

# Övergripande handlingsplan informationssäkerhet och dataskydd 2020-2021

Enheten för krisberedskap, säkerhet och miljö  
Informationssäkerhet

2019-10-29  
Beslutad 2020-01-14

RS/697/2019

## INNEHÅLL

1	Inledning.....	3
2	Handlingsplanens mål.....	5
3	Aktiviteter för att nå målen.....	8
4	Beskrivning av hur handlingsplanen avser uppnå krav enligt särskilda perspektiv .....	21
5	Uppföljning .....	21
6	Definitioner .....	21

# 1 Inledning

## 1.1 Allmänt

Informationssäkerheten i Region Jämtland Härjedalen ska ytterst tillvarata medborgarnas krav på integritet, rättssäkerhet och god service. Information är viktiga tillgångar för regionen i likhet med andra verksamhetstillgångar som är viktiga för regionens verksamheter. Därför behöver tillgångarna skyddas på rätt sätt.

Området informationssäkerhet omfattar hela regionens verksamhet.

Det finns allvarliga risker förknippat med ett bristande informationssäkerhetsarbete. Detta gäller inte minst inom hälso- och sjukvården där känsliga personuppgifter hanteras. Dataskyddslagstiftningen är numera mycket långtgående i sina krav på att personuppgifter kan hanteras på rätt sätt. Om så inte sker kan höga viten utdömas och skadeståndsanspråk kan ställas från enskilda personer mot regionen.

## 1.2 Handlingsplanens syfte och innehåll

Syftet med handlingsplanen är att säkerställa ett systematiskt informationssäkerhetsarbete som ska bidra till att uppnå en ökad förmåga och robusthet i regionens informationshantering. Genom detta ska regionen kunna möta de utökade hot som finns mot informationen.

Regionen behöver kunna säkra att personuppgifter hanteras på rätt sätt för att kunna värna medborgliga fri- och rättigheter enligt gällande dataskyddslagstiftning. En del i detta är också att kunna undvika kostnader i form av utdömda viten från tillsynsmyndighet för dataskydd samt skadestånd från enskilda personer.

Mål och aktiviteter i denna plan ska öka förmågan att upprätthålla regionens samhällsviktiga verksamheter genom en fungerande informationsförsörjning enligt krav från NIS-lagstiftningen (säkerhet i nätverk och informationssystem). Genom det systematiska arbetet kan medborgarnas behov av trygg vård och av ett väl fungerande stöd till regional utveckling tillgodoses.

Handlingsplanen ska ange de närmaste två årens inriktning och prioritering av regionens informationssäkerhetsarbete. Då informationssäkerhet är komplext och involverar ett flertal staber samt all verksamhet är det nödvändigt att skapa en gemensam bild av ansvars- och rollfördelning inom området.

## 1.3 Giltighetstid

Handlingsplanen gäller fr o m 2020-01-01 t o m 2021-12-31.



## 1.4 Övergripande mål som handlingsplanen har att förhålla sig till

Följande övergripande mål finns i regionplanen 2020-22 samt i regionstyrelsens och hälso- och sjukvårdsnämndens verksamhetsplan som styrande för denna övergripande handlingsplan.

### **Regionplan:**

- Modern sjukvård: Teknik ger nya möjligheter som ska användas för att utveckla vården. Innovationer, digitalisering och nya arbetsmetoder ska möjliggöra en närmare vård, standardiserade vårdförlopp ska tillämpas.

### **Hälso- och sjukvårdsnämndens och regionstyrelsens verksamhetsplaner:**

- Målområde modern sjukvård: god vård: Distansoberoende nära vård – användning av ny teknik, högre mobilitet, distanstjänster och appar samt digitalisering  
*Det här målet omfattar lösningar för informationsförsörjning som uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid. Målet blir mätbart genom att peka ut att vissa typer av stöd ska finnas framtagna. I regionstyrelsens ansvar ligger också att genomföra aktiviteter för att minska det digitala utanförskapet, dvs åtgärder för och med medborgare så att de kan och vill använda ny teknik, distanstjänster och appar i kontakt med regionen.*

Dessa mål har i denna handlingsplan brutits ned i följande effektmål per förvaltningsområde:

### **För förvaltningsområde hälso- och sjukvård:**

- God vård: Anskaffade lösningar för informationsförsörjning uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid.

