Regiondirektören

Alf Jönsson
alf.jonsson@skane.se

BESLUT

Datum: 2020-05-22
Dnr: 1800025

Instruktion för tillämpning av riktlinjer för informationssäkerhet

Instruktionen utgår från riktlinjer för informationssäkerhet[1] som Regionstyrelsen beslutat om. Instruktionen anger hur riktlinjernas krav ska tillämpas med utgångspunkt i den standard för informationssäkerhet som Region Skåne följer, SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002. Instruktionens krav är övergripande och uppföljningsbara och för det praktiska genomförandet kompletteras denna instruktion med ytterligare instruktioner och handledningar inom specifika områden.
Instruktionen är en del i att nå de mål för informationssäkerheten som Regionfullmäktige och Regionstyrelsen beslutat om och slår bland annat fast organisation, roller och ansvar och övergripande skyddsåtgärder.

Härmed beslutas att:

- Instruktion för tillämpning av riktlinjer för informationssäkerhet fastställs.
- Beslut om ”Förslag till organisation för informationssäkerhetsarbetet i Region Skåne”, daterad 2009-12-21 med diarienummer 0900521 upphör att gälla.
- Beslut med rubrik ”Förtydligande av organisation för informationssäkerhet” daterad 2010-06-23 upphör att gälla.
- Beslut om ”Ledningssystem för informationssäkerhet i Region Skåne”, daterad 2011-05-24 upphör att gälla.
- Beslut om ”Regelverk för användning av IT-baserade verktyg i Region Skåne”, daterad 2016-12-08, dnr 1603091 upphör att gälla.
- Informationssäkerhetschefen har mandat att uppdatera instruktionen och genomföra ändringar som endast innebär mindre påverkan.

Alf Jönsson

---

[1] Beslutad av Regionstyrelsen 2017-12-07, dnr 1604263

Innehållsförteckning

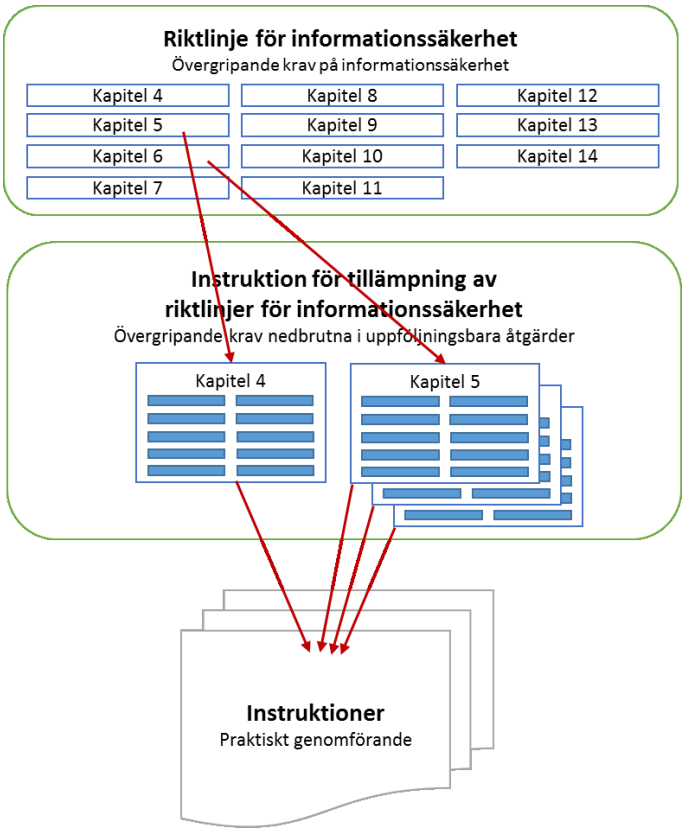
Ändringslogg

Datum	Ändrad av	Förändring
2018-12-18	Johan Reuterhäll	Uppdaterat kapitel 12.3 och kompletterat med kontrollåtgärder som rör e-post och hemmakataloger som tidigare fanns i RD-beslut ” Regelverk för användning av IT-baserade verktyg i Region Skåne”.
2020-05-22	Johan Reuterhäll	5.2.2. om samverkan tas bort eftersom RD fattat särskilt beslut om detta. 12.1.9 Tillägg angående e-post i tjänsten. I övrigt mindre uppdateringar av text.

1 Inledning och syfte

Syftet med instruktionen är att specificera vilka övergripande säkerhetsåtgärder som ska vidtas inom de områden som standarden för ledningssystem för informationssäkerhet, SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002, omfattar.
Standarden anger övergripande vilka skyddsåtgärder som ska finnas men Region Skåne behöver anpassa detta till sin egen verksamhet och finna en lämplig nivå utifrån organisationens förutsättningar. Region Skåne är i detta avseende en mycket stor organisation med skiftande verksamhet där kraven på skydd av information skiljer sig åt mellan de olika verksamheterna.

Instruktionens krav är uppföljningsbara och ska ligga till grund för den uppföljning som ska göras både centralt och inom varje förvaltning. Instruktionens krav konkretiseras genom ytterligare instruktioner och handledningar. Se nedan bild.



2 Mål

Målet är att höja kvaliteten i Region Skånes informationshantering och skapa förutsättningar för enhetliga arbetssätt för att nå de mål för informationssäkerhet som Regionfullmäktige och Regionstyrelsen beslutat om.

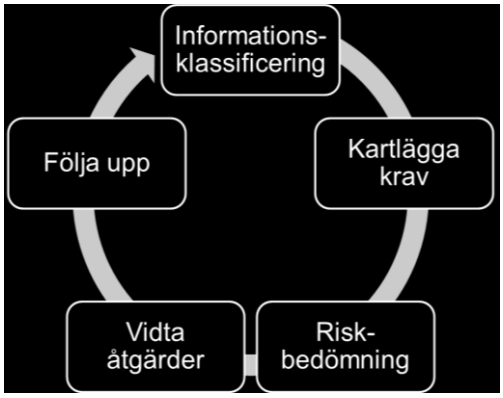
3 Omfattning

Instruktionen ska efterlevas av samtliga förvaltningar. Instruktionen gäller även i vissa delar de som arbetar på uppdrag av Region Skåne som

exempelvis privata vårdgivare och konsulter som Region Skåne tecknat avtal med.

4 Övergripande process

Processen visar övergripande de olika delarna för att uppnå en god informationssäkerhet. I processens olika steg deltar flera delar av organisationen.



4.1 Övergripande styrdokument

Säkerhetspolicyn[2] beskriver Region Skånes syn på säkerhetsarbetet och de övergripande principer som gäller. Säkerhetspolicyn beslutas av Regionfullmäktige.

Riktlinje för informationssäkerhet konkretiserar säkerhetspolicyn avseende grundläggande delar inom informationssäkerhet. Riktlinjen beslutas av Regionstyrelsen.

Instruktioner och anvisningar för informationssäkerhet anger hur arbetet ska bedrivas utifrån säkerhetspolicy och riktlinjerna. Instruktioner och anvisningar beslutas av Regiondirektören.

5 Roller och ansvar

I enlighet med vad som gäller för övrig verksamhet, är ansvaret för informationssäkerheten kopplat till det delegerade verksamhetsansvaret. Det innebär att varje anställd som är ansvarig för en verksamhet eller får ett delegerat verksamhetsansvar också är ansvarig för att informationssäkerheten upprätthålls och efterföljs i denna verksamhet. Utöver ovan har nedan roller ett särskilt ansvar.

5.1 Roller och ansvar i tjänstemannaorganisationen

5.1.1 Regiondirektör

Beslutar om regionövergripande instruktioner och anvisningar.

---

[2] Regionfullmäktige 2017-06-20, § 56, dnr 1701090

Beslutar om informationsägare för regiongemensamma informationstillgångar

5.1.2 Förvaltningschef

Förvaltningschef har, inom sin förvaltning, ansvaret för att utforma och kommunicera innehållet i styrande dokument för informationssäkerhet, verkställa och följa upp beslut samt ansvara för att all informationshantering sker i enlighet med fastställda styrande dokument.
Förvaltningschef ska inom sin förvaltning utse informationssäkerhetssamordnare som har ett tydligt mandat och uppdrag att leda, samordna och följa upp förvaltningens informationssäkerhetsarbete.

5.1.3 Informationsägare

Informationsägaren har ansvar för informationstillgångar och beslutar om informationshantering inom ramen för befintlig lagstiftning och interna regelverk. Informationsägarens ansvar beskrivs i särskilt beslut[3] om informationsägare.
Informationsägare som inte är förvaltningschef ska inom sin organisation utse informationssäkerhetssamordnare.

5.1.4 Systemägare

Systemägare har det övergripande ansvaret för system. System kan innehålla information som tillhör en eller flera informationsägare.
Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.
Systemägares ansvar finns i bilaga 1.

5.1.5 Informationssäkerhetssamordnare

Informationssäkerhetssamordnare ska leda, utveckla, samordna och följa upp informationssäkerhetsarbetet utifrån regionövergripande styrande dokument.
Informationssäkerhetssamordnares ansvar finns i bilaga 1.

5.1.6 Organisation för informationssäkerhet

Inom respektive förvaltning ska finnas en organisation som hanterar frågor om informationssäkerhet inklusive dataskydd. Förvaltningen ska avsätta tillräckligt med resurser för att arbetet ska kunna bedrivas effektivt.
Storleken på organisationen avgörs utifrån förvaltningens storlek samt mängden och känsligheten i den information som hanteras.
Det är av vikt att organisationen för informationssäkerhet har koppling till ledningen i förvaltningen för effektiv rapportering och eventuella beslut om åtgärder.
Se även beslut[4] av Regiondirektören rörande dataskyddsorganisation.

---

[3] Beslut om informationsägare, daterat 2018-05-22, dnr 1800025
[4] Beslut om dataskyddsorganisation i Region Skåne, dnr 1800025, daterat 2018-05-31

5.1.7 **Informationsanvändare**

Informationsanvändare är samtliga personer som i sin yrkesutövning hanterar information i Region Skåne, vilket inkluderar såväl anställda som andra användare. Informationsanvändarnas medverkan och engagemang är väsentligt för en effektiv informationssäkerhet. De ska vara medvetna om sin skyldighet att ta del av och följa beslut liksom att rapportera informationssäkerhetsincidenter.

5.2 Samordning och uppföljning

5.2.1 **Informationssäkerhetsråd**

Det ska finnas ett informationssäkerhetsråd som har till uppgift att stödja, samordna och följa upp Region Skånes informationssäkerhetsarbete på en övergripande nivå. Rådet ska främja erfarenhets- och kunskapsutbyte, bevaka vilket behov av stöd som finns i verksamheterna och föreslå förbättringar, förankra och samordna viktiga informationssäkerhetsaktiviteter samt följa upp efterlevnaden av Region Skånes riktlinjer för informationssäkerhet.
Utöver informationssäkerhetschefen ska rådet bestå av informationssäkerhetssamordnare från respektive förvaltning. För att främja ett enhetligt arbete, kunskapsutbyte och synkronisering av insatser ska även dataskyddsombudets representanter delta vid behov.
Informationssäkerhetsrådet leds av informationssäkerhetschefen.

6 Utbildning

Utbildning krävs för ett framgångsrikt och effektivt informationssäkerhetsarbete. Ett högt säkerhetsmedvetande hos personalen med aktuella kunskaper om lagar och regler och hur informationen ska skyddas är det mest effektiva sättet att skydda informationen. Därför ska utbildning vara en högprioriterad del av informationssäkerhetsarbetet. Vid utbildningar av chefer och medarbetare, vare sig det är för nyanställda eller redan anställda ska utrymme ges för att informera om informationssäkerhet. Informationssäkerhetssamordnarna har en viktig roll i genomförandet av detta inom varje förvaltning. Utbildningarna ska anpassas efter målgruppen. Det ska även finnas e-utbildningar i den utsträckning som är lämplig med avseende på målgrupper med olika arbetsuppgifter och arbetsområden. Genomförande av utbildningar ska samordnas mellan de expertfunktioner som påverkar kraven på informationshantering mest, d.v.s. regionarkivarien, dataskyddsombudet och informationssäkerhetschefen.

7 Externa leverantörer

Om Region Skåne använder externa leverantörer ska skriftligt avtal reglera nödvändiga roller och kontaktytor som möjliggör för Region Skåne att styra och följa upp leverantörens informationssäkerhetsarbete och efterlevnad av informationssäkerhetskrav. Med externa leverantörer avses även andra regioner. Här ska särskilt noteras skyldigheten enligt dataskyddsförordningen att ha ett s.k. personuppgiftsbiträdesavtal när en part behandlar personuppgifter på uppdrag av en annan part vilka ofta är

fallet när det handlar om externa leverantörer som lagrar eller behandlar Region Skånes information.
Se även Regiondirektörens beslut om Instruktion för Region Skånes behandling av personuppgifter[5].

8 Bedömning och hantering av risker

I takt med att omvärlden och den interna verksamheten förändras så förändras även behovet av skyddsåtgärder. Region Skåne behöver därför ha god kunskap om de hot, risker och sårbarheter som påverkar oss eller som kan komma att påverka oss. Detta åstadkoms genom omvärldsanalys och genom att arbeta systematiskt med riskbedömningar.
Region Skånes arbete med riskbedömningar regleras bland annat i

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Dataskyddsförordningen
- Säkerhetsskyddslag (2018:585)
- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
- Myndigheten för samhällsskydd och beredskaps föreskrifter om landstings risk- och sårbarhetsanalyser (MSBFS 2015:4)
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

8.1.1 Varje verksamhet ska genomföra och dokumentera analyser avseende vilka risker som kan påverka informationssäkerheten, och utifrån dessa analyser vidta lämpliga skyddsåtgärder.

8.1.2 Riskbedömning ska, om inte särskilda skäl föreligger, ske med delprocesserna riskidentifiering, riskanalys samt riskutvärdering och genomföras i enlighet med gällande instruktioner för genomförande av riskbedömningar inom informationssäkerhet.

