# Informationssäkerhetsberättelse 2019

Beslutad 2020-04-29 § 59, av: Regionstyrelsen

REGION JÄMTLAND HÄRJEDALEN

# Sammanfattning/bakgrund

Samtidigt som Regionens informationssäkerhetsarbete har tagit stora och viktiga steg framåt de senaste åren så går utvecklingen inom IT-området oerhört snabbt och de tekniska möjligheterna ökar för all verksamhet inom Regionen. Den pågående digitaliseringen påverkar också arbetet i hög grad. Verksamheterna idag har ett högt IT-beroende och därmed ökar också våra risker och sårbarheter. Det finns ett växande behov av att Regionen har förmåga att arbeta med systemförvaltning på ett strukturerat och kvalitetssäkrat sätt. Detta är en grundförutsättning för att kunna nyttja digitaliseringens fördelar inom en allt större del av verksamheten.

Ny lagstiftning som påverkar arbetet i hög grad är NIS-direktivet med tillhörande svensk lagstiftning (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) som trädde i kraft i november 2018. En ny reviderad säkerhetsskyddslag trädde i kraft i april 2019 och vikten av informationssäkerhetsarbete kopplat till säkerhetsskydd och civilt försvar/totalförsvar ökar i omfattning. Utvecklingen har således gått mot en hårdare kravbild och ett ökat behov av tydligare kontroll avseende att det finns rätt åtgärder på plats för att skydda vår information. Behovet av ett systematiskt informationssäkerhetsarbete och riskbaserade gransknings- och uppföljningsverktyg har aldrig varit större.

Behov finns att snabba på genomförande av riskanalyser och informationsklassningar i syfte att få ett bättre underlag för prioriteringar av förebyggande säkerhetsåtgärder som minskar sannolikheten för IT-avbrott. Om ett IT-avbrott ändå inträffar måste verksamheterna ha en genomtänkt planering för hur man ska agera med hjälp av reservrutiner. Ett arbete med avbrottsplanering har därför startats upp i ett flertal verksamhetsområden i Hälso- och sjukvården under 2019. Arbetet är prioriterat att fortsätta under 2020.

Inspektionen för vård och omsorg (IVO) genomförde under våren 2019 en inspektion av Region Jämtland Härjedalens ledningssystem för informationssäkerhet utifrån NIS direktivet och motsvarande svensk lagstiftning (lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster). IVO har inte identifierat några brister inom området, så bedömningen är att informationssäkerhetsarbetet kan fortsätta på inslagen väg.

Ett antal förbättringsåtgärder har vidtagits såväl inom informationssäkerhets – som IT säkerhetsarbetet. Det har också genomförts riskanalyser samt internrevision och internkontroll. Behoven inom området är fortsatt stora och det krävs avvägda prioriteringar i det fortsatta arbetet. För att skapa effektiv styrning av arbetet som även tar höjd för digitaliseringen, har en översyn och justering gjorts avseende vilka interna forum som ska finnas för informationssäkerhetsfrågorna. Dataskyddsorganisationen kommer att stärkas upp kommande år, vilket är välbehövligt.

# INNEHÅLLSFÖRTECKNING

# 1 Informationssäkerhetsarbete 2019

Utvecklingen har gått mot en hårdare kravbild och ett ökat behov av tydligare kontroll avseende att det finns rätt åtgärder på plats för att skydda vår information. Behovet av ett systematiskt informationssäkerhetsarbete och riskbaserade granskning- och uppföljningsverktyg har aldrig varit större. Samtidigt som Regionens informationssäkerhetsarbete har tagit viktiga steg framåt de senaste åren så går utvecklingen inom IT-området oerhört snabbt och de tekniska möjligheterna ökar för all verksamhet inom Regionen.

Verksamheternas redan tidigare höga IT-beroende har ökat ytterligare i och med införandet av fler IT-stöd och ökad digitalisering. Många IT-stöd är idag i mycket hög grad verksamhetskritiska vilket gör att sårbarheten ökar för eventuella avbrott i tillgängligheten för dessa IT-stöd. Behov finns att snabba på genomförande av riskanalyser och informationsklassningar i syfte att få ett bättre underlag för prioriteringar av förebyggande säkerhetsåtgärder som minskar sannolikheten för IT-avbrott. När IT-avbrott väl inträffar ska verksamheterna ha en genomtänkt planering för hur man ska agera med hjälp av reservrutiner som kan användas under ett avbrott.

Det finns ett växande behov av att Regionen har förmåga att arbeta med systemförvaltning på ett strukturerat och kvalitetssäkrat sätt. Detta är en grundförutsättning för att kunna nyttja digitaliseringens fördelar inom en allt större del av sina verksamheter.

NIS-direktivet med tillhörande svensk lagstiftning (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) trädde i kraft i november 2018. En ny reviderad säkerhetsskyddslag trädde i kraft i april 2019 och vikten av informationssäkerhetsarbete kopplat till säkerhetsskydd och civilt försvar/totalförsvar ökar i omfattning.

Mycket av det som prioriterades inför 2019 har genomförts eller är påbörjat. Allt har inte hunnits klart, utan arbete får fortsätta under kommande år. Behovet av informationssäkerhets- och dataskyddsarbete ökar. Behovet av stöd i verksamheterna är också stort. Inför 2020 planeras en utökning av resurs för dataskyddsarbetet, vilket känns viktigt för det fortsatta arbetet.

Informationssäkerhet ska enligt föreskriften HSLF-FS 2016:40, Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, vara en del av den årliga patientsäkerhetsberättelsen. I Region Jämtland Härjedalen finns därför, förutom denna informationssäkerhetsberättelse, en kortare sammanfattning avseende informationssäkerhet i patientsäkerhetsberättelsen.

## 1.1 Ledningssystem för informationssäkerhet (LIS)

Under ett flertal år lades stort fokus på att bygga upp ledningssystemet för informationssäkerhet. Ett kontinuerligt arbete krävs dock för att utveckla och hålla ledningssystemet aktuellt. Nya områden tillkommer i takt med att arbetssätt förändras och vidareutvecklas. Under 2018 byggdes ett regelverk upp för personuppgiftshantering. Införandet av Microsoft Office 365 (O365) med nya lagringsytor och kommunikationskanaler har ytterligare bidragit till att regler och rutiner behövs för att styra informationshanteringen

via de tjänster som ingår i O365. Ledningssystemet för informationssäkerhet har inte varit i fokus under 2019, omtag behöver göras kommande år.

## 1.2 Ledningens genomgång och långsiktig handlingsplan

Vid ledningens genomgång (2 gånger per år) är informationssäkerhet en av de delar som följs upp avseende ledningssystemets verkan. Detta har genomförts enligt plan. Vid varje tillfälle finns ett antal beslutspunkter för informationssäkerhet. Detta är en viktig del för att uppnå ständiga förbättringar i ledningssystemet. Denna genomgång med dess beslut om åtgärder tillsammans med den långsiktiga tvååriga handlingsplanen för informationssäkerhet skapar ett planerings- och uppföljningsunderlag som underlättar arbetet med att förbättra säkerheten. En ny handlingsplan för informationssäkerhet 2020 – 2021 är utarbetad. Exempel på frågor som varit uppe på ledningens genomgång är:

- Behovet av en strategi för informationssäkerhet och dataskydd.
- Behovet av att utse informationsägare för de 3–4 viktigaste verksamhetsprocesserna inom respektive område. Dessa är kravställare på säkerheten i sina processer.
- Tydliggöra registerkoordinatorernas uppdrag och stötta dessa för att de även ska kunna ge metodstöd för klassningar och riskanalyser. Syftet är att uppnå en förbättrad dataskyddsorganisation.
- Säkerställa att kritiska IT-system har tillgång till ändamålsenlig förvaltningsmodell och stöd. Det kan bidra till att sänka det mycket höga personberoendet för nyckelroller inom förvaltningen av verksamhetskritiska IT-system.
- Tydliggör ansvaret för att uppnå tillräcklig säkerhet i SCADA-systemen och tilldela resurser för att detta arbete ska kunna utföras.

## 1.3 Styrning av informationssäkerhetsarbete och digitalisering

Styrningen av regionens systematiska satsningar på digitalisering har under 2019 börjat ta form. Exempel på detta är inrättandet av *styrgrupp digitalisering* (tidigare ”styrgrupp digitalisering i vården”). Dessutom har *Utvecklings- och digitaliseringsenheten* skapats och de första resurserna där har påbörjat sitt arbete. Det är väsentligt att säkerhetsaspekter kan börja integreras i arbetsprocesserna för denna enhet redan från början. Exempelvis ska säkerhetskrav tas med i kravfångsten vid anskaffning av nya (digitaliserings-)lösningar. Inte minst gäller det att utse informationsägare för den information som hanteras i de digitala tjänsterna för att på så sätt få en tydligare kravställning och kravuppföljning av tjänstens säkerhetsfunktioner.

Under 2019 har en översyn därav gjorts avseende vilka forum som behövs för att hantera frågor kring informationssäkerhet och dataskydd. Informationssäkerhetsrådet som funnits under 2017 t o m 2019 ska fr o m 2020 avvecklas. Istället tas vissa av motsvarande frågor som detta råd tagit upp inom ramen för det nyinrättade *rådet för informationsförvaltning*. Andra säkerhetsrelaterade frågor kan också tas upp av regionens *styrgrupp för digitalisering*. Dataskyddsarbetet planeras och styrs i första hand i *funktionsområdesträffar för dataskydd*. Utöver det finns också en mindre arbetsgrupp för informationssäkerhet, där IT säkerhetssamordnare deltar, då det är av vikt att IT säkerhetsfrågorna kontinuerligt är en del av Regionens informationssäkerhetsarbete.

## 1.4 Dataskydd och personuppgiftshantering

För att dataskyddslagstiftningen ska kunna efterlevas krävs etablerade arbetssätt, skyddsåtgärder och en fungerande förvaltningsorganisation. Under 2019 har en översyn av förvaltningsorganisationen gjorts, då det har varit svårt att bemanna alla roller och organisationen har haltat. Behovet av stöd till verksamheterna gällande dataskydd är relativt stort. Utifrån översynen föreslogs att nuvarande DSO ska fortsätta i sin roll, i en omfattning av ca 20–40%. Som organisatoriskt stöd till DSO föreslås fortsatt biträdande DSO för Hälso- och sjukvården motsvarande 10% att finnas kvar. Rollen registerkoordinator föreslås också finnas kvar inom respektive avdelning/verksamhetsområde. Inför 2020 kommer en rekrytering av en ny Dataskyddssamordnare att rekryteras. Både Dataskyddsombud och dataskyddssamordnare kommer att vara organisatoriskt placerad i Samordningskansliet.

Regionen har rutiner för rapporteringen av PU-incidenter till Datainspektionen, som är tillsynsmyndighet för dataskyddsområdet. Regionen är skyldig att rapportera inträffade incidenter inom 72 timmar. Under 2019 har 3 incidenter rapporterats i enlighet med lagkraven.

Dataskyddsarbetet har under 2019 bedrivits genom bland annat samordnings- och utbildningsinsatser av regionens utsedda registerkoordinatorer som är lokala handläggare av personuppgiftsbehandlingar inom respektive verksamhet. Regelbundna träffar (4-5 gånger/år) har genomförts med registerkoordinatorerna. Dessa tillfällen är viktiga för informationsutbyte och samarbete kring dataskyddsarbetet i verksamheterna.

Ett antal konsekvensbedömningar har utförts för s.k. högriskbehandlingar (av känsliga och extra skyddsvärda personuppgifter) enligt krav från GDPR/dataskyddslagstiftningen. Ett omfattande arbete inom dataskyddsarbetet är att etablera biträdesavtal för de PU-behandlingar som utförs för Regionens räkning av externa parter. Regionen arbetar löpande med att få dessa avtal på plats. Ett prioriterat område inom dataskydd har varit hantering av personuppgifter inom personaladministration (HR). Upprättande av ett flertal s.k. personuppgiftsbiträdesavtal med externa leverantörer som behandlar regionens personuppgifter i sina IT-tjänster har också gjorts för att avtalsmässigt säkra behandlingen av dessa uppgifter. Även detta är ett krav enligt lagstiftningen.

## 1.5 Behov av en strategi för informationssäkerhet

Under 2019 har behoven av att ha tillgång till en strategi för regionens informations-säkerhetsarbete blivit allt tydligare. En strategi kan bidra till att göra befintlig (kortfattad) policy för informationssäkerhet och dataskydd mer konkret genom att peka ut önskade principer, framgångsfaktorer/indikatorer och arbetssätt. Strategin kan bidra till ett ökat fokus på styrning mot önskade arbetssätt och prioriteringen av säkerhetshöjande aktiviteter.

Behovet av en strategi lyftes vid ledningens genomgång november 2019 som rekommendation till beslut, men prioriterades inte för beslut vid det tillfället.