### **För förvaltningsområde regional utveckling:**

- Anskaffade lösningar för informationsförsörjning uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid.

### **För regionstab:**

- Anskaffade lösningar för informationsförsörjning uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid.

## 1.5 Ansvarig för genomförande

Respektive förvaltningsområdeschef ansvarar för att innehållet i denna handlingsplan tas med i förvaltningsområdenas verksamhetsplanering.

- Informationssäkerhetssamordnaren ansvarar för att samordna och stödja aktiviteter samt för uppföljning av denna övergripande handlingsplan.
- Områdeschefer och systemansvariga ansvarar för att utse representanter till medverkan i angivna egna aktiviteter.
- Dataskyddsombudet ansvarar för att ge stöd och råd till verksamheterna i dataskyddsfrågor. Dataskyddsombudet är kontaktperson för regionen mot tillsynsmyndighet för dataskydd.
- Dataskyddshandläggaren ansvarar för att samordna och sammanställa inventering av register som hanterar personuppgifter samt följa upp åtgärder gällande dataskydd.
- Objektägare/systemägare (ansvarig roll inom förvaltningsstyrning av objekt/IT-tjänster) ansvarar för att hantera säkerhetskrav och krav på dataskydd inom ramen för sitt objekt. Observera att objektägare (förvaltningsmodell baserad på pm3 tillämpas) samt systemägare (förvaltningsmodell som inte baseras på pm3 tillämpas) används som alternativa rollnamn beroende på vilken typ av förvaltningsmodell som tillämpas för aktuell IT-tjänst/-system.
- Regionstabschef ansvarar för att tillgodose vissa verksamhetsgemensamma processer och stöd för utpekade områden.
- Digitaliseringsenheten ansvarar för att samordna och styra krav-, anskaffnings- och införandeprocessen för nya IT-tjänster.

## 2 Handlingsplanens mål

### Förvaltningsområde hälso- och sjukvård

1. God vård: Anskaffade lösningar för informationsförsörjning uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid.
2. Regionens samhällsviktiga verksamheter har en fungerande avbrottshantering för sina kritiska IT-system.
3. Styrning och kontroll över behörigheter till kritiska IT-system och till känslig information är god.

Enheten för krisberedskap, säkerhet och miljö  
Informationssäkerhet

2019-10-29  
Beslutad 2020-01-14

RS/697/2019

4. Chefer har fått utökat stöd att klara sina ansvarsområden relaterade till informationssäkerhet.
5. Interna revisioner gällande regionens tillämpning av dataskyddslagstiftningen visar på hög grad av efterlevnad.

### **Förvaltningsområde regional utveckling**

1. Anskaffade lösningar för informationsförsörjning uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid.
2. Styrning och kontroll över behörigheter till kritiska IT-system och till känslig information är god.
3. Chefer har fått utökat stöd att klara sina ansvarsområden relaterade till informationssäkerhet.
4. Interna revisioner gällande regionens tillämpning av dataskyddslagstiftningen visar på hög grad av efterlevnad.

### **Regionstab**

1. Anskaffade lösningar för informationsförsörjning uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid.
2. Regionens samhällsviktiga verksamheter har en fungerande avbrottsshantering för sina kritiska IT-system.
3. Styrning och kontroll över behörigheter till kritiska IT-system och till känslig information är god.
4. Chefer har fått utökat stöd att klara sina ansvarsområden relaterade till informationssäkerhet.
5. Interna revisioner gällande regionens tillämpning av dataskyddslagstiftningen visar på hög grad av efterlevnad.
6. Regionens ledningssystem för informationssäkerhet (LIS) ger medarbetarna ett ändamålsenligt stöd för att kunna utföra sina arbetsuppgifter i enlighet med gällande regelverk och lagkrav.
7. Införande av ny modell för förvaltningsstyrning för regionens IT-stöd har påbörjats och modellen har tydliggjort fördelning av informationsägarskap.
8. Krav på skyddet mot cyberattacker finns etablerade.

Ovanstående målområden syftar till att regionen ska kunna uppfylla gällande lagkrav samt kunna hantera sin information på ett säkert sätt. Detta bidrar till nytta i form av nöjdare

Enheten för krisberedskap, säkerhet och miljö  
Informationssäkerhet

2019-10-29  
Beslutad 2020-01-14

RS/697/2019

medarbetare och brukare/intressenter samt bättre fungerande verksamheter med högre leveransförmåga.

### 3 Aktiviteter för att nå målen

#### Förvaltningsområde hälso- och sjukvård

3.6 Mål HS: God vård: Anskaffade lösningar för informationsförsörjning uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
HS förvaltningsområde utser deltagare i arbetet med framtagning av anskaffningsprocess för nya IT-stöd	OC, verksamhetsutvecklare inom HS	Deltagare från HS förvaltningsområde i arbetet med framtagning av anskaffningsprocess utsedda	2020	Förvaltningsområdeschef HS	-

3.7 Mål HS: Regionens samhällsviktiga verksamheter har en fungerande avbrottshantering för sina kritiska IT-system

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Steg 1. Kartlägga och beskriva verksamhetens beroende av kritiska IT-system på områdesnivå	OC, AC, EC	Kritiska beroenden i konsekvensanalys är framtagna och godkända för samtliga områden inom HS.	2020	OC	Informationssäkerhets-samordnare
Steg 2. Utarbeta och godkänn reservrutiner för verksamhetskritiska IT-system baserat på verksamheternas beskrivna beroenden (i steg 1)	OC, AC, EC	Reservrutiner är framtagna och godkända för samtliga verksamhetskritiska IT-system som förvaltas av HS.	2020	OC	Informationssäkerhets-samordnare



### 3.8 Mål HS: Styrning och kontroll över behörigheter till kritiska IT-system och till känslig information är god

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Informationsägare identifieras och utses för verksamhetskritiska informationstillgångar	Informationsägare	Informationsägare är utsedda för informationstillgångar i COSMIC vård-administrativt system	2020	Förvaltningsområdeschef HS	Informationssäkerhets-samordnare
Kontroll av att användarbehörigheter i utpekade kritiska informationssystem är anpassade till medarbetarnas arbetsuppgifter vad gäller åtkomstnivåer och tidsbegränsning för tilldelad åtkomst	Objektägare/systemägare för utpekade system/tjänster	Användarbehörigheterna i COSMIC vård-administrativt system har verifierats.	2020	Förvaltningsområdeschef HS	Systemägare/system-ansvariga för berörda system, informations-säkerhetssamordnare
Kontroll av att behörighetsprocessen efterlevs för utpekade IT-system/-tjänster	Förvaltningsområdeschef HS	Behörigheter ska hanteras enligt minst nivå 2 för efterlevnad i COSMIC vårdadministrativt system (se mognadsmodell för behörighetshantering)	2020	Förvaltningsområdeschef HS	Systemägare/system-ansvariga för berörda system, informations-säkerhetssamordnare

### 3.9 Mål HS: Chefer har fått utökat stöd att klara sina ansvarsområden relaterade till informationssäkerhet

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Rollen Registerkoordinator har fått tydliggjort uppdrag som stöd till chefer inom varje verksamhetsområde	OC, AC, EC	Samtliga HS-områden har utsedd registerkoordinator	2020	Dataskyddsbud	Dataskyddshandläggare
E-utbildning i informationssäkerhet för chefer genomgås av berörda	Förvaltningsområdeschef, OC, AC, EC	E-utbildning för chefer i informationssäkerhet har fullföljts av 100% av chefer 2020-12-31.	2020	Förvaltningsområdeschef HS	Informationssäkerhets-samordnare
E-utbildning för rollen Registerkoordinator genomgås av berörda	Registerkoordinatorer (RK)	E-utbildning för Registerkoordinator i informationssäkerhet har fullföljts av 100% av utsedda RK 2020-12-31.	2020	OC, AC, EC	Dataskyddshandläggare

### 3.10 Mål HS: Interna revisioner gällande regionens tillämpning av dataskyddslagstiftningen visar på hög grad av efterlevnad

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Intern revision genomförs gällande att konsekvensbedömningar har upprättats för samtliga högrisk-PU-behandlingar	Registerägare	100% av identifierade högriskbehandlingar har en genomförd konsekvensbedömning	2020	Dataskyddsbud	Dataskyddshandläggare
Intern revision genomförs gällande att åtgärdsplaner efter konsekvensbedömningar har	Registerägare	100% av identifierade högriskbehandlingar har en upprättad åtgärdsplan	2020	Dataskyddsbud	Dataskyddshandläggare

upprättats för samtliga högrisk-PU-behandlingar samt att prioriterade åtgärder har överförts och implementerats i verksamhetsplaneringen					
Intern revision genomförs gällande arbetssätt för systematisk registrering av PU-behandlingar	Registerägare	100% av verksamheterna har rapporterat efterlevnad för systematiskt arbetssätt	2020	Dataskyddsbud	Dataskyddshandläggare

