Regionens revisorer
Anneth Nyqvist
Certifierad kommunal revisor
Tfn: 063-147523

2021-03-30

Dnr: REV/39/2020

Regionstyrelsen

Granskning av IT-säkerhet

På vårt uppdrag har KPMG under ledning av regionens revisionskontor genomfört en granskning av regionens arbete med IT-säkerhet. Granskningens syfte har varit att svara på om regionens organisation och interna kontroll är ändamålsenlig gällande IT-säkerhet.

Vår sammanfattande bedömning är att regionen delvis har en ändamålsenlig organisation för arbetet med IT-säkerhet men att den interna kontrollen avseende efterlevnaden av lagar, förordningar och interna regelverk för IT-säkerhet är bristfällig. Granskningen visar på att det både saknas ett systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar och en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsåtgärder.

Vidare framkommer att nuvarande organisation är sårbar då det vilar ett stort ansvar för både det strategiska och operativa arbetet på de nyckelpersoner som leder arbetet med informationssäkerhet och IT-säkerhet. En annan iakttagelse är att medarbetare inte har fått tillräcklig utbildning och därigenom den kunskap och medvetenhet som krävs för att efterleva de lagkrav och interna regler som finns för hantering av känslig information och informationstillgångar generellt.

Vi rekommenderar regionstyrelsen att:

- *säkerställa att avdelningar och områden tillsätter resurser och tar sitt ansvar för det systematiska informationssäkerhetsarbetet i enlighet med ledningssystem för informationssäkerhet.*
- *säkerställa att informationsklassning och riskbedömning genomförs för samtliga verksamhetskritiska system och att kontinuitetsplaner upprättas.*
- *säkerställa att regionens behörighetshantering hanteras i enlighet med lagar och interna regelverk samt att en tillräcklig uppföljning sker för att kontrollera efterlevnaden.*
- *riskanalyser upprättas regelbundet för IT-infrastruktur och drift.*
- *upprätta en riskanalys över att privata enheter kan ansluta via fjärraccess till regionens IT-miljö och utifrån dessa risker fatta beslut om relevanta åtgärder för att möta dessa.*
- *uppdatera kontinuitetsplan för IT-driften.*

- *besluta om regionövergripande organisation för incidenthantering och rapportering för informationssäkerhetsincidenter samt att kommunicera denna till verksamheterna. Det behöver även säkerställas att en uppföljning sker av samtliga inträffade incidenter så att dessa kan beaktas i förbättringsarbetet.*
- *säkerställa att den interna kontrollen inkluderar en riskbedömning kopplat till regionens informations- och IT-säkerhet utifrån gällande lagar och interna styrdokument.*

Vi emotser senast den 15 augusti 2021 en redovisning av vilka åtgärder som regionstyrelsen har vidtagit eller avser att vidta med anledning av granskningsresultatet.

För Region Jämtland Härjedalens revisorer

Viveca Asproth
Ordförande

Gustaf Onilsgård
Förtroendevald revisor

Bilaga
Revisionsrapport – Granskning av IT-säkerhet
Rapportsammandrag - Granskning av IT-säkerhet
Kopia till
Regiondirektören
Chef IT- och e-hälsoavdelningen