8.1.3 För varje risk som identifieras under riskbedömningen ska ett riskhanteringsbeslut fattas. Riskhanteringsbeslut som innebär att risk inte kan godtas ska leda till åtgärdsplan för att minska risken till godtagbar nivå.

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

8.1.5 Genomförd informationsklassificering, riskbedömning och riskhanteringsbeslut ska lagras på plats som anvisas av informationssäkerhetschefen.

---

[5] Diarienummer 1800025, daterad 2018-06-25

9 Övergripande informationssäkerhetsåtgärder

Riktlinjen utgår från standarden för informationssäkerhet SS-ISO/IEC 27002. Från kapitel 10 redovisas övergripande skyddsåtgärder med utgångspunkt i ”SS-ISO/IEC 27002 – Riktlinjer för informationssäkerhetsåtgärder”.

10 Personalsäkerhet

10.1 Före anställning

10.1.1 Arbetssökandes formella meriter (såsom utbildning, yrkeslegitimation, referenser etc.) ska kontrolleras och den arbetssökandes identitet ska verifieras. Vid rekrytering till särskilt informationssäkerhetskritiska arbetsuppgifter ska fler och mer detaljerade kontroller övervägas.

10.1.2 Innan anställning eller annat deltagande i verksamhet som innebär tillgång till sekretessbelagda uppgifter med betydelse för Sveriges säkerhet ska säkerhetsprövning med registerkontroll göras. Säkerhetsskyddschefen ska i dessa fall kontaktas.

10.2 Under anställning

10.2.1 Anställda ska i samband med rekrytering samt kontinuerligt under anställningstiden göras medvetna om sitt ansvar för informationssäkerhet och tillämpliga lagkrav, t.ex. beträffande allmänna handlingar och sekretess.

10.2.2 Anställda ska göras medvetna om att bristande efterlevnad av gällande regler för informationssäkerhet och sekretess kan utgöra brott, både mot gällande lagstiftning samt mot anställningsavtalet. Ytterst kan detta leda till uppsägning eller avsked.

10.3 Sekretess

10.3.1 I det fall information som omfattas av sekretess ska hanteras av anställda ska erinran om sekretess ske där medarbetaren informeras om vilka skyldigheter som följer av lag.

10.3.2 Sekretessen omfattar inte enbart den som är anställd av Region Skåne eller dess bolag. Vid anlitande av konsult eller annan extern uppdragstagare ska det klargöras om han eller hon deltar i verksamheten på samma sätt som en anställd i Region Skåne.

10.3.3 Deltar personen inte i verksamheten på sådant sätt att offentlighets- och sekretesslagen blir tillämplig, ska tystnadsplikten regleras civilrättsligt, det vill säga i avtal samt informeras om konsekvenser av bristande efterlevnad.

10.4 Utbildning

10.4.1 Anställda inom Region Skåne ska få den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Detsamma gäller även vid förflyttning och

omplacering av redan anställda och när tillfällig personal och externa konsulter anlitas.

10.4.2 Anställda ska minst ha genomgått den grundläggande e-utbildningen i informationssäkerhet.

10.5 Avslut eller ändring av anställning

10.5.1 Det ska finnas en fastställd rutin för hantering av personal som avslutar sin anställning. Rutinen ska säkerställa att ansvarsuppgifter avlämnas och att åtkomsträttigheter upphör vid anställningens slut.

11 Hantering av tillgångar

11.1 Förteckning över viktiga informationstillgångar

11.1.1 Respektive chef ska ha en förteckning över viktiga informationstillgångar inom sin verksamhet.

11.2 Klassificering av information

11.2.1 Respektive informationstillgång ska tilldelas en informationssäkerhetsklass som motsvarar dess betydelse för den aktuella verksamheten och de legala krav som finns.

11.2.2 Vid informationsklassificering ska Region Skånes gällande informationsklassificeringsmodell användas.

11.2.3 Informationsklassificering ska baseras på säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet. Nivåbestämningen ska utgå från de konsekvenser som obehörig åtkomst, bristande riktighet och bristande tillgänglighet till informationstillgång ger upphov till.

11.3 Märkning av information

11.3.1 Märkning av information är en förutsättning för att information ska hanteras rätt vid informationsdelning. Märkning av information ska ske med utgångspunkt i Region Skånes informationsklassificeringsmodell[6]. Detta ska gälla för information i såväl fysisk som elektronisk form.

11.4 Hantering av information som omfattas av sekretess

En offentlig verksamhets informationshantering styrs av ett omfattande regelverk, däribland grundlagarna.

---

[6] Se RD-beslut om Instruktion för informationsklassificering, 2018-10-15

Alla handlingar som upprättas eller inkommer till en myndighet är i princip allmänna och normalt offentliga och ska vara tillgängliga för allmänheten. Det finns dock allmänna handlingar där uppgifter sekretessmarkerats och som behöver hanteras på säkert sätt.

11.4.1 Det ska finnas styrande dokument för utlämnande av information. I dessa ska det framgå vem eller vilka som har rätt att fatta beslut om ett utlämnande och vem som fattar beslut om att inte lämna ut en allmän handling.

11.4.2 Det ska finnas styrande dokument som reglerar på vilket sätt säkerhetsskyddsklassificerade uppgifter och handlingar som omfattas av säkerhetsskyddslagen praktiskt ska hanteras.

11.5 Personuppgifter

11.5.1 Om personuppgifter behandlas omfattas behandlingen av dataskyddsförordningen. Innan behandling av personuppgifter får ske kan särskilda skyddskrav behöva vidtas. Vilka kraven är ska avgöras med stöd av underlag från informationsklassificering och genomförande av konsekvensbedömning (DPIA).

11.6 Skyddade personuppgifter

Skyddade personuppgifter innebär att personer som lever under hot får ett ökat skydd. Det finns tre typer av skyddsåtgärder i folkbokföringen; sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter.

11.6.1 Alla personer ska kunna känna sig trygga med att deras personuppgifter inte kommer i orätta händer. Informationsutbyte, elektronisk eller icke-elektronisk, får inte leda till att skyddade uppgifter röjs.

11.6.2 Det ska finnas styrande dokument som reglerar hur skyddade personuppgifter ska hanteras.

11.6.3 Personuppgifter som är skyddade ska vara tydligt märkta så att detta framgår för personer som hanterar dem.

11.6.4 Vid utveckling och förvaltning av informationssystem ska hantering av skyddade personuppgifter beaktas särskilt. Informationssystem ska utformas så att endast de som har behov får tillgång till sådana uppgifter.

11.7 Sammanställning och analys

11.7.1 Vid sammanställning och analys av stora mängder personuppgifter inom hälso- och sjukvården ska informationsklassificering och riskanalys alltid genomföras och dokumenteras. Den information som sammanställs och analyseras liksom den information som blir resultat av den ska ha tillräckligt skydd från insamling till färdigt

resultat. Informationsägare fattar beslut om hur informationen ska hanteras. Beslutet ska dokumenteras.