## Förvaltningsområde regional utveckling

### 3.11 Mål RU: Styrning och kontroll över behörigheter till kritiska IT-system och till känslig information har förbättrats

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Kartläggning görs av vilka IT-system som stödjer samhällsviktig verksamhet	Förvaltningsområdeschef, EC	Kartläggning av beroenden för IT-system för samhällsviktig verksamhet genomförd	2020	Förvaltningsområdeschef RU	Informationssäkerhets-samordnare
Informationsägare identifieras och utses för verksamhetskritiska informationstillgångar	Informationsägare	Behörigheter ska hanteras enligt minst nivå 2 för efterlevnad i två prioriterade system/tjänster.* (se mognadsmodell för behörighetshantering)	2020	Förvaltningsområdeschef RU	Informationssäkerhets-samordnare
Kontroll av att behörighetsprocessen efterlevs för utpekade IT-system/-tjänster	Förvaltningsområdeschef RU	Behörigheter ska hanteras enligt minst nivå 2 för efterlevnad i två prioriterade	2020	Förvaltningsområdeschef RU	Informationssäkerhets-samordnare

		system/tjänster.* (se mognadsmodell för behörighetshantering)			
Verifiering av att användarbehörigheter i utpekade kritiska informationssystem är anpassade till medarbetarnas arbetsuppgifter vad gäller åtkomstnivåer och tidsbegränsning för tilldelad åtkomst	Informationsägare	Användarbehörigheterna i två verksamhetskritiska system har verifierats.	2020	Förvaltningsområdeschef RU	Systemägare/systemansvariga för berörda system, informations-säkerhetssamordnare

### 3.12 Mål RU: Chefer har fått utökat stöd att klara sina ansvarsområden relaterade till informationssäkerhet

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Rollen Registerkoordinator har fått tydliggjort uppdrag som stöd till chefer inom varje verksamhetsområde	Förvaltningsområdeschef, EC	Uppdrag för registerkoordinator är beskrivet och kommunicerat till samtliga områdeschefer. Registerkoordinatorer är utsedda för samtliga regionens områden.	2020	Förvaltningsområdeschef, EC	Dataskyddshandläggare, dataskyddsombud
E-utbildning för chefer i informationssäkerhet och dataskydd genomgås	Förvaltningsområdeschef, EC	E-utbildning för chefer i informationssäkerhet har fullföljts av 100% av chefer 2020-12-31.	2020	Förvaltningsområdeschef RU	Informationssäkerhets-samordnare

### 3.13 Mål RU: Interna revisioner gällande regionens tillämpning av dataskyddslagstiftningen visar på hög grad av efterlevnad

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Intern revision genomförs gällande att konsekvensbedömningar har upprättats för samtliga högrisk-PU-behandlingar	Registerägare	100% av identifierade högriskbehandlingar har en genomförd konsekvensbedömning	2020	Dataskyddsombud	Dataskyddshandläggare
Intern revision genomförs gällande att åtgärdsplaner efter konsekvensbedömningar har upprättats för samtliga högrisk-PU-behandlingar samt att prioriterade åtgärder har överförts och implementerats i verksamhetsplaneringen	Registerägare	100% av identifierade högriskbehandlingar har en upprättad åtgärdsplan	2020	Dataskyddsombud	Dataskyddshandläggare
Intern revision genomförs gällande arbetssätt för systematisk registrering av PU-behandlingar	Registerägare	100% av verksamheterna har rapporterat efterlevnad för systematiskt arbetssätt	2020	Dataskyddsombud	Dataskyddshandläggare

## Regionstab

### 3.14 Mål RS: Anskaffade lösningar för informationsförsörjning uppfyller verksamhets- och lagkrav och ger rätt åtkomst till rätt person, på rätt plats i rätt tid

