**Koncernkontoret**
**Enheten för säkerhet och intern miljöledning**

Johan Reuterhäll
Informationssäkerhetschef
johan.reuterhall@skane.se

**RIKTLINJER**

Datum: 2017-12-07
Dnr: 1604263



# Riktlinjer för informationssäkerhet

Riktlinjerna slår fast hur organisation, roller och ansvar för informationssäkerhet på en övergripande nivå ska utformas i Region Skåne. Syftet är att arbetet med informationssäkerhet ska bedrivas effektivt och nå de mål som Regionfullmäktige och Regionstyrelsen beslutat om.

Riktlinjen är en del av Region Skånes ledningssystem för informationssäkerhet.

# 1 Inledning

Information är en grundläggande byggsten i Region Skåne. Information inhämtas, lagras, kommuniceras och bearbetas i olika former. En stor del av informationen är känslig och värdefull. Det kan innebära stora negativa konsekvenser för Region Skåne om information går förlorad eller inte finns till hands när den behövs. Det kan också få stora konsekvenser om information som är känsliga eller omfattas av sekretess röjs för obehöriga.
Organisationens krav på informationssäkerhet baseras på interna krav i verksamheten samt externa krav i form av lagstiftning.
Medborgarna ska vara förvissade om att information inom Region Skåne hanteras korrekt och har tillräckligt skydd.
Informationen ska därför skyddas så att endast behörig får tillgång till den (**konfidentialitet**), att den är korrekt och inte är manipulerad eller förstörd (**riktighet**) och att den finns när den behövs (**tillgänglighet**).
Patientsäkerhet är ett prioriterat område för Region Skåne där informationssäkerhet är en förutsättning för att uppnå kvalitet och säkerhet i vården samt för skydda den personliga integriteten för patienter.
Det systematiska informationssäkerhetsarbetet i Region Skåne har sin grund i standarden för informationssäkerhet, ISO/IEC 27000.

## 1.1 Mål

Målen för informationssäkerheten definieras i de långsiktiga mål som beslutas av Regionfullmäktige samt de kortsiktiga mål som beslutas av Regionstyrelsen.

## 1.2 Syfte

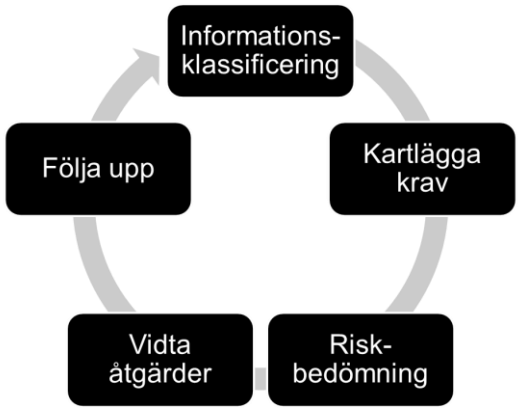
Riktlinjen utgår från Region Skånes säkerhetspolicy och anger hur Region Skåne ska arbeta med informationssäkerhet.
Riktlinjen baseras på standarden för informationssäkerhet SS-ISO/IEC 27000. Från kapitel fyra redovisas övergripande skyddsåtgärder med utgångspunkt i standarden. Dessa kommer att ligga till grund för den uppföljning som ska ske till Regionstyrelsen minst en gång per år.

## 1.3 Omfattning

Riktlinjen omfattar alla informationstillgångar oavsett om de behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö de förekommer.

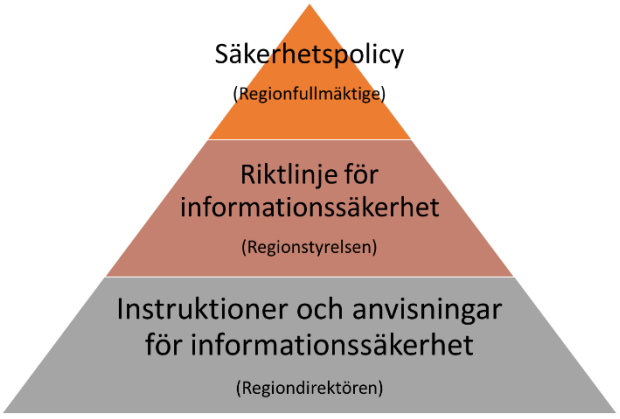
## 1.4 Övergripande process

Process visar övergripande de olika delarna för att uppnå en god informationssäkerhet. Alla delar av organisationen berörs av processen.




