Samordningskansliet
Sanna Othman
Tfn: 063-147586
E-post: sanna.othman@regionjh.se

2020-11-25

DNR:RS/937/2018

Informationssäkerhetspolicy

Region Jämtland Härjedalens verksamhet ska utgå från principerna om öppenhet, personlig integritet och respekt för individen. Medborgarna ska möjliggöras insyn i verksamheten och kunna förlita sig på regionens hantering av dennes information och dess skydd.

Digitalisering av processer och verksamhet och en utveckling med informationshantering i IT-system och nya funktioner innebär stora förbättringar i många avseenden. Det innebär också att beroendet till informationssystem och att sårbarheten och riskexponeringen ökar om inte säkerhetsaspekterna beaktas.

Information är en av regionens mest kritiska resurser. Hela verksamheter är beroende av information. Avbrott i tillgången och felaktig information kan orsaka allvarliga konsekvenser i verksamheten eller för enskilda individer.

1.1 Inledning

Policyn beskriver de övergripande principer som ska gälla för informationssäkerhetsarbetet i Region Jämtland Härjedalen. Informationssäkerhetspolicyn gäller för hantering av all information, i alla dess former i Region Jämtland Härjedalen inklusive bolag och stiftelser och för de som arbetar på uppdrag av regionen. Det sistnämnda regleras genom avtal. Informationssäkerhetsarbetet styrs av regionens ledningssystem för informationssäkerhet utformat utifrån ISO/IEC 27000 och organisationens verksamhetskrav samt gällande författningar. Ledningssystemet består av styrande dokument som utgörs av denna policy med tillhörande regler och eventuella rutiner samt tillämpningsanvisningar. Eventuellt verksamhetsspecifika styrande dokumenten ska utformas utifrån de regiongemensamma. Metodstöd och manualer är inte styrande utan utgör stöd och metod för att utföra informationssäkerhets - och dataskyddsåtgärder.

1.2 Värdering

Regionens informationssäkerhetsarbete ska skydda informationen inom verksamheten mot yttre och inre hot. Skyddet ska vara anpassat till skyddsvärdet, risk och lagkrav och därigenom möjliggöra för regionens verksamheter att uppnå sina mål. Följande mål är styrande för informationssäkerheten i regionen.

- **Säker och riskbaserad informationshantering**

Informationstillgångar klassificeras och riskbedöms samt hanteras utifrån dess skyddsbehov, så att den är riktig och tillgänglig när den behövs och skyddas mot obehörig åtkomst. Det för att värna verksamhetens förmåga att utföra sitt uppdrag och skydda individer mot skada men lika viktigt är att värna integriteten för medborgarna. Medborgarna ska känna trygghet i att regionen omhändertar deras intressen avseende integritet och säkerhet i behandlingen av dennes uppgifter.

Samordningskansliet
Sanna Othman
Tfn: 063-147586
E-post: sanna.othman@regionjh.se

2020-11-25

DNR:RS/937/2018

• God informationssäkerhetskultur
Behovet av skydd av information bedöms och är en central del i arbetet på alla nivåer i verksamheten utifrån de risker och hot som finns mot informationen och medarbetare är medvetna om sitt ansvar som användare.

• Effektiv incidenthantering
Regionen har förmåga att hindra och hantera allvarliga informationssäkerhetsincidenter.

• Robust informationshantering
Verksamheterna, IT och IT-infrastrukturen är riskbedömda och har planerat för vilka åtgärder som ska vidtas vid avbrott, störningar och kriser.

• Informationssäkerhetsberättelse
Ledningen och Regionstyrelsen ska informeras av särskild utsedda roller om informationssäkerhetsläget i Regionen samt vilka åtgärder som bör vidtas.

• Handlingsplan
Informationssäkerhetsaspekter ska beaktas i handlingsplaner och verksamhetsplaner.

1.3 Roller och ansvar

Regionfullmäktige fastställer informationssäkerhetspolicy för regionen. Regionstyrelsen ansvarar för att informationssäkerhetspolicy och regler för informationssäkerhet utarbetas och hålls aktuella. Regionstyrelsen beslutar om regler för informationssäkerhet och följer upp handlingsplan med mätbara mål för informationssäkerhet. Varje nämnd och styrelse är ansvarig för informationssäkerhet och personuppgiftshanteringen inom sitt verksamhetsområde och ska, inom ramen för regionens ledningssystem anta verksamhetsspecifika styrdokument för informationssäkerhet och personuppgiftshanteringen där så är nödvändigt. Det åligger även varje nämnd och styrelse att årligen följa upp informationssäkerheten och personuppgiftshanteringen. Ansvaret för informationssäkerheten är generellt kopplat till det delegerade verksamhetsansvaret.

1.4 Uppföljning och revidering

Uppföljning och revidering av denna policy ska ske i enlighet med Region Jämtland Härjedalens styrmodell och hantering av styrande dokument. Uppföljning av följsamhet gentemot denna policy med tillhörande regler, rutiner och anvisningar ska kontrolleras årligen och rapporteras till regiondirektör och styrelser/nämnder.