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Processtöd för informationssäkerhet och dataskydd gällande <b>anskaffning och införande</b> av nya IT-tjänster tas fram	Beställare av nya IT-tjänster i verksamheten	Stöd vid anskaffning-upphandling (upphandling, GDPR, juridik, infosäk, IT-säk) med säkerhetskrav finns framtaget  Införandestöd för nya IT-tjänster för att identifiera, kommunicera och verifiera uppfyllnad av säkerhetskrav finns framtaget	2020	Digitaliseringsenheten	Informationssäkerhets-samordnare
Uppföljning görs av anskaffningsprocessens ändamålsenlighet	Beställare av nya IT-tjänster i verksamheten	Mätning utförs av anskaffningsprocessens ändamålsenlighet	2021	Regionstabschef	Internrevisor
Processtöd för informationssäkerhet inom <b>förvaltning</b> av IT-tjänster tas fram i syfte att upprätthålla säkerhetskrav under IT-tjänstens hela livscykel	Objektägare/systemägare	Stöd till förvaltning av IT-tjänster finns framtaget	2020	Objektägare administrativa system	Informationssäkerhets-samordnare, förvaltningsledare administrativa system
Informationsskydd för känslig information utanför verksamhetssystemen	Verksamheter/målgrupper som har behov av att	Informationsskydd är infört till berörda verksamheter/målgrupper	2020	Regionstabschef	Informationssäkerhets-samordnare. IT-säkerhetsansvarig

kravställs och införs till berörda verksamheter/ målgrupper	använda informationsskydd				
Regelverk för godkända lagringsytor och handhavanderegler kopplade till informationsklassning tas fram och kommuniceras.	Samtliga medarbetare	Regelverk framtaget och godkänt och kommunicerat.	2020	Regionstabschef	Strateg informationsförsörjning, dataskyddsombud, informationssäkerhets-samordnare, arkivarie

### 3.15 Mål RS: Regionens samhällsviktiga verksamheter har en fungerande avbrottsshantering för sina kritiska IT-system

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Steg 1. Kartlägga och beskriva verksamhetens beroende av kritiska IT-system på områdesnivå	OC, AC, EC	Kritiska beroenden i konsekvensanalys är framtagna och godkända för samtliga områden inom RS	2020	OC	Informationssäkerhets-samordnare
Steg 2. Utarbeta och godkänn reservrutiner för verksamhetskritiska IT-system baserat på verksamheternas beskrivna beroenden (i steg 1)	OC, AC, EC	Reservrutiner är framtagna och godkända för samtliga verksamhetskritiska IT-system som förvaltas av RS	2020	OC	Informationssäkerhets-samordnare

### 3.16 Mål RS: Styrning och kontroll över behörigheter till kritiska IT-system och till känslig information är god

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Informationsägare identifieras och utses för	Informationsägare	Informationsägare är utsedda för	2020-21	Regionstabschef	Informationssäkerhets-samordnare

verksamhetskritiska informationstillgångar		informationstillgångar i Heroma personal-administrativt system, i Rainsdance ekonomisystem samt i Centuri dokumentsystem			
Kontroll av att behörighetsprocessen efterlevs för utpekade IT-system/-tjänster	Objektägare/systemägare för utpekade system/tjänster	Behörigheter ska hanteras enligt minst nivå 2 för efterlevnad i två prioriterade system/tjänster.* (se mognadsmodell för behörighetshantering)	2020-21	Regionstabschef	Informationssäkerhets-samordnare  Förvaltningsledare för utpekade system/tjänster
Kontroll av att användarbehörigheter i utpekade kritiska informationssystem är anpassade till medarbetarnas arbetsuppgifter vad gäller åtkomstnivåer och tidsbegränsning för tilldelad åtkomst	Informationsägare	Användarbehörigheterna i två verksamhetskritiska system har verifierats vid planeringsperiodens första uppföljning (2020-12-31).	2020	Objektägare/systemägare för utpekade system/tjänster	Informationssäkerhets-samordnare
Etablering av central behörighetskälla och införande av spårbara, centralt hanterade beställningar av behörigheter	EKO-katalogens förvaltning (förvaltnings-ansvarig för behörighet-källa)	Central behörighetskälla etablerad med kvalitetssäkrade grundattribut/informationsmängder.	2020	Objektägare/systemägare för EKO- katalogen	Informationssäkerhets-samordnare



