk form.

5.3 Hantering av informationstillgångar vid lagring och överföring

5.3.1 Informationstillgångar, som är skyddsvärda ur perspektivet konfidentialitet, ska skyddas mot obehörig åtkomst vid lagring och överföring.

5.3.2 Informationstillgångar, som kan leda till kritisk skada ur perspektivet riktighet, ska förses med skydd för att upptäcka olovlig förändring av data vid lagring och överföring.

5.4 Hantering av it-utrustning

5.4.1 Nämnder och bolag ansvarar för att det finns en uppdaterad inventarieförteckning över all teknisk utrustning som har förmågan att lagra eller bearbeta information.

5.5 Hantering av lagringsmedium

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 den ordinarie arbetsplatsen.

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 system.

6.1.2 Ägare av it-system ansvarar för att system som hanterar information som kan leda till kritisk skada ur perspektiven riktighet, tillgänglighet och konfidentialitet, 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 den lösning som den regionala nätägaren tillhandahåller. 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 informationen via den inloggningen på utrustningen.

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

6.3.2 Innan icke-digital information överlämnas ska mottagaren informeras om hur informationen ska hanteras och förvaras.

6.4 Avstängning av åtkomst

6.4.1 Medarbetares tillgång till it-system får stängas av vid misstanke om brott mot lag eller interna styrande dokument. Beslut om sådan avstängning ska fattas av nämnd eller bolag, eller person med delegation därifrån.

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

6.4.3 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

7.1.1 Vid kryptering av information ska algoritmer och nyckellängder som bedöms pålitliga 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 Utformningen av det fysiska skyddet av informationstillgångar ska baseras på genomförda riskanalyser och vara dimensionerat utifrån tillgångarnas värde, identifierade risker och styrande regelverk.

8.1.2 Nämnder och bolag som ansvarar för förvaring av informationstillgångar ansvarar även för det fysiska skyddet för dessa. I fråga om förvaring av it-system och nätverk är det ägaren som ansvarar för förvaringen och därmed för det fysiska skyddet.

8.2 Skalskydd och tillträdeskontroll

8.2.1 Fysiska avgränsningar ska användas för att skydda utrymmen som innehåller informationstillgångar.

8.2.2 Utrymmen där informationstillgångar förvaras eller bearbetas ska skyddas genom lämpliga säkerhetsåtgärder för att säkerställa att endast behöriga medarbetare får tillträde till informationstillgångarna.

8.2.3 För förvaring av informationstillgångar som kan leda till kritisk skada ur perspektiven riktighet, tillgänglighet och konfidentialitet ska tillträdet till utrymmet loggas.

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 Produktionsdata som är skyddsvärda ur perspektivet konfidentialitet ska inte användas under test och utveckling av it-miljön.

9.1.2 Produktionsdata som är skyddsvärda ur perspektivet konfidentialitet ska inte användas i utbildningsmiljö om inte utbildningsmiljön har samma skydd som produktionsmiljön.

9.1.3 Tester av it-miljön ska riskhanteras och ska inte introducera risker som kan leda till kritisk 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 är verksamhetskritiska ur perspektiven riktighet, tillgänglighet och konfidentialitet 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

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

9.3.3 Ägaren av ett it-system ansvarar för att användarna får information om att händelser i it-systemet loggas.

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 Säkerhetsloggar ska sparas i minst sex månader.

9.4.6 Säkerhetsloggar ska sparas i minst fem år då informationen kan leda till kritisk skada.

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 riskbild för informationen.

10. Kommunikationssäkerhet

En viktig förutsättning för att skydda Region Stockholms it-system är att det finns bra skyddsåtgärder i nätverken samt kontroll på sådan kommunikation som går in i och ut från 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 tillhandahållen och kontrollerad 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 informationstillgångar som leverantören kommer att hantera.

12.1.2 Kraven som ställs i samband med anskaffning ska säkerställa skyddet för de informationstillgångar som leverantören 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 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.

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 motsvarande 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-standarder[1] och förskrifter[2] på området.

Begrepp	**Förklaring**
Autentisering	Kontroll av uppgiven identitet.
Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.
Fysisk säkerhet	Tekniska säkerhetsåtgärder relaterade till skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten.
Hot	Möjlig orsak till en oönskad händelse som kan medföra negativa konsekvenser för verksamheten.
Informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
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.
IT-system	System med teknik som hanterar och utbyter information med omgivningen.
Konfidentialitet	Skydd mot obehörig insyn.
Kontinuitetsplanering	Åtgärder för att säkerställa verksamhetens kontinuitet vid olika allvarliga störningar.

[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**
Kritisk skada	Betydande negativ påverkan för Region Stockholm, annan myndighet eller enskilda fysiska eller juridiska personer. (Kan t.ex. handla om att sekretessbelagda uppgifter eller känsliga personuppgifter röjs till obehörig; att ett sjukhus inte kan leverera en viss typ av vård eller att en tunnelbanelinje har stora störningar.) Betydande negativ förtroendepåverkan för Region Stockholm.
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.
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.
Riskbedömning	Övergripande process som innefattar delprocesserna riskidentifiering, riskanalys och riskutvärdering.
Riskbehandling	Process för att förändra risker.
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.

