Krisberedskap, säkerhet och miljö
Sanna Othman
Tfn: 063-147586
E-post: anna-lena.alfreds@regionjh.se

2018-05-08

RS/937/2018

Informationssäkerhets- och dataskyddspolicy

1 Inledning

Information är en av Region Jämtland Härjedalens viktigaste tillgångar och en förutsättning för all verksamhet och effektivitet. Region Jämtland Härjedalens verksamhet och trovärdighet får inte äventyras på grund av brister i informationshantering. Informationssäkerheten i Region Jämtland Härjedalen ska ytterst tillvarata medborgarnas krav på integritet, rättssäkerhet och god service. Syftet är att all information ska hanteras på ett säkert sätt.

Region Jämtland Härjedalens (RJH) informationssäkerhetsarbete ska bedrivas på ett strukturerat och riskorienterat sätt och ta sin utgångspunkt i den internationella ledningssystemstandarden för informationssäkerhet, ISO/IEC SS 27001:2014.

Region Jämtland Härjedalen ska ha ett tydligt regelverk för informationssäkerhet och för personuppgiftsbehandling som säkerställer att gällande lagar och föreskrifter följs. När personuppgifter behandlas inom hälso- och sjukvården ska Patientdatalagen (2008:355) samt Socialstyrelsens föreskrift HSLF-FS 2016:40 *Journalföring och behandling av personuppgifter i hälso- och sjukvården* tillämpas på dess hantering. Det innebär bland annat att Region Jämtland Härjedalen som vårdgivare ska utföra riskanalyser om en behandling av personuppgifter inom verksamheten riskerar att inte uppfylla kraven som ställs på behandlingen enligt föreskriften. Riskanalyserna ska dokumenteras.

2 Värdering och förhållningssätt

Det övergripande syftet med Region Jämtland Härjedalens informationssäkerhetsarbete är att säkerställa ett väl avvägt skydd för Region Jämtland Härjedalens informationstillgångar. Policyn omfattar alla informationstillgångar inom verksamheten utan undantag, oavsett om den behandlas manuellt eller automatiskt, och oberoende av i vilken form eller miljö den förekommer. All information ska vara klassificerad med avseende på känslighetsgrad.

Informationssäkerhetsarbetet ska ta sin utgångspunkt i risk- och konsekvensanalyser som syftar till att avväga rätt skyddsnivå i alla delar av verksamheten, samt motivera investeringar eller utbildningsinsatser för att:

- förhindra eller försvåra för obehöriga att få tillgång till information (konfidentialitet)
- säkerställa att den information som produceras och bearbetas är korrekt, aktuell och fullständig (riktighet)
- bidra till att informationen är åtkomlig vid behov (tillgänglighet)
- säkerställa ursprunget av varje transaktion (spårbarhet)

För vart och ett av dessa områden ska organisatoriska, administrativa och tekniska skyddsåtgärder vidtas och dokumenteras på ett sådant sätt att möjlighet ges att kontrollera att en tillfredsställande skyddsnivå uppnåtts. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för verksamheterna att uppnå sina mål.

Informationssäkerhetsskyddet ska granskas regelbundet. Avvikelser och incidenter ska systematiskt dokumenteras och följas upp, så att erfarenheter från dessa kan tas till vara som en del av det kontinuerliga förbättringsarbetet. Resultatet av Region Jämtland Härjedalens informationssäkerhetsarbete ska årligen redovisas vid ledningens genomgång.

3 Personuppgiftsbehandling och dataskydd

Personuppgiftsbehandling är centralt i Region Jämtland Härjedalens informationssäkerhetsarbete och kraven i Dataskyddsförordningen (EU 2016/679) ska efterlevas. Varje behandling av personuppgifter ska på alla människors lika villkor med hänsyn till den enskildes personliga integritet och rättighet i enlighet med gällande lagstiftning. Behandlingen ska vara laglig och korrekt. Innan en personuppgiftsbehandling påbörjas ska ett särskilt och uttryckligt samt berättigat ändamål med behandlingen vara fastställt. Region Jämtland Härjedalen ska ha ett regelverk för personuppgiftsbehandling som säkerställer att:

- Endast de uppgifter som är adekvata och relevanta för ändamålet får samlas in. Detta innebär att insamlingen inte får vara mer omfattande än nödvändigt.
- Insamlade personuppgifter ska vara korrekta och uppdaterade.
- Personuppgifterna ska behandlas på ett transparent sätt gentemot de registrerade. Det innebär bland annat att de registrerade ska få information om regionens behandling av personuppgifter.
- Insamlade personuppgifter får bara bevaras så länge det är nödvändigt för ändamålet. Personuppgifterna kan dock komma att behandlas längre för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.
- Endast behöriga ska få åtkomst till personuppgifter.
- Personuppgifterna ska skyddas av lämpliga tekniska och organisatoriska åtgärder baserade på informationsklassificeringar och riskanalyser.

- Integritetsaspekten ska genomsyra hela livscykeln för personuppgifter såsom vid utveckling, upphandling, vidmakthållande, förvaltning och avveckling av informationssystem som hanterar personuppgifter.
- Vid varje behandling av personuppgifter ska ett sådant förhållningssätt iakttas att risken för skada för den registrerade minimeras.

4 Begrepp

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter