REGION
JÄMTLAND
HÄRJEDALEN
Regionens revisorer

Leif Gabrielsson
Revisionsdirektör
Tfn: 063-147528

SKRIVELSE

2024-02-28

REV/6/2023

Regionstyrelsen

Uppföljande granskning av IT-säkerhet

På vårt uppdrag har revisionskontoret tillsammans med upphandlad konsult genomfört en uppföljande granskning av regionens IT-säkerhetsarbete.

Granskningens syfte har varit att ta reda på om brister som framkom i den tidigare granskningen (2020) blivit åtgärdade.

Resultatet av granskningen redovisas i bifogad revisionsrapport.

- Under föregående granskning bedömdes hanteringen av den interna kontrollen vara bristfällig. Bristerna har delvis blivit åtgärdade men en internkontroll baserad på en riskanalys saknas.
- I föregående granskning framkom en avsaknad av tillräckliga och adekvata resurser i förvaltningarna som kan ta arbetet från den strategiska nivån till den praktiska nivån. Resurser har tillförts och bristerna bedöms ha blivit åtgärdade.
- I den tidigare granskningen framkom att det inte pågick något systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar, dock gjordes riskanalyser inom IT-säkerhet på ett tillfredsställande sätt. Vid den uppföljande granskningen uppges att det implementerats en systematisk metod för säkerhetsklassificering av funktioner och tjänster.
- Den tidigare granskningen visade att regionens rutiner för behörigheter och lösenord var bristfälliga. Regionen har genomfört vissa åtgärder för att förbättra hanteringen av behörigheter. Under 2024 planeras en genomgripande förändring av lösenordskraven vilket är en positiv åtgärd för att stärka behörighetshanteringen och därigenom öka den övergripande säkerheten. Utifrån ett tekniskt säkerhetsperspektiv görs bedömningen att skyddsnivån för patientinformation är tillräcklig.
- I den tidigare granskningen noterades att regionen saknade en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter. Vi anser att åtgärder vidtagits och regionens incidenthanteringsprocess bedöms vara utformad enligt god praxis och är välfungerande.
- I den tidigare granskningen bedömdes att medarbetare inte erhöll tillräcklig utbildning som krävdes för att efterleva de lagkrav och interna regler som finns för hantering av patientuppgifter. I den uppföljande granskningen bedöms bristerna kvarstå på grund av att endast hälften av personalen som genomgått den utbildning i informationssäkerhet som samtliga anställda ska genomgå i regionens kompetensportal.
- I den tidigare granskningen bedömdes att regionens riskanalysarbete kunde utvecklas för att kunna göra rätt prioriteringar. I den uppföljande granskningen bedöms bristerna delvis kvarstå.

Vi rekommenderar Regionstyrelsen att:

- Säkerställa att riktlinjerna för IT-säkerhet efterlevs i praktiken.
- Säkerställa att en systematisk och fullständig process för informationsklassning etableras.
- Säkerställa att arbetet med att fastställa och etablera en systemförvaltningsmodell färdigställs.
- Implementera ett automatiserat identitets- och åtkomstverktyg för att adressera sårbarheter som kan uppstå genom manuell hantering. Olämpliga behörigheter och inaktuella användarkonton innebär ökad risk för obehörig åtkomst. En automatiserad metod för hantering av behörigheter kan mitigera risken för obehörig åtkomst, samtidigt som användarupplevelsen förbättras.
- Införa ett obligatoriskt krav för medarbetare att fullfölja utbildning inom informations-/IT-säkerhet inom en given tidsram för att på så sätt öka deltagandet och stärka informationssäkerheten.
- Säkerställa att medarbetarna kontinuerligt utbildas inom området. Detta är viktigt både för att repetera kunskaperna men också för att kunskapskraven ändras relativt snabbt inom detta område.
- Fullfölja arbetet med att utveckla internkontrollarbetets riskbaserade ansats, vilket innebär att etablerade kontrollaktiviteter bör stå i proportion till verksamhetens befintliga risker. Ett riskbaserat förhållningssätt syftar till