### 3.17 Mål RS: Regionens ledningssystem för informationssäkerhet (LIS) ger ändamålsenligt och målgruppsanpassat stöd till medarbetarna

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
E-utbildning för medarbetare i informationssäkerhet genomgås	Samtliga medarbetare inom regionen, OC, EC	E-utbildning för medarbetare i informationssäkerhet har fullföljts av 80% procent av medarbetarna 2020-12-31.  Mätetal för 2021-12-31: 95%  Nya medarbetare har genomgått e-utbildningen senast 3 månader efter att de påbörjat sin tjänst inom regionen.	2020	OC	Informationssäkerhets-samordnare
E-utbildning för förvaltningsansvariga i informationssäkerhet/ systemsäkerhetsplan genomgås	Förvaltningsansvariga (förvaltningsledare)	E-utbildning för förvaltningsansvariga i informationssäkerhet har fullföljts av 70% procent av medlemmarna i identifierad målgrupp 2021-12-31	2021	Objektägare/systemägare (för respektive förvaltningsobjekt)	Informationssäkerhets-samordnare
Översyns utförs för styrdokument inom ledningssystem för informationssäkerhet	Samtliga medarbetare inom regionen	Styrdokument har uppdaterats och kompletterats	2020	Informationssäkerhets-samordnare	Kvalitetsstrateg (förvaltningsansvarig för regionens ledningssystem)

### 3.18 Mål RS: Krav på skyddet mot cyberattacker finns etablerade

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Identifiera de mest allvarliga intrångshoten gällande cyberattacker (intrång, stölder och bedrägerier)	IT-säkerhetsansvarig	De 10 st mest allvarliga intrångshoten gällande cyberattacker (intrång, stölder och bedrägerier) har identifierats	2020	Regionstabschef	Informationssäkerhets-samordnare, IT-säkerhetsansvarig
Hantera skyddsåtgärder för de mest allvarliga intrångshoten gällande cyberattacker	IT-säkerhetsansvarig	De 10 mest allvarliga intrångshoten (enligt föregående punkt) har hanterats i åtgärdsplan för skyddsåtgärder	2021	Regionstabschef	IT-säkerhetsansvarig, informationssäkerhets-samordnare,

### 3.19 Mål RS: Chefer har fått utökat stöd att klara sina ansvarsområden relaterade till informationssäkerhet

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Rollen Registerkoordinator har fått tydliggjort uppdrag som stöd till chefer inom varje verksamhetsområde	OC	Uppdrag för Registerkoordinator framtaget och etablerat i verksamheterna.	2020	Regionstabschef	Dataskyddsbud
E-utbildning för rollen Registerkoordinator tas fram	Registerkoordinatorer	E-utbildning framtagen.	2020	OC, AC, EC	Dataskyddshandläggare
Forum för Registerkoordinatorer upprätthålls	Registerkoordinatorer	Forum/träffar för samverkan och utbildning för Registerkoordinatorer hålls löpande.	2020-21	Dataskyddsbud	Dataskyddshandläggare
E-utbildning för chefer i informationssäkerhet och dataskydd genomgås	RD, förvaltningsområdeschefer, OC, AC, EC	Samtliga regionens chefer har genomgått e-utbildning 2020-12-31	2020	Förvaltningsområdeschef RS	Informationssäkerhets-samordnare

		Nya chefer har genomgått e-utbildningen senast 3 månader efter att de påbörjat sin chefstjänst			
Framtagning av utbildning för Regionstyrelsen i informationssäkerhet och dataskydd	Regionstyrelsen	Utbildning framtagen för Regionstyrelsen	2020	Regionstabschef	Informationssäkerhets-samordnare
E-utbildning för Regionstyrelsens medlemmar i informationssäkerhet/systemsäkerhetsplan genomgås	Regionstyrelsen	Samtliga medlemmar i Regionstyrelsen har genomgått utbildning i informationssäkerhet och dataskydd 2020-12-31	2020	Regionstabschef	Informationssäkerhets-samordnare

### 3.20 Mål RS: Införande av ny modell för förvaltningsstyrning för regionens IT-stöd har påbörjats och modellen har tydliggjort fördelning av informationsägarskap

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Modell och mall för systemsäkerhetsplan (SSP) ska utarbetas och anpassas till aktuell förvaltningsmodell	Förvaltningsansvariga och informationsägare	Mall för SSP framtagen	2020	Informationssäkerhet-samordnare	Samordnare för förvaltningsstyrning, IT-säkerhetsansvarig
Systemsäkerhetsplan (SSP) ska tas fram för kritiska IT-system som stödjer samhällsviktiga verksamheter	Förvaltningsansvariga och informationsägare	25% av IT-system som är kritiska för samhällsviktig verksamhet inom regionen har framtagen, godkänd SSP 2020-12-31.  75% av IT-system som är kritiska för samhällsviktig verksamhet inom regionen	2020-21	Objektägare/systemägare (för respektive förvaltningsobjekt)	Informationssäkerhets-samordnare

		har framtagen, godkänd SSP 2021-12-31.			
Regiongemensamt verktyg för digitalt stöd gällande förvaltningsstyrning ska tillämpas för regionens IT-stöd som stödjer samhällsviktig verksamhet.	Förvaltningsansvariga och informationsägare	Verktyg är etablerat och klart att användas	2020	Regionstabschef	Samordnare för förvaltningsstyrning
Beslut fattas om att informationsklassning och riskanalyser ska utföras i regiongemensamt verktyg för digitalt stöd gällande förvaltningsstyrning	Informationsägare	Beslut fattat	2020-21	Regionstabschef	Informationssäkerhets-samordnare

### 3.21 Mål RS: Interna revisioner gällande regionens tillämpning av dataskyddslagstiftningen visar på hög grad av efterlevnad

Aktivitet	Målgrupp	Mätetal	Tidsplan	Ansvarig för genomförande	Kontaktperson/stöd
Intern revision genomförs gällande att konsekvensbedömningar har upprättats för samtliga högrisk-PU-behandlingar.	Registerägare	100% av identifierade högriskbehandlingar har en genomförd konsekvensbedömning	2020	Dataskyddsbud	Dataskyddshandläggare
Intern revision genomförs gällande att åtgärdsplaner efter konsekvensbedömningar har upprättats för samtliga högrisk-PU-behandlingar.	Registerägare	100% av identifierade högriskbehandlingar har en upprättad åtgärdsplan	2020	Dataskyddsbud	Dataskyddshandläggare
Intern revision genomförs gällande arbetssätt för systematisk registrering av PU-behandlingar.	Registerägare	100% av verksamheterna har rapporterat efterlevnad för systematiskt arbetssätt	2020	Dataskyddsbud	Dataskyddshandläggare

## 4 Beskrivning av hur handlingsplanen avser uppnå krav enligt särskilda perspektiv

### **Jämställdhet- och jämlikhet, Barnens rättigheter**

Informationssäkerhetsarbetet är könsneutralt ur ett jämställdhetsperspektiv. Att utarbeta rutiner och utbildning för att hantera information och personuppgifter på ett säkert sätt ska bidra till ökad trygghet för alla Regionens patienter oavsett kön, ålder, etnicitet.

### **Miljöperspektiv**

Handlingsplanen bedöms inte heller ha någon direkt miljöpåverkan i form av t ex materielförbrukning eller mängden avfall. Aktiviteterna innebär inte något ökat resande.

### **Ekonomi**

De flesta aktiviteter i planen kräver arbetstimmar med deltagare från olika avdelningar inom Regionstaben och verksamheter. För 2020 finns budget för informationssäkerhet inom Enheten för krisberedskap, säkerhet och miljö. Budgeten är främst riktad mot systemstöd för informationsklassning samt de förberedelser som krävs för anpassning till Dataskyddsförordningen.

## 5 Uppföljning

De övergripande handlingsplanerna följs upp i tertilsrapport, delårsrapport och årsbokslut. Utifrån dessa uppföljningar får avdelningschefer och områdeschefer under maj och december månad särskilda redovisningar om måluppfyllelse och hur arbetet går med handlingsplanens aktiviteter.

Regionstabschef ansvarar för uppföljningen med hjälp av ansvarig verksamhetsstrateg för respektive handlingsplan. Uppföljningen sker genom en kortfattad beskrivning om läget för varje handlingsplan, vad som gjorts och vad som planeras samt om målen i handlingsplanen bedöms vara uppfyllda till årets slut.

## 6 Definitioner

Tydliggör begrepp och ord som används i handlingsplanen och som inte kan ses som allmänt vedertagna.

PU = Personuppgifter