11.8 Hantering av lagringsmedia

Med lagringsmedia avses media där information finns. Det kan röra sig om hårddiskar, papper, USB-minnen, minneskort m.m. Vid förvaring och transport av lagringsmedia ska skyddet motsvara det skyddsvärde som informationen har utifrån den informationsklassificering som genomförts.

11.8.1 Lagringsmedia som innehåller skyddsvärd information ska skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport.

11.8.2 Om transport av lagringsmedia sker med transportföretag ska sådana åtgärder vidtas som skyddar informationen och som säkerställer att endast rätt mottagare kan ta emot lagringsmediet.

11.8.3 När fasta eller löstagbara lagringsmedier som innehåller eller kan innehålla personuppgifter, information som omfattas av sekretess eller av andra anledningar kan vara känslig ska gallras, utrangeras, kasseras, säljas eller på annat sätt lämna verksamheten ska lagringsmedierna förstöras alternativt raderas på ett sådant sätt att uppgifterna inte kan återskapas. Detta gäller även om informationen är krypterad.

11.8.4 För hantering av lagringsmedia som innehåller säkerhetsskyddsklassificerade uppgifter finns särskilda hanteringsregler som ska följas. Säkerhetsskyddschefen ska kontaktas om osäkerhet råder kring hanteringen.

12 Användning av informationssystem

12.1 Generella regler

Med godkänd utrustning och godkända tjänster nedan avses sådan utrustning och sådana tjänster som godkänts av informationsägare eller systemägare.

12.1.1 Region Skånes resurser (datorer, mobila enheter, nätverk och kringutrustning) är avsedda att användas som arbetsredskap vid tjänsteutövning. Privat användning är tillåten i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga risker eller kostnader för Region Skåne.

12.1.2 Information ska sparas på anvisad plats. För information som omfattas av sekretess finns särskilda krav på skydd och endast godkända tjänster och lagringsytor får användas. Detta gäller även säkerhetskopior.

12.1.3 Till Region Skånes nätverk, datorer, mobila enheter får användare endast ansluta utrustning som godkänts.

12.1.4 Information som rör Region Skånes verksamhet ska som regel bearbetas och lagras med hjälp av informationssystem som godkänts av Region Skåne.

12.1.5 Vilken slags information som får bearbetas, lagras, eller kommuniceras i ett system ska framgå av systemdokumentationen för systemet.

12.1.6 Informationssystemens skyddsmekanismer och säkerhetsprogramvaror ska hållas uppdaterade och får inte kringgås eller inaktiveras.

12.1.7 Användare ska hantera utrustning på ett sätt som minimerar risken för att obehöriga får tillgång till utrustningen, att den stjäls eller går förlorad på annat sätt.

12.1.8 Användare får endast installera och använda programvaror eller system som godkänts av Region Skåne.

12.1.9 Privata e-postadresser får inte användas i yrkesutövningen. I yrkesutövningen ska e-postadress som tilldelats i tjänsten användas.

12.1.10 Patientuppgifter, känsliga personuppgifter och annan information som omfattas av sekretess eller i övrigt är skyddsvärd får inte skickas via e-post, internt eller externt, utan godkänd kryptering.

12.2 Användaridentiteter, lösenord och e-tjänstekort

12.2.1 Användaridentiteter, lösenord och e-tjänstekort är personliga och får inte lånas ut.

12.2.2 Användare ansvarar för att användaruppgifter (till exempel lösenord och pin-kod) inte blir kända för andra. I de fall användaruppgifter blir kända för andra ansvarar användaren för att de utan dröjsmål byts i aktuellt system.

12.2.3 Vid misstanke om att ett lösenord eller pin-kod blivit känd för andra ska lösenordet eller pin-koden ändras. Om ett e-tjänstekort tappats bort ska det omgående rapporteras så att det kan spärras och bytas ut.

12.3 Kontrollåtgärder

12.3.1 Information om vad som sker i it-system och på användares dator loggas. Loggning görs för driftövervakning och felsökning men kan även göras för uppföljning av att interna styrande dokument följs samt för att identifiera hot (t.ex. intrångsförsök och skadlig kod) som kan utgöra en fara för Region Skånes

informationstillgångar.

12.3.2 För e-post finns loggar om bland annat mottagare, avsändare, tidpunkt och ämnesrad. För internetanvändning loggas interna och externa IP-adresser samt tidpunkt.

12.3.3 Kontroller kan ske av tekniska och säkerhetsmässiga skäl för att ta fram statistik eller för att utreda misstanke om brott, misstanke om att användaren brutit mot interna styrande dokument samt misstanke om att arbetstagaren allvarligt missbrukat arbetsgivarens förtroende. Verksamhetschef beslutar i enskilda ärenden om kontroll. Vid behov kan samråd ske med enheten för juridik och/eller HR-funktion.

12.3.4 Under vissa omständigheter kan arbetsgivaren behöva komma åt innehållet i en enskild medarbetares hemmakatalog. Dessa tillfällen kan vara att medarbetaren slutat och inte överlämnat handlingar som Region Skåne behöver, någon begär ut en handling och handlingen finns i medarbetarens hemmakatalog och medarbetaren är otillgänglig eller det finns misstanke om brott, både mot lagstiftning och interna styrande dokument som gör att arbetsgivaren behöver åtkomst till hemmakatalogen. Verksamhetschef beslutar i enskilda ärenden om kontroll. Vid behov kan samråd ske med enheten för juridik och/eller HR-funktion.

12.3.5 Regiondirektören eller den Regiondirektören utser i sitt ställe beslutar om särskild kontroll ska ske av säkerhetsloggar i central IT-infrastruktur i syfte att identifiera och oskadliggöra hot mot Region Skånes informationstillgångar, exempelvis olaga dataintrång, skadlig kod, överbelastningsattack m.m. Privata vårdgivare och andra som genom avtal är bundna av dessa riktlinjer är skyldiga att bistå i detta arbete.

12.3.6 Anslutning till Region Skånes nätverk kan stängas av om anslutningen utgör hot mot Region Skånes informationstillgångar, exempelvis olaga dataintrång, skadlig kod, överbelastningsattack m.m. Innan beslut om avstängning fattas ska riskerna med avstängningen ha analyserats. Beslut om avstängning fattas av Regiondirektören eller den Regiondirektören utser i sitt ställe.

13 Åtkomst till information

13.1 Styrning av åtkomst till elektronisk information

13.1.1 All tillgång till elektronisk information inom Region Skåne ska styras med hjälp av administrativa och tekniska skyddsåtgärder så att endast behöriga får tillgång till informationssystem.

13.1.2 Behörigheter ska vid varje tillfälle baseras på aktuella arbetsuppgifter.

13.1.3 Innan en användare tilldelas åtkomsträttighet ska en behovs- och riskbedömning göras.

13.1.4 Tilldelning av åtkomsträttigheter ska dokumenteras och regelbundet följas upp. Detta ska även ske efter varje större organisations- eller systemförändring.

13.1.5 Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, ska begränsas till så få personer som möjligt och baseras på aktuella arbetsuppgifter.

13.1.6 Varje användares identitet ska verifieras. Detta sker genom autentisering, det vill säga verifiering av användarens identitet. Alla användare ska ha en unik identitet. Det grundläggande kravet på utformningen av identiteter är att de ska vara spårbara till en fysisk person.

13.1.7 e-Tjänstekort med pin-kod eller annan godkänd autentisering ska användas för att fastställa en användares identitet . För information med lägre skyddskrav och när det inte är möjligt att använda tvåfaktorsautentisering kan andra metoder användas om riskerna analyserats och bedömts vara acceptabla.

13.1.8 Åtkomst ska loggas och tilldelade rättigheter följas upp för att säkerställa att endast behöriga användare har åtkomst till information.

13.1.9 Loggar ska vara skyddade mot obehörig åtkomst och manipulation. Loggarna ska omfattas av fastställda rutiner för säkerhetskopiering och arkivering.

13.1.10 Systematiska och regelbundna stickprovskontroller av loggar ska göras enligt fastställda styrande dokument. Av dessa ska framgå vad som ska loggas, hur ofta loggarna ska granskas, vem som ska utföra granskningen samt vad som är att betrakta som överträdelse. Vidare ska det finnas regler för hur överträdelser hanteras.

13.1.11 För system som innehåller personuppgifter eller uppgifter som omfattas av sekretess, bör loggarna analyseras med hjälp av automatiserade verktyg med koppling till larm när gränsvärden överskrids. Om detta inte är möjligt ska manuella kontroller göras. Extra vikt ska läggas vid uppföljning av konton med höga behörigheter.

13.2 Extern informationsanvändning

13.2.1 För informationsanvändare som ges åtkomst till Region Skånes icke-publika informationstillgångar från miljöer utanför Region Skånes kontroll, ska särskilda krav ställas på autentisering av användare och utrustning, liksom på kryptering.

13.2.2 Personuppgifter i hälso- och sjukvård (patientuppgifter) eller andra uppgifter med höga skyddskrav ska krypteras med relevant metod och endast vara tillgängliga genom stark autentisering. Undantag kan under vissa förutsättningar göras för kallelser och påminnelser via sms och e-post.

13.3 Styrning av åtkomst till icke digital information

13.3.1 Skyddsvärd icke digital information ska omgärdas av skyddsåtgärder vid all hantering, det vill säga kopiering, distribution, förändring, läsning, makulering, förvaring och arkivering.

14 Fysisk och miljörelaterad säkerhet

14.1 Generella regler för fysisk säkerhet

14.1.1 Nivån på det fysiska skyddet av tillgångar ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad.

14.1.2 System och utrustning som är känslig i sig själv eller behandlar information som omfattas av sekretess eller av andra skäl är känslig, ska placeras så att tillträde minimeras och utformningen av lämpliga skyddsåtgärder underlättas.

14.1.3 Kritiska informationstillgångar ska inrymmas i säkra utrymmen.

14.1.4 Tillträdeskontroll till viktiga byggnader och lokaler ska finnas, för att säkerställa att endast behörig personal ges tillträde.

14.1.5 Fysiska säkerhetsåtgärder för information, system och utrustning ska samordnas med fysisk säkerhet och säkerhetsåtgärder för patienter, resenärer och andra brukare där så är tillämpligt.

14.2 Säkra utrymmen

Med säkra utrymmen avses utrymmen som är speciellt planerade och uppbyggda för att uppfylla höga krav på otillåten åtkomst, skada och störning. Skydd av sådana utrymmen ska utformas i proportion till förekommande risker och ska omfatta skal- och brandskydd, säkerhetsspärrar och tillträdeskontroller.

14.2.1 Skalskyddet ska anpassas till säkerhetskrav för tillgångarna inom skalskyddet och resultatet av en riskbedömning/säkerhetsskyddsanalys. Branschnormer ska följas.

14.2.2 För att säkerställa att endast behörig personal ges tillträde till säkrade utrymmen, ska dessa skyddas med lämpligt skalskydd och tillträdesbegränsningar.

14.2.3 För att möjliggöra loggning av in- och utpasserande ska kontrollsystemen vara kopplade till individuella passagekort eller koder.

14.2.4 Elektronisk utrustning är känslig för brand, annan temperaturhöjning och rök. Det är viktigt att ett ändamålsenligt skydd finns i de utrymmen där sådan utrustning finns.

14.2.5 Rör, där vatten står under tryck, bör inte finnas i säkra utrymmen. Vätskelarm ska finnas, om det i utrymmet finns rördragningar innehållande vatten, eller om det av andra orsaker finns risk för vattenskada.

14.3 Reservkraft och avbrottsfri kraft

14.3.1 Verksamhetskritiska system och verksamhetsställen med starkt beroende av elförsörjning ska vara försedda med reservkraft.

14.3.2 System och annan elektronisk utrustning bör skyddas mot elavbrott och andra störningar i elförsörjningen. Strömförsörjning av verksamhetskritiska system och utrustningar bör ske via avbrottsfri kraft (UPS), som i sin tur bör anslutas till reservkraft.

14.3.3 Tester ska göras regelbundet för att säkerställa att övergången till reservkraft fungerar. Risker rörande den elektromagnetiska miljön bör beaktas.

14.4 Säkerhet för tillgångar utanför egna lokaler

14.4.1 Risker i samband med hantering av system och utrustning och andra tillgångar utanför de egna lokalerna ska beaktas och nödvändiga skyddsåtgärder vidtas. Styrande dokument ska fastställas för sådan hantering.

15 Driftsäkerhet

15.1 Generella krav på systemmiljö

15.1.1 Region Skåne ska som regel ha en systemmiljö med åtskilda produktions-, utvecklings-, test-, acceptanstest-, och utbildningsmiljöer. Säkerhetsreglerna för produktionsmiljöer ska i

relevanta delar även gälla för utvecklings- och acceptanstestmiljöer.

15.1.2 Region Skåne har en systemmiljö med industriella informations- och styrsystem, t.ex. SCADA-system. Dessa system och anslutningar ska vara kartlagda.

15.2 Systemförvaltning

15.2.1 För att upprätthålla säker och tillförlitlig tillgång till information, ska administration, drift och underhåll av system ske på ett strukturerat och systematiskt sätt, enligt en fastställd modell för systemförvaltning.

15.2.2 System ska ha fastställda och aktuella rutiner för administration, drift och underhåll, dokumenterade i en systemförvaltningsplan. Planen ska säkerställa att systemen hanteras på ett enhetligt och informationssäkerhetsmässigt korrekt sätt och att beroendet av enskilda personers kunskaper minskas.

15.2.3 Beskrivning av systemets ändamål och kraven utifrån informationssäkerhetsklass ska finnas i systemdokumentationen, hållas aktuella och uppdateras om informationssäkerhetsklassningen ändras.

15.2.4 Informationsklassificering och riskhantering[7] ska genomföras regelbundet och innan viktiga förändringar genomförs, för att utvärdera kraven på skydd. Utifrån dessa analyser ska lämpliga skyddsåtgärder vidtas för att fastställd skyddsnivå ska få avsedd effekt. I analyserna ska ingå kontroll av att systemen följer interna och juridiska krav.