## 1.5 Övergripande styrdokument

Säkerhetspolicyn beskriver Region Skånes syn på säkerhetsarbetet och de övergripande principer som gäller. Säkerhetspolicyn beslutas av Regionfullmäktige.
Riktlinje för informationssäkerhet, denna handling, konkretiserar säkerhetspolicyn avseende grundläggande delar inom informationssäkerhet. Riktlinjen beslutas av Regionstyrelsen.
Instruktioner och anvisningar för informationssäkerhet anger hur arbetet ska bedrivas i praktiken utifrån säkerhetspolicy och riktlinjerna. Dessa beslutas av Regiondirektören.




# 2 Grundläggande principer

- Inom Region Skåne ska ett systematiskt och långsiktigt informationssäkerhetsarbete bedrivas.
- Region Skånes informationstillgångar ska identifieras, klassificeras och ges en lämplig skyddsnivå med utgångspunkt i att de finns tillgängliga när de behövs (tillgänglighet), att de är korrekta (riktighet) och att obehöriga inte kan få tillgång till dem (konfidentialitet).

- Region Skåne ska, utifrån återkommande riskbedömningar och inträffade incidenter, avgöra hur risker ska hanteras och vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivå för informationen.
- För att uppnå målet med informationssäkerheten ska säkerhetsarbetet omfatta samtliga delar av administrativ respektive teknisk säkerhet.
- 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.

# 3 Organisation, ledning och ansvar

För att uppnå och bibehålla en god informationssäkerhet ska ansvar definieras och tilldelas.

## 3.1 Övergripande ansvar för informationssäkerheten

**Regionfullmäktige**
Regionfullmäktige beslutar om Region Skånes säkerhetspolicy samt om långsiktiga mål för informationssäkerhetsarbetet.

**Regionstyrelsen**
Regionstyrelsen har det övergripande ansvaret för informationssäkerhet i Region Skåne. Regionstyrelsen beslutar om Region Skånes riktlinjer för informationssäkerhet. Regionstyrelsen ska minst en gång per år, vid ledningens genomgång, informeras om status på informationssäkerhetsarbetet och besluta om en övergripande handlingsplan för informationssäkerhetsarbetet samt om kortsiktiga mål.

**Regiondirektören**
Regiondirektören beslutar om regionövergripande instruktioner och anvisningar inom informationssäkerhetsområdet. Regiondirektören ansvarar för att informationssäkerhetsarbetet bedrivs effektivt så att informationssäkerhetsmålen kan uppnås.
Regiondirektören beslutar om vem som ska vara informationsägare för informationstillgångar som är gemensamma för Region Skåne.

**Informationssäkerhetschefen**
Informationssäkerhetschefen ansvarar för att leda, utveckla, samordna och övergripande följa upp informationssäkerhetsarbetet inom Region Skåne. I ansvaret ingår att förvalta riktlinjen för informationssäkerhet, regionövergripande instruktioner och anvisningar samt den övergripande handlingsplanen och målen för informationssäkerhet. I uppdraget ingår omvärldsbevakning och kontakt med externa myndigheter i informationssäkerhetsfrågor.

Informationssäkerhetschefen ska minst en gång om året sammanställa information om arbetet till Regionstyrelsen[1].