Begrepp	**Förklaring**
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.
Verksamhetsskydds-policy	Dokument innehållande Region Stockholms styrande principer rörande skyddet av verksamheten,

[redacted]

Regionledningskontoret

PM
2020-03-24

RS 2020-0148

Riktlinjer för informationssäkerhet

Remiss-PM

PM
2020-03-24 RS 2020-0148

Innehållsförteckning

1. Regionledningskontorets förslag och motivering 3
1.1 Sammanfattning 3
1.2 Bakgrund 3

2. Sammanfattning av förändringar 3
2.1 Arbetsprocess och förankring 4
2.2 Ekonomiska konsekvenser 4

1. Regionledningskontorets förslag och motivering

1.1 Sammanfattning

Remissen behandlar förslag på nya riktlinjer för informationssäkerhet att ersätta nuvarande riktlinjer för informationssäkerhet. Förslaget till riktlinjer är utformade så att de till utformning och innehåll harmonierar med beslutad inriktning för integrerad ledning och styrning i Region Stockholm budget. Remissen är ett led i beredningen av ärendet om riktlinjer för informationssäkerhet inom Region Stockholm, avsett att beslutas om i regionfullmäktige den 17–18 november 2020.

1.2 Bakgrund

Det finns behov av att uppdatera nuvarande riktlinjer för informationssäkerhet inom Region Stockholm.

Nuvarande riktlinjer för informationssäkerhet är: LS 2018-0652 Riktlinjer för informationssäkerhet. Med anledning av inriktningen i Region Stockholms budget avseende styrning och ledning finns behov av att minska administrativ överbyggnad och detaljstyrningen i möjligaste mån. Det innebär exempelvis behov att ta bort sådana bestämmelser i nuvarande riktlinjer som ställer krav på lokala styrande dokument där sådana kan tas fram centralt. Dessutom är ambitionen med föreslagna förändringar att förenkla tillämpning och tolkning av bestämmelserna kring informationssäkerhet samt att ta bort upprepning av krav som redan regleras i lag.

I samband med att riktlinjerna fastställs kommer Regionledningskontoret att tillgängliggöra en vägledning som tydliggöra bakgrund och ger förslag på hantering av punkterna in riktlinjerna.

2. Sammanfattning av förändringar

Ambitionen är att styrningen i riktlinjerna ska vara i enlighet med det som anges i standarderna för informationssäkerhet[1].
Ett antal bestämmelser tas bort då de innehåller upprepningar av sådant som står i andra styrande dokument. Det handlar t.ex. om bestämmelser i EU:s dataskyddsförordning, patientdatalagen och säkerhetsskyddslagen.

Ett antal bestämmelser tas bort och kommer istället att hanteras i dokumentet Uppförandekod för Region Stockholm samt genom utbildning.

[1] Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Översikt och terminologi (ISO/IEC 27000:2018)
Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav (ISO/IEC 27001:2013 med Cor 1:2014 and Cor 2:2015)
Informationsteknik - Säkerhetstekniker - Riktlinjer för Informationssäkerhetsåtgärder (ISO/IEC 27002:2013 med Cor 1:2014 and Cor 2:2015)

I enlighet med inriktningen i Region Stockholm budget tas ett antal bestämmelser bort då de är av konkretiserande karaktär och därför bättre hanteras i vägledningar för informationssäkerhetsområdet.

Begreppet informationsägare tas bort då begreppet har bidragit till att skapa ökad otydlighet snarare än nyttor. Det som rollen ursprungligen var avsedd att hantera täcks istället av bestämmelsen [3.1.1] att ”varje person som är ansvarig för en verksamhet, eller får ett delegerat verksamhetsansvar, också är ansvarig för informationssäkerheten i denna verksamhet”.

I syfte att förenkla för verksamheten har modell för informations-klassificering inom Region Stockholm ersätts med krav att istället värdera information utifrån en förtida skadebedömning.

Kravet på att förteckna information har tagits bort då detta anses täckas av Region Stockholms modell för att redovisa handlingar/information, verksamhetsbaserad informationsredovisning (VIR) samt genom lagkraven på diarieföring och på förteckning av personuppgiftbehandlingar.

2.1 Arbetsprocess och förankring

Arbetet med översynen av riktlinjerna för informationssäkerhet har skett tillsammans med informationssäkerhetssamordnare vid nämnder och bolag inom Region Stockholm. Samråd har även skett med Ekonomi och finans, Strategiskt inköp, Strategisk HR, Juridik samt Säkerhet och Beredskap, regelefterlevnad inom Regionledningskontoret, liksom med Regionarkivet.

2.2 Ekonomiska konsekvenser

Förslaget på riktlinjer bedöms inte medföra några utökade kostnader jämfört med regleringar i nuvarande riktlinjer. Vissa besparingar bedöms kunna uppstå då administrativt dubbelarbete minskar. Ett väl etablerat systematiskt arbete med informationssäkerhet innebär på sikt betydande kostnadsbesparingar genom minskade kostnader för hantering av it-säkerhetsrelaterade incidenter och verksamhetsstörningar.