## 1.6 Avbrottsplanering för vårdverksamheterna

Hösten 2019 påbörjades arbete med att kartlägga kritiska beroenden till information och IT-system i ett antal verksamhetsområden i Hälso- och sjukvården. Arbetet har bedrivits i workshopform där metodstöd har givits till chefer, verksamhetsutvecklare och vårdpersonal kring hur kartläggningar och konsekvens-bedömningar ska göras. Ett gemensamt arbetssätt för detta har inletts. Avgränsning har gjorts till kritisk information – övriga avbrottstyper

såsom elbortfall, vattenavbrott och bortfall av personalbemanning har inte tagits med. Arbetet har försvårats av att ett tydligt utpekat ansvar har saknats i form av riktlinjer för kontinuitetsplanering, något som ska tas fram under 2020. Arbetet med avbrottsplanering kommer fortsatt att vara prioriterat under 2020.

## 1.7 Inspektion från IVO – NIS-direktivet

Inspektionen för vård och omsorg (IVO) genomförde under våren 2019 en inspektion av Region Jämtland Härjedalens ledningssystem för informationssäkerhet utifrån NIS direktivet och motsvarande svensk lagstiftning (lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster). Den nya lagen ska syfta till en ökad informationssäkerhet hos samhällsviktiga aktörer vilket skyddar individer och organisationer. Hälso- och sjukvård omfattas generellt av denna lagstiftning. Lagen innebär skyldigheter att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande respektive avsevärd inverkan på kontinuiteten i tjänsten. Föreläggande förenat med vite kan tillämpas om lagen inte efterlevs.

IVO är tillsynsmyndighet för de samhällsviktiga tjänster som omfattar hälso- och sjukvård. Denna lag trädde i kraft ca ett halvår innan inspektionen (november 2018) varför tillämpningen av lagen under 2019 ännu inte blivit helt etablerad.

Vid inspektionen har IVO gjort en bedömning av Region Jämtland Härjedalens proaktiva förmåga (strukturerat säkerhetsarbete enligt ISO 27000 inklusive att riskbaserat arbete bedrivs) liksom av den reaktiva förmågan (upptäcka och rapportera incidenter). Bland det som bedömdes fanns arbetet med risker och hot, kontohantering/behörigheter, fördelning av ansvar samt styrning av informationsägarskap. IVO har meddelat att de inte funnit några brister i Regionens arbete. Bedömningen är att informationssäkerhetsarbetet kan fortsätta arbeta på inslagen väg. Betydelsen av det riskbaserade arbetet samt att arbeta med ledningssystem för informationssäkerhet (LIS) och att integrera IT säkerhet och MT säkerhet i arbetet betonades.

## 1.8 Förbättrad förvaltningsstyrning inom regionen

Under 2019 har steg tagits för att uppnå en förbättrad och mer strukturerad styrning av regionens förvaltning av IT-tjänster/-system. Detta har gjorts via en externt driven förstudie, beställd av regiondirektören. Förstudien har kartlagt IT-verksamheten och tagit fram rekommendationer för förbättrade arbetssätt och organisation.

Förstudien rekommenderar bland annat att regionens IT-resurser (som idag delvis finns utspridda i olika verksamheter) sammanförs som regiongemensamma resurser. Dessutom rekommenderas att en strukturerad förvaltningsstyrning baserad på pm3-modellen införs för merparten av regionens IT-stöd. Hur budgetstyrning ser ut för förvaltningen är också en kritisk faktor som behöver revideras för att kunna få effektivitet i styrning och utveckling. Hur denna styrning utformas kommer att få stor inverkan på möjligheterna att kunna bedriva ett ändamålsenligt säkerhetsarbete.

Området förvaltningsstyrning är fortsatt mycket viktigt för Regionen. Att utveckla och införa en modernare förvaltningsmodell bedöms som en kritisk framgångsfaktor för digitaliseringsarbetet och för hanteringen av IT-systemen inom Regionen i stort. Under 2019

har arbete bedrivits inom Samordningskansliet med att ta fram stöd för en ny förvaltningsmodell för regionen baserad på pm3-modellen.

För att möta kraven på att regionen har tillgång till ett integrerat stöd för strukturerad förvaltning av Regionens IT-system/-tjänster och personuppgiftsbehandlingar har verktyget DIGFrame anskaffats under 2019. Detta verktyg har hittills använts i liten skala för att kunna lära mer om hur ett IT-baserat verktyg av denna typ kan införas i bredare omfattning inom regionen under kommande år.