**Dataskyddsombudet (Personuppgiftsombudet)**
Dataskyddsombudets uppgifter är enligt Dataskyddsförordningen bland annat att informera och ge råd om vilka skyldigheter som gäller enligt såväl Dataskyddsförordningen som nationella bestämmelser. Ombudet ska också bevaka att dessa regler följs och ge råd om den konsekvensbedömning avseende dataskydd som ska göras enligt förordningen. Slutligen ska ombudet fungera som kontaktpunkt för dataskyddsmyndigheten och samarbeta med denna.
Dataskyddsombudet har en självständig position och ska i frågor som rör behandling av personuppgifter kunna rapportera direkt till den del av organisationen som Dataskyddsombudet bedömer vara lämpligt för att möjliggöra sin uppgift. Dataskyddsombudets roll och uppgifter definieras närmare i särskilt beslut om uppdrag till denne.

# 4 Personalsäkerhet

Alla som arbetar i Region Skåne ska kunna förstå sitt ansvar för och bidra till att hantera och skydda Region Skånes informationstillgångar. Personalens kunskaper och insikt i informationssäkerhetsrisker och hur dessa hanteras är en viktig del i ett effektivt informationssäkerhetsarbete. Informationssäkerhetsåtgärder ska vara en del av anställningsprocessen och stå i proportion till verksamhetens krav, klassificeringen av information som den anställde ska ges behörighet till och de risker som kan förekomma. Detsamma gäller under hela anställningen tills dess att anställningen upphör.

# 5 Hantering av tillgångar

Region Skåne hanterar stora mängder information som har ett högt skyddsvärde. Det är exempelvis personuppgifter inom hälso- och sjukvård, information om upphandlingar, risk- och sårbarhetsanalyser och annan känslig information. Viktiga informationstillgångar ska identifieras och klassificeras för att möjliggöra en lämplig skyddsnivå med utgångspunkt i att informationen finns tillgänglig när den behövs (tillgänglighet), att den är korrekt (riktighet) samt att obehöriga inte kan få tillgång till informationen (konfidentialitet). Viktiga[2] informationstillgångar ska tilldelas en informationsägare som fattar beslut om krav på skydd av informationstillgången.

[1] I enlighet med 1 kap. 6 §, HSLF-FS 2016:40
[2] Med viktiga informationstillgångar avses sådana informationstillgångar som behövs i verksamhet som bedöms vara samhällsviktig eller verksamhetskritisk.

## 6 Åtkomst till information

All tillgång till information inom Region Skåne ska styras med hjälp av administrativa och tekniska skyddsåtgärder så att endast behöriga får tillgång till informationen.
Behörigheter till information och system ska baseras på aktuella arbetsuppgifter och organisatorisk tillhörighet och ska därtill följas upp regelbundet.
Varje användares identitet ska kunna verifieras och alltid vara spårbar till en fysisk person. För att kunna säkerställa korrekt användning av behörigheter behöver i vissa fall loggning och uppföljning genomföras.
Informationsägaren beslutar om vilka säkerhetsåtgärder som krävs för åtkomst till information baserat på genomförd informationsklassificering och riskbedömning.

## 7 Fysisk och miljörelaterad säkerhet

Riskbedömning ska ligga till grund för det fysiska skalskydd som ska finnas för att skydda informationstillgångar. Utformning och styrka för skalskyddet ska vara anpassat till skyddsvärdet.
I skyddet ska behovet av brandskydd, skalskydd, avbrottsfri kraft, kylsystem, kablagesäkerhet m.m. utvärderas med stöd av expertis inom området.
De skyddsåtgärder som införs ska testas regelbundet för att verifiera att det har avsedd effekt.

## 8 Driftsäkerhet

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.
System som stödjer samhällsviktig eller verksamhetskritisk verksamhet ska driftövervakas kontinuerligt för att minimera avbrott och andra informationssäkerhetsincidenter.
När en verksamhet inom Region Skåne köper en tjänst från en extern part eller förlägger drift av system hos en sådan, ska i vart fall samma krav för informationssäkerhet gälla som när driften hanteras i egen regi.
System och utrustning som kan drabbas av skadlig kod, ska skyddas.