15.3 Systemdokumentation

15.3.1 Det ska finnas systemdokumentation[8] för varje system. Dokumentationen ska normalt bestå av system-, drift- och användardokumentation, och utformas enligt krav i gällande styr- och förvaltningsmodell.

15.3.2 Systemdokumentation ska vara fullständig och aktuell. Ändring i dokumentationen ska ske enligt fastställda rutiner.

15.3.3 Det ska finnas en kopia av systemdokumentationen, liksom av andra, för systemets användning och drift, viktiga dokument. Dessa kopior ska förvaras skilda från originalen i annan brandcell eller

---

[7] Krav enligt bland annat 3 kap. 7, 10 §§ HSLF-FS 2016:40

[8] Krav enligt bland annat 3 kap. 8 § HSLF-FS 2016:40 när det gäller behandling av personuppgifter inom hälso- och sjukvård

annan byggnad och de ska vara åtkomliga även om systemet de normalt sett förvaras på är otillgängligt.

15.3.4 Delar av systemdokumentationen som innehåller känslig information, till exempel om systemets säkerhetsfunktioner, ska förvaras så att den endast är åtkomlig för behörig personal.

15.3.5 I systemdokumentationen ska det framgå hur informationen ska bevaras och gallras samt vilken bevarande- och gallringsplan som gäller för systemet.

15.4 Säkerhetsuppdateringar

15.4.1 Leverantörers säkerhetsuppdateringar ska installeras skyndsamt. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringarna testas och analyseras innan de installeras i produktionsmiljön.

15.5 Skydd mot skadlig kod

15.5.1 System och utrustning som kan drabbas av skadlig kod, ska skyddas. Kontrollen ska ske obligatoriskt och automatiskt. Skyddsmekanismerna ska automatiskt uppdateras löpande, för att garantera generellt och aktuellt skydd.

15.5.2 Förekomst av skadlig kod är att beteckna som informationssäkerhetsincident och ska rapporteras.

15.6 Styrning av ändringar i system

15.6.1 Ändringar i eller kring ett system ska planeras. Innan ändringsbeslut fattas ska riskbedömning ske.

15.6.2 Beslut om ändringar i eller kring ett system ska fattas av systemägaren i enlighet med informationsägarens fastställda krav gällande ändamål och krav på informationssäkerhet. Beslut om ändringar som väsentligen avviker från fastställt ändamål för ett system eller på annat sätt kan påverka informationssäkerheten ska fattas av informationsägaren.

15.6.3 Samtliga ändringar ska kunna härledas till en ansvarig beställare.

15.6.4 Rutiner ska fastställas för ändringshantering och testning, och ska vara kända av berörda personer. Rutinerna ska även säkerställa att det är möjligt att återgå till läget före ändringen.

15.6.5 Ändringar, som bedöms kunna påverka informationssäkerheten, ska testas i separat testmiljö innan de införs i produktionsmiljö.

15.7 Felhantering

15.7.1 Allvarliga störningar i produktionsmiljö kräver ofta att åtgärder genomförs omgående och att fastställda rutiner för ändringshantering inte kan följas. Sådana akuta ändringar ska dokumenteras och i efterhand följas upp enligt rutinen för ändringshantering.

15.8 Kapacitetsplanering

15.8.1 Kapacitetsplanering som syftar till att förutse och förebygga kapacitets- eller prestandaproblem ska ske. Regelbunden mätning och uppföljning av kapaciteten ska genomföras. Detta är särskilt viktigt för de system som stödjer samhällsviktig eller verksamhetskritisk verksamhet.

15.9 Säkerhetskopiering och återläsning av data

15.9.1 Säkerhetskopiering av information och programvara ska utföras regelbundet, med frekvens och omfattning anpassad till verksamhetskrav respektive legala krav.

15.9.2 Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras.

15.9.3 Säkerhetskopior och original ska förvaras i olika byggnader eller brandceller och med skyddsåtgärder som överensstämmer med informationens klassificering.

15.10 Driftövervakning

15.10.1 System som stödjer samhällsviktig eller verksamhetskritisk verksamhet ska driftövervakas kontinuerligt och händelser ska loggas för att minimera avbrott och andra informationssäkerhetsincidenter. Loggar ska skyddas mot radering, manipulation och obehörig åtkomst.

15.10.2 Behovet av och rutiner för loggning och uppföljning av loggar (analys) ska fastställas av informationsägaren. Lagkrav som är tillämpliga på övervakningsaktiviteterna ska följas. Områden som ska övervägas är till exempel behörig åtkomst, privilegierade aktiviteter, obehöriga åtkomstförsök, systemlarm, ändringar eller försök till ändringar av säkerhetsinställningar.

15.11 Drift hos extern part

Innan lagring eller behandling av känsliga personuppgifter eller information som omfattas av sekretess sker hos extern leverantör ska informationsklassificering och riskanalys genomföras. Om personuppgifter ska behandlas som kan leda till en hög risk för de registrerade ska även konsekvensbedömning (DPIA) avseende dataskydd genomföras. Resultatet

utgör underlag för beslut av informationsägare om vilka krav som ska ställas på informationshanteringen.

15.11.1 När en verksamhet inom Region Skåne köper en tjänst hos extern part eller förlägger drift av system hos en sådan, ska minst samma regler för informationssäkerhet gälla som när driften hanteras i egen regi.

15.11.2 Kraven på informationssäkerhet ska regleras i avtalet mellan parterna och uppföljning av avtalad säkerhetsnivå ska ske. Detta ska göras möjligt genom att i avtalet specificera att Region Skåne har rättighet att genomföra revision av informationssäkerheten eller ta del av revisioner som utförs av godkänd tredje part.

15.11.3 I en upphandlingsprocess där det i förfrågningsunderlaget eller under uppdragets utförande förekommer säkerhetsskyddsklassificerade uppgifter eller där leverantören kommer att delta i verksamhet med betydelse för Sveriges säkerhet, ska det träffas ett skriftligt säkerhetsskyddsavtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs.

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

15.11.5 I avtalet med tjänsteleverantör ska det regleras i vilka format data ska hämtas ut vid avslutande av tjänst.

15.11.6 Det ska i avtalet regleras inom vilken tid data ska levereras i samband med avtalets upphörande.

15.11.7 System som ska hantera information som klassificerats i informationsklass K2 eller högre enligt Region Skånes informationsklassificeringsmodell ska inte upphandlas som en molntjänst utan att laglighetsprövning, riskbedömning samt prövning av lämpligheten genomförts och dokumenterats. Molntjänsten får inte tas i drift innan beslutade skyddsåtgärder genomförts och lagkrav uppfylls.

15.11.8 Extern drift, inkluderande molntjänster, ska som grundregel inte användas om det är oklart var information kommer att lagras eller bearbetas fysiskt (geografiskt).

15.12 Gallring av information och avveckling av informationssystem

15.12.1 Gallring av information och avveckling av informationssystem ska ske på ett säkert sätt och i enlighet med Regionarkivets beslut.

15.12.2 I samband med kravställning av informationssystem ska det, i den mån det är möjligt, ingå delar som reglerar hur en framtida avveckling ska hanteras.

16 Kommunikationssäkerhet

16.1.1 Om privata verksamheter med egen internetkoppling ska anslutas till Region Skånes nätverk fordras att riskbedömning utförs och att avtal tecknas som reglerar det gemensamma trafikskyddet.

16.1.2 Region Skånes nätverk ska vara uppdelat i nätverkssegment för att minimera risken för obehörig åtkomst samt möjliggöra uppdelning i t.ex. åtskilda produktions-, utvecklings- och testmiljöer etc. Utvecklings- och testarbete ska inte kunna störa produktionen.

16.1.3 Publika nätverk ska vara logiskt separerade från produktionsnätverk.

16.1.4 Sammankoppling av nätverk får endast ske efter genomförd riskanalys och sedan nödvändiga skyddsåtgärder vidtagits av respektive nätverks systemägare. Sammankoppling av nätverk får ske först efter skriftligt beslut.

16.1.5 Respektive nätverksägare ansvarar för de skyddsåtgärder som krävs för att motverka avlyssning och förändring av överförd information. Skyddsåtgärderna ska ha sin grund i aktuell informationsklassificering och riskanalys och motsvara det skyddsvärde som informationen har.

16.1.6 Respektive nätverksägare ska utifrån informationsägarnas krav på tillgänglighet besluta om nätverksinfrastruktur och val av aktiva nätkomponenter.

16.1.7 Respektive nätverksägare ska se till att det finns styrande dokument för anslutning mot nätverket.

16.1.8 Nätverk, dess komponenter och systemsamband ska vara dokumenterade och det ska finnas tydliga instruktioner hur dokumentation ska utformas.

16.1.9 Fjärranslutningar till system för till exempel fjärrdiagnostik eller fjärrövervakning m.m. ska ske genom Region Skånes nätverk under

kontrollerade och säkra former fastställda av respektive systemägare.

17 Anskaffning, utveckling och underhåll av system

17.1 Generella regler

Informationssäkerhetskraven, vid upphandling, ny- och vidareutveckling av system, i egen regi eller i samverkan med samarbetspartner, ska analyseras och definieras utifrån en dokumenterad informationsklassificering och riskbedömning.

17.1.1 Vid utveckling och anskaffning av system ska det analyseras vilket skydd systemet kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt. Kraven på systemet ska tydligt framgå i kravspecifikationen.

17.1.2 Innan ett system tas i drift ska informationen som ska hanteras i systemet vara klassificerad enligt Region Skånes gällande klassificeringsmodell.

17.1.3 Ett system ska, innan det tas i drift, ha godkänts av den eller de informationsägare vars information ska hanteras i systemet.

17.1.4 All anskaffning, utveckling, förändring och avveckling av it-system ska ske i enlighet med beslutad förvaltningsmodell.

17.2 Systemutveckling

17.2.1 Det ska i systemutvecklingsarbete tillses att dokumenterade modeller för systemutveckling och projektstyrning finns och tillämpas.

17.2.2 I systemutvecklingsarbete ska system, programvara och informationstillgångar skyddas på motsvarande sätt som de färdiga produkterna. Produktionsmiljöer ska skyddas.

17.2.3 Information i samband med systemutveckling ska skyddas enligt samma principer som övrig verksamhetsinformation. Testmiljö ska, om inte särskilda skäl föreligger, inte innehålla produktionsdata. Användning av personuppgifter eller information i informationssäkerhetsklass K2 eller högre enligt Region Skånes informationsklassificeringsmodell får inte förekomma i testmiljö.

17.2.4 Styrande dokument för acceptanstest, driftgodkännande och produktionssättning ska finnas och tillämpas. System ska genomgå acceptanstest före godkännande. I godkännandet ska det ingå en uppföljning av säkerhetskraven. Ett beslut ska fattas om eventuella avvikelser hindrar en produktionssättning och inom vilken tidsram de ska åtgärdas. Är systemet godkänt kan det därefter överlämnas

för driftsättning. Driftgodkännande ska ske av respektive informationsägare.

17.3 Upphandling av system och systemutveckling

17.3.1 För upphandling som innefattar hantering av säkerhetsskyddsklassificerade uppgifter[9] finns krav utifrån lagstiftning (säkerhetsskyddslagen) som ska följas.

17.3.2 I kravspecifikationen ska informationssäkerhetskraven alltid ingå. Vidare ska det i det slutliga lösningsförslaget finnas specifikation av i vilka tekniska miljöer och på vilka plattformar systemet ska fungera.

17.3.3 Avtal ska utformas så att Region Skåne erhåller fullständig förfoganderätt till allt kundunikt arbete och material som leverantören tar fram särskilt för beställaren i samband med uppdrag.

17.3.4 För att möjliggöra och bibehålla kontinuitet och fortsatt utveckling av viktiga tjänster ska Region Skåne, vid behov, avtala om att få tillgång till källkoden om vissa förutsättningar är uppfyllda som exempelvis att leverantören går i konkurs, om nyckelpersoner som utvecklat programmet lämnar leverantören eller om leverantören missköter sitt utvecklings- eller underhållsåtagande. I ett sådant Källkodsdepositionsavtal ska leverantören åta sig att deponera aktuell källkod hos en oberoende tredje part som under vissa förutsättningar ger Region Skåne tillgång till källkoden. Region Skåne ges då möjlighet att själv underhålla och uppdatera det aktuella it-systemet.

[9] Säkerhetsskyddad upphandling

18 Informationssäkerhetsincidenter

18.1.1 Informationssäkerhetsincidenter ska hanteras enligt fastställda processer.

18.1.2 Incidenter som kräver rapportering till tillsynsmyndighet ska rapporteras till dessa inom givna tidsramar.

18.1.3 Medarbetare ska rapportera avvikelser som kan utgöra ett hot mot Region Skånes informationstillgångar.

18.1.4 Vid utredning av en incident ska information samlas in på ett sådant sätt att det inte finns risk att bevis förstörs.

19 Verksamhetens kontinuitet

19.1 Generella regler

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

19.1.2 I verksamhetens kontinuitetsplan ska det behandlas hur verksamheten ska bedrivas vid avsaknad av kritiska funktioner och informationstillgångar samt hur återgång till normalläge ska ske.

19.1.3 Kontinuitetsplaner och återstartsplaner skall finnas för all information och alla system som klassats i tillgänglighetsklass T2 eller högre enligt Region Skånes informationsklassificeringsmodell. Planer kan vara gemensamma för flera verksamheter och flera system och ska innehålla fastställda prioriteringsordningar för återgång till normalläge.

19.1.4 Målet med kontinuitetsplaneringen ska vara att kritiska verksamheter ska kunna upprätthållas, på rimlig nivå, vid olika typer av katastrofsituationer, störningar och oplanerade avbrott. De delar av kontinuitetsplaneringen som berör katastrof- och beredskapssituationer ska ingå i verksamhetens övriga katastrofplanering.

19.1.5 Det ska finnas fastställda och aktuella reservrutiner för katastrofsituationer, störningar eller oplanerade avbrott. Rutinerna kan vara såväl manuella som IT-baserade.

19.1.6 Kontinuitetsplanerna ska testas regelbundet, enligt fastställd plan samt efter större organisationsförändringar. Planerna ska underhållas genom regelbundna granskningar och övningar, för att säkerställa att de är aktuella och ändamålsenliga.

20 Uppföljning och efterlevnad

20.1 Generella regler

20.1.1 Förvaltningar ska löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

20.1.2 Förvaltningar ska regelbundet granska sin informationssäkerhet. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas.

20.1.3 Varje år ska förvaltningarnas informationssäkerhetssamordnare rapportera arbetet med informationssäkerheten till förvaltningschef.

Bilaga 1 – Ansvar för särskilda roller

Systemägare

Systemägaren förvaltar system. Systemägaren ska utifrån informationsägarens krav utforma systemet så att informationen skyddas på adekvat sätt.

Systemägaren ansvarar för att:

- förteckning förs över vilken information som behandlas i system och vem eller vilka som är informationsägare till denna information
- verksamhetens behov av systemstöd tillgodoses
- krav på informationssäkerhet och funktionalitet uppfylls
- åtgärder vidtas för att åtgärda systemrelaterade risker utifrån genomförda riskanalyser
- system- och användardokumentation upprättas och hålls uppdaterad
- förvaltningsplaner upprättas
- driftgodkännande dokumenteras
- avbrottsplan för kritiska system utarbetas, hålls uppdaterade och testas så den uppfyller verksamhetens kontinuitetsplan
- incidenter, funktionsfel och brister dokumenteras, analyseras och hanteras

Informationssäkerhetssamordnare

Informationssäkerhetssamordnaren ska leda, utveckla, samordna och följa upp informationssäkerhetsarbetet utifrån regionövergripande styrande dokument. Utöver det ska informationssäkerhetssamordnaren:

- Informera, utbilda och ge råd
- Samarbeta med förvaltningens dataskyddssamordnare med att stödja verksamheten vid genomförandet av informationsklassificering och olika typer av riskbedömningar inkluderande konsekvensanalyser avseende dataskydd enligt dataskyddsförordningen
- Informera förvaltningschefen/informationsägaren om legala krav inte efterlevs och vid behov rapportera till regionala stödfunktioner
- Delta i framtagande av regionövergripande styrande dokument avseende informationssäkerhet
- Samarbeta med övriga säkerhetsområden med målet att säkerhetsåtgärder blir välbalanserade och heltäckande
- Utgöra första kontaktpunkt vid informationssäkerhetsincidenter inom förvaltningen.
- Samråda med dataskyddssamordnaren kring hantering av personuppgiftsincidenter och dataintrångsärenden inom förvaltningen
- Delta i regionalt informationssäkerhetsråd, se punkt 5.2.1.
- Vara informationssäkerhetschefens kontaktperson i informationssäkerhetsfrågor.
- Minst en gång per år rapportera status för informationssäkerhetsarbetet till informationssäkerhetschefen

Bilaga 2 – Ordlista

Ordlistan utgår i sin grund från **SIS tekniska rapport SIS-TR 50:2015**. Termer och definitioner i rapporten har anpassats till aktuellt språkbruk och gällande standarder och praxis.

Term	**Förklaring**
Hot	möjlig, oönskad händelse med negativa konsekvenser för verksamheten
Information	Innebörd i data **Data** måste tolkas för att information ska erhållas.
Informationssystem	**System som innehåller information.** Omfattar både IT-system och MT-system, applikationer, tjänster eller andra komponenter som hanterar **information** IT-system är informationssystem om det hanterar information.
Informationssäkerhet	bevarande av **konfidentialitet**, **riktighet** och **tillgänglighet** hos information Informationssäkerhet ses som en uppsättning **säkerhetsåtgärder** för bevarande av egenskaper som **konfidentialitet**, **riktighet** och **tillgänglighet** men även spårbarhet, autenticitet, ansvarsskyldighet, oavvislighet och auktorisation. Informationssäkerhet omfattar områdena **administrativ säkerhet** och **teknisk säkerhet**.
Informationstillgång	information, och resurser som hanterar den, som är av värde för en organisation Exempel på informationstillgångar är: – **information** (patientjournal, metodik, handling, provsvar, mätvärden etc.) – program (applikation, operativsystem etc. samt mjukvara i medicintekniska produkter) – tjänster (kommunikationstjänst, abonnemang etc.) – fysiska tillgångar (dator, medicinteknisk produkt, datamedier, lokala nätverk etc.) – personal och deras kompetens, färdigheter och erfarenheter – immateriella tillgångar (rykte och image etc.)

	Informationstillgångar kan vara av fysisk eller logisk karaktär, eller bådadera.
Informationsägare	person eller enhet som har ansvaret för den information som skapas och hanteras inom ramen för tilldelat ansvar Ansvaret omfattar bl.a. underhåll av och tillgänglighet hos **informationen**, dess riktighet samt kontroll av att **informationen** motsvarar ställda krav. Uttrycket -ägare innebär inte en faktisk äganderätt till **informationen**.
IT-säkerhet	IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet IT-säkerhet omfattar områdena **datasäkerhet** och **kommunikationssäkerhet**.
Konfidentialitet	skydd mot obehörig insyn
Konsekvens	resultat av en händelse
Medarbetare	person som är anställd av Region Skåne eller som arbetar på uppdrag av Region Skåne
Molntjänst	Koncept som möjliggör nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser som via självbetjäning levereras och administreras på begäran[10].
Riktighet	skydd mot oönskad förändring
Risk	osäkerhetens effekt på mål
Riskbedömning	övergripande process som innefattar delprocesserna riskidentifiering, riskanalys och riskutvärdering
Skyddsnivå	grad av skydd något behöver
Skyddsvärde	något som behöver skyddas
System	Omfattar både IT-system och MT-system och andra typer av system oavsett om de innehåller information
Säkerhetsåtgärd	Identifierad uppsättning åtgärder för att möta en organisations risker. Säkerhetsåtgärder för **informationssäkerhet** omfattar åtgärder inom det administrativa och tekniska säkerhetsområdet.
Teknisk säkerhet	tekniska säkerhetsåtgärder för att upprätthålla informationens **konfidentialitet**, **riktighet** och **tillgänglighet**. Teknisk säkerhet omfattar områdena **it-säkerhet** och **fysisk säkerhet**.

[10] Informationsteknik – Molnbaserade datortjänster – Översikt och terminologi (ISO/IEC 17788:2014)

Tillgänglighet	åtkomst för behörig person vid rätt tillfälle
Vårdgivare	Statlig myndighet, landsting och kommun i fråga om sådan hälso- och sjukvård som myndigheten, landstinget eller kommunen har ansvar för samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvård.
Vårdprocess	Process avseende hälso- och sjukvård som hanterar ett eller flera relaterade hälsoproblem eller hälsotillstånd i syfte att främja ett avsett resultat.