## 1.9 Godkända lagringsytor

Det finns, generellt sett, ett stort behov av att ensa och tydliggöra var medarbetarna får lagra information. Detta gäller den information som hanteras utanför verksamhetssystemen (t ex HR-system och vårdadministrativa system). Införandet av Office365 som regiongemensam plattform under 2018 utökade antalet tillgängliga lagringsytor ytterligare och införde dessutom dimensionen med externt lagrad information i molntjänst (utanför regionens lokala IT-miljö). Under 2019 har därför ett arbete initierats med att etablera ett utökat stöd för informationsklassning som också innehåller tydliga hanteringsregler för var informationen får hanteras/lagras baserat på dess klassningsnivåer. Eftersom detta arbete innehåller mycket av utbildningsinsatser för att lära medarbetarna på en övergripande nivå hur informationen ska klassas innebär det att en relativt stor arbetsinsats kommer att krävas framöver. Framtagning av regelverket och anvisningar har påbörjats under 2019 och arbetet fortsätter under 2020-21 med en etablering av arbetssättet i verksamheterna genom utbildning.

## 1.10 Informationsägarskap

En viktig fråga för hur det systematiska säkerhetsarbetet lyckas är att ha fortsatt fokus på hur ägarskap utses för informationen som regionen hanterar. Eftersom information är en tillgång på samma sätt som exempelvis fastigheter och utrustning krävs att vem som är informationens ägare är tydliggjort.

Exempel på där denna informationsägarroll (eller avsaknad av utpekad roll) blir extra tydlig är då det gäller utdata för verksamhetsuppföljning (datalager/beslutsstöd). För att kunna uppnå en effektiv och kvalitetssäkrad uppföljning krävs tillgång till relevant utdata från regionens verksamhetssystem in till beslutsstödet. En framgångsfaktor i detta arbete är då att ha en utsedd informationsägare för varje uppföljningsprocess, t ex uppföljning ekonomi, uppföljning vård etc. Denne ägare ska ansvara för att utdata är kvalitetssäkrad och uppfyller beslutsstödet krav på korrekthet, aktualitet och fullständighet. På motsvarande sätt finns behov av utpekat informationsägarskap i andra processer som kräver kvalitetssäkrad information för att fungera. Att koppla informationsägarskap till processägarskap har därför identifierats som en viktig framgångsfaktor för säkerhetsarbetet. Mycket arbete återstår inom detta område.

## 1.11 Förstudie behörighetshantering

Ett flertal lagkrav, däribland Patientdatalagen, Socialstyrelsens föreskrifter HSLF-FS 2016:40 samt GDPR med den tillhörande nya svenska dataskyddslagen, anger att behörigheter ska styras och följas upp på ett strukturerat sätt så att åtkomst till skyddsvärda uppgifter kan minimeras. Även NIS-direktivet med tillhörande svensk lagstiftning för informationssäkerhet i samhällsviktiga och digitala tjänster (SFS 2018:1174) ställer krav på effektiv och säker behörighetshantering. Därför har regionen under 2019 genomfört en förstudie och utrett hur

behörighetshanteringen kan förbättras genom en mer strukturerad och automatiserad hantering. Detta syftar till att underlätta tilldelning och uppföljning av behörigheter så att rätt information kan nås av rätt medarbetare i rätt tid.

Förstudien innehåller en kartläggning av nuvarande behörighetshantering samt förslag för hur Regionen ska uppnå en förbättrad och säkrare behörighetshantering. Resultaten från förstudien innehåller dessa två huvuddelar:

- Ökad centralisering av behörighetsbeställningar för regionens IT-stöd
- Ökad automation vid tilldelning och borttag av behörigheter i regionens IT-stöd

För att uppnå förbättrade arbetssätt för de två delarna har förstudien föreslagit att etablera en gemensam, kvalitetssäkrad central behörighetskälla (som ska kunna styra behörigheter i anslutna system) samt att införa en central behörighetsportal som underlättar beställning och uppföljning av behörigheter. IT har fått i uppdrag av Regionstabschef att arbeta med dessa delar. En omvärldsbevakning (RFI) avseende behörighetsportal är påbörjad.

Genom att införa dessa delar kan en väsentligt förenklad och effektiviserad behörighets-hantering uppnås jämfört med dagens hantering som i hög grad är decentraliserad och innehåller många manuella moment. Exempelvis kan åtkomst till känsliga uppgifter minimeras så att endast de användare som har behov av åtkomst ges sådan åtkomst. Tilldelning av inaktuella behörigheter kan därmed undvikas.

## 1.12 Loggkontroller av obehörig åtkomst till patientuppgifter

Under 2019 har en ny, väsentligt förbättrad version av loggverktyg (LogPoint AAHC) införts för kontroll/uppföljning av åtkomster till det vårdadministrativa systemet COSMIC. Detta verktyg möjliggör en mer systematiserad och effektiviserad loggkontroll vilken ska bidra till högre efterlevnad av såväl GDPR som Patientdatalagen då det gäller att säkra rätt åtkomst till patientuppgifter. Kontrollerna består av såväl löpande stickprovskontroller som riktade kontroller vid misstanke om obehörig åtkomst.

Under 2019 har också en lösning utvecklats inom Regionen för att patienten själv ska kunna läsa loggarna för sin vårdinformation i COSMIC via den nationella Journal via Nätet-tjänsten/ 1177. Denna möjlighet, som ska införas under 2020, innebär ett alternativ där patienten själv ges tillgång till logginformationen via direktåtkomst. Sedan tidigare har patienten vid behov fått begära ut loggutdrag på pappersutskrifter från Regionen, något som även fortsatt blir möjligt.

Loggkontroller genomförs löpande i vårdens verksamheter och uppföljning avseende att kontroller genomförs sker vid internrevisionen.

## 1.13 SCADA-säkerhet

Arbete med SCADA-säkerhet (säkerhet i styrsystem för fastighetsdrift och andra försörjningstjänster) har under 2019 påbörjats inom ramen för regionens arbete med säkerhetsskydd och civilt försvar. Kartläggningar av säkerheten i SCADA-system har planerats i samverkan med informationssäkerhetsfunktionen. På grund av resursbrist är arbetet försenat och planeras genomföras 2020.

## 1.14 Säkerhet i medicintekniska system och utrustningar

Regionens centrala informationssäkerhetsarbete har ännu inte omfattat medicintekniska produkter. Hur detta ska ske behöver kartläggas framöver, bland annat genom omvärldsbevakning. Att medicinteknisk säkerhet hör nära samman med ett strukturerat informationssäkerhetsarbete framstår som mer och mer tydligt och påtalades även av IVO vid deras besök. Samverkan med den medicintekniska verksamheten kommer att inledas under kommande år.

# 2 Riskanalyser och egenkontroll

## 2.1 Internrevision avseende informationssäkerhetsarbetet

Under året har två omgångar med internrevisioner med revisionspunkter för informationssäkerhet genomförts inom ramen för regionens övergripande internrevisionsprogram. Denna revision har skett hos utvalda verksamheter enligt löpande treårig revisionsplan. Följande tre revisionspunkter har genomförts inom ramen för denna revision:

- Genomförande av e-utbildning i informationssäkerhet (där dataskydd ingår som en del)
- Chefers kännedom om sitt ansvar för behörighetshantering (i IT-systemen) för sina medarbetare
- Kännedom om regiongemensam regel för behörighetshantering

Revisionen visar på en låg kännedom om/genomförande av ovanstående delar hos samtliga reviderade verksamheter. Resultatet kan tolkas som att de angivna områdena/processerna som relaterar till informationssäkerhet ännu inte har integrerats tillräckligt i det dagliga arbetet.

## 2.2 Övergripande riskanalys avseende informationssäkerhet

Under 2017 gjordes en övergripande riskanalys avseende informationssäkerhet (gemensamma generella risker för regionen), samma analys reviderades 2018. Ambitionen är att denna övergripande riskanalys ska revideras två gånger per år, men under 2019 hanns detta inte med. Analysen beaktar två områden; 1. De största riskerna i det systematiska arbetssättet för informationssäkerhet samt 2. De mest framträdande specifika operativa riskerna för Regionens informationshantering.

De huvudsakliga övergripande risker som identifierats inom ovanstående två områden är:

1. Våra medarbetare har inte kunskap om var de får lagra olika typer av information (utanför verksamhetssystemen)
2. Kritiska IT-system har inte informationsklassats (säkerhetanalyserats) och åtgärdsplanerats vilket medför ohanterade sårbarheter som riskerar stora störningar hos kritiska verksamheter – kan ge obehöriga åtkomst till känslig information och hindra åtkomst till IT-systemen
3. Dataintrång sker genom bristande säkert i behörighet/inloggning/kryptering – detta kan medföra spridning av känsliga uppgifter till obehöriga

## 2.3 Övriga riskanalyser och egenkontroll

Övriga riskanalyser inom informationssäkerhet som har genomförts under 2019 är:

- Riskanalys avvikelsehantering – skydd av uppgifter i avvikelseärenden
- Riskanalys ögonremisser
- Riskanalys övergripande behörighetshantering
- Riskanalys konfigurationsdatabas IT-infrastruktur

## 2.4 Internkontroll/egenkontroll

Under 2019 har arbetet med att förbättra uppföljning av informationssäkerheten främst inriktats på att bygga upp de processer och verktyg som krävs för att kunna mäta och följa upp säkerhetsarbetet. Uppföljningen ska främst göras på aktivitetsnivå vilket bedöms kunna bidra till en enkel och tydlig uppföljning för alla parter.