## 9 Kommunikationssäkerhet

Säkerhetsåtgärder ska finnas för att skydda information och anslutna tjänster mot obehörig åtkomst.
Vid kommunikation över öppna nätverk ska särskilda skyddsåtgärder vidtas för att garantera konfidentialitet och riktighet för data som överförs.
Detsamma gäller för att upprätthålla krav på tillgänglighet till nätverkstjänster och anslutna enheter.
Loggning och övervakning ska tillämpas för att registrera och upptäcka åtgärder som kan påverka informationssäkerheten.
Alla anslutningar till Region Skånes nätverk ska vara dokumenterade och godkända.

## 10 Anskaffning, utveckling och underhåll av system

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.
Informationssäkerhetskrav och säkerhetsåtgärder ska återspegla värdet av den information som ska hanteras och den potentiella negativa påverkan på verksamheten som brist på tillräcklig säkerhet kan leda till.
Identifiering av informationssäkerhetskrav ska integreras i samtliga ingående processers tidiga faser då det kan leda till mer verkningsfulla och kostnadseffektiva lösningar.
Ett system ska, innan det tas i drift, ha godkänts ur säkerhetssynpunkt av informationsägaren.

## 11 Leverantörsrelationer

Leverantörers åtkomst till Region Skånes tillgångar ska vara reglerat i avtal. Det omfattar sådana leverantörer som kan få åtkomst till, behandlar eller kommunicerar information som ägs av Region Skåne. Det omfattar även leverantörer som tillhandahåller infrastrukturkomponenter.
Region Skåne ska regelbundet övervaka, granska och revidera avtalade leveranser för att säkerställa att avtalet följs och att informationssäkerhetsincidenter och problem hanteras korrekt.
Region Skåne ska ha kontroll över och insyn i alla säkerhetsaspekter där känslig eller kritisk information är nåbar, bearbetas eller förvaltas av en extern leverantör.

## 12 Informationssäkerhetsincidenter

Region Skåne ska på ett strukturerat sätt proaktivt förebygga att informationssäkerhetsincidenter inträffar.
Inträffade informationssäkerhetsincidenter ska hanteras effektivt för att minimera skadorna i verksamheten så långt som möjligt och när det behövs, med hjälp av krishanteringsplaner.
Identifierade sårbarheter ska åtgärdas så att incidenter kan undvikas och lärdomar ska dras av inträffade incidenter och händelser samt rapporterade och åtgärdade sårbarheter.
Informationssäkerhetsincidenter där anmälningsskyldighet finns enligt lag eller förordning ska anmälas till ansvarig myndighet.

## 13 Verksamhetens kontinuitet

Det är viktigt att fastställa hur länge avbrott är acceptabla. För att hitta rätt ambitionsnivå ska juridiska krav samt verksamhetens behov av tillgång till information dokumenteras och riskbedömning genomföras.
Kontinuitetsplanerna ska innefatta reservrutiner och övriga åtgärder som kan vidtas för att säkerställa verksamhetens kontinuitet. Om verksamheten

är beroende av en annan organisation som till exempel en leverantör ska även leverantören vara involverad i arbetet[3].

## 14 Uppföljning och efterlevnad

Regionstyrelsen har det övergripande ansvaret[4] för informationssäkerheten inom Region Skåne och därmed för uppföljning av denna.
Varje verksamhet är ansvarig för informationssäkerheten inom sin verksamhet och ska:

- löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll
- granska sin informationssäkerhet och baserat på genomförda granskningar och identifierade avvikelser vidta skyddsåtgärder

För att säkerställa att styrande dokument efterföljs ska uppföljningar genomföras såväl årligen som när det inträffar väsentliga händelser som påverkar informationssäkerheten. Dessa kan initieras av Region Skånes informationssäkerhetschef eller av Region Skånes revisorer; på eget initiativ eller inom ramen för en planerad revision.

Efterlevnaden av Region Skånes riktlinjer för informationssäkerhet ska årligen följas upp och rapporteras till Regionstyrelsen av informationssäkerhetschefen.

[3] Riktlinjer för leverantörers medverkan i Region Skånes krisberedskap, beslutad 2014-05-08 med diarienummer 1400190
[4] Personuppgiftsansvarig representeras även av Regionstyrelsen