Något som lyfts fram som försvårande för kontroll- och uppföljningsarbetet är den underrapportering som finns gällande avvikelser kopplade till informationssäkerhet. Orsaken till detta är främst brister i medvetenhet om att dessa avvikelser ska rapporteras men även brister i stödet för avvikelserapportering (Centuri) har identifierats. Hur man ska identifiera en avvikelse av denna typ beskrivs i regionens nya e-utbildning för informationssäkerhet. I takt med att denna utbildning har genomgåtts av fler medarbetare kommer också medvetenheten att öka för att denna typ av rapportering ska göras.

Internkontrollen (riskbaserad), där egenkontrollen i respektive verksamhet är en del, är tillsammans med avvikelsehanteringen ”motorn” i förbättringsarbetet inom såväl informationssäkerheten som annan kvalitetsutveckling. Under 2019 har internkontrollen avseende informationssäkerhet fått större fokus och tid jämfört med föregående år.

## 2.5 Behörigheter i SQL-databaser

I samband med egenkontroller av Regionens största SQL-kluster identifierades felaktigt satta behörigheter som medgav samtlig regionpersonal teknisk möjlighet att läsa innehåll i en känslig databas. Följande åtgärder vidtogs:

- Regionens DSO anmälde bristen till Datainspektionen som en GDPR-incident
- Aktuell objektsleverantör korrigerade omgående bristen
- Säkerhetsrevision av aktuellt SQL-kluster beställdes av extern konsultfirma

Under slutet av 2019 har en extern konsult genomfört en Säkerhetsrevision på Regionens största SQL-kluster.

Revisionen innefattar

- Kontroll av behörigheter och tjänster utifrån principen om lägsta möjliga behörighet gällande databaser, roller och användare
- Analys av genomförda sårbarhets- och regelefterlevnadsrapporter
- Framtagande av åtgärdsförslag gällande identifierade brister

## 2.6 Avvikelser om dataintrång

Under 2019 finns följande fall av anmälda dataintrång, alltså fall där misstänkt dataintrång med obehörig läsning av patientjournal har rapporterats:

- Ett fall där det konstaterades otillåten journalgranskning som ledde till polisanmälan. Ärendet lades senare under året ned av polismyndigheten
- Ett fall där det inte kunde bevisas att fel begåtts
- Ett fall där intrång fortfarande utreds

Ytterligare ett pågående fall finns där polisen i slutet på 2019 påbörjat utredning. Detta handlar om en anmälan som gjordes under 2018.

## 2.7 Egenkontroll dataskydd – personuppgiftshantering

Regelbundna träffar sker med Registerkoordinatorer (lokala personuppgiftshandläggare i verksamheterna). Arbetet med registerinventering av personuppgiftsbehandlingar har tydliggjorts. GAP-analyser och åtgärdsplaner begärs löpande in från verksamheterna. Incidentrapportering och konsekvensbedömningar följs upp. Resultat har rapporterats på ledningens genomgång.

## 2.8 Riskanalys: exponering via leverantörer

Under året har extern konsult genomfört en riskanalys gällande Regionens riskexponering för IT/informationssäkerhetsrisker från leverantörer. Input till arbetet har bland annat varit Försvarets radioanstalts publikation *Åtgärdsförslag - Angrepp via tjänsteleverantörer*.

## 2.9 NIS-analys baserat på Cyber Assessment Framework

Regionen har under 2019 genomfört en nulägesanalys gällande hur kraven i Lagen om informationssäkerhet i samhällsviktig verksamhet och digitala tjänster (2018:1174) efterlevs. Analysen har baserats på Cyber Assessment Framework som tagits fram av Brittiska NCSC.

Analysen består 39 st individuella utvärderingar inom följande fyra huvudområden:

- Hantering av säkerhetsrisker
- Försvar mot cyberattacker
- Detektering av cybersäkerhetsevent
- Minimera effekterna av cybersäkerhetsincidenter

Framtagandet av åtgärdsförslag har påbörjats och behöver slutföras under 2020.

# 3 Genomförda förbättringar

Ett flertal förbättringar har gjorts under 2019, exempel listas nedan.

- **Robust server-konfiguration:** Pilotprojekt har genomförts där en mer robust server-konfiguration baserat på internationella rekommendationer har arbetats fram.
- **Förbättringar i AD-struktur:** Pilotprojekt har genomförts där ett antal system flyttats in i den uppsatta segmenterade behörighetsstrukturen.

- **Säkerhetscentret:** Breddinförandet har fortgått under året och Regionen genomför nu kontinuerliga sårbarhetsskanningar.
- **Central logghantering:** Genomfört projekt för att samla in loggar från samtliga servrar och klienter för att möta lagkrav i både Dataskyddsförordningen och Lagen om Informationssäkerhet i samhällsviktig verksamhet och Digitala tjänster.
- **Office 365 intrångsförsök:** Regionen, tillsammans med de flesta andra kunderna av publika molntjänster såg under året en ökning i mängden intrångsförsök till de tjänster som nyttjas i molnet. Regionen såg under början av året hur intrångsförsöken, i en begränsad omfattning, resulterade i att anställdas konton låstes ut. För att motverka dessa och liknande brute force attacker har Regionen stängt alla autentiseringsmetoder mot Office 365 som kunnat nyttjas för att undgå flerfaktorsautentisering.
- **Rutin hantering skadlig kod:** Under året har rutin slutförts för hur Helpdesk och objektsleverantörer skall hantera och samarbeta kring misstänkta utbrott av skadlig kod.
- **Teknisk skuld:** Under året har Regionen och dess objektsleverantörer jobbat med att korrigera brister som ackumulerats över ett stort antal år. Det rör sig om tekniska förändringar i allt från operativsystem till nätverk och som sammantaget ökar Regionens robusthet mot både cyberangrepp och skadlig kod.
- **Klassning av tillgångar:** Införande av verktygsstöd för informationsklassning, riskanalyser samt förvaltningsstyrning.
- **Behörigheter:** Förstudie framtagen för förbättrad behörighetshantering.
- **Avbrottsplanering:** Kartläggning av beroenden till kritisk information i vårdverksamheterna och etablering av avbrottsrutiner för denna information.
- **Loggning:** Införande av nytt verktyg för granskning av loggar från vårdinformationssystem.
- **Kravställning vid anskaffning nya IT-stöd:** Tydliggörande av anskaffnings-process för nya IT-stöd/-tjänster.
- **Förvaltningsstyrning:** Etablering av ny modell för förvaltningsstyrning av förvaltningsobjekt/IT-tjänster.
- **Riskhantering generellt:** Utvärdering av riskverktyg som stöd vid riskhantering.
- **Utbildning:** Revidering av e-utbildning i informationssäkerhet för samtliga medarbetare.
- **Stöd till verksamheten:** Etablering av hanteringsregler kopplade till nivåer inom informationsklassning.
- **Införande av informationsskydd:** Etablering av skyddsfunktioner för skydd/kryptering av dokument och e-post.

# 4 Prioriterade åtgärder för 2020

Följande prioriterade åtgärdsområden finns med i den övergripande handlingsplanen för informationssäkerhet 2020-21 samt i planen för IT-säkerhet:

- Ta fram och etablera utbildning/stöd i informationssäkerhet till chefer och systemförvaltningsansvariga roller
- Etablera systematisk kontinuitetshantering för verksamhetskritiska informationssystem i utpekade vårdverksamheter
- Etablera en ändamålsenlig internkontroll med ett riskbaserat arbetssätt för informationssäkerhet (generellt)

- Identifiering, planering och genomförande av skyddsåtgärder för att efterleva NIS-direktivets krav enligt Cyber Assessment Framework
- Revidera regionens informationsklassningsmodell inklusive hanteringsregler genom att arbeta enligt MSB:s metodstöd för informationssäkerhet
- Etablera arbetssättet med informationsklassning och hanteringsregler i verksamheterna genom utbildning
- Fortsatt arbete med avbrottsplanering för vårdverksamheterna
- Fortsätta arbetet och slutföra de uppdrag som delats ut utifrån förstudie behörighetshantering
- Fortsatta förbättringar av system för sårbarhetsskanningar och logganalys
- Vidareutveckla användning och nytta av insamlade infrastrukturella loggar
- Utarbeta processtöd avseende informationssäkerhet och dataskydd för anskaffning och införande av nya IT tjänster

Utöver detta är det också prioriterat att fortsätta arbetet med informationsklassning och implementering av IT-verktyg för att stödja en mer strukturerad förvaltningsstyrning av regionens IT-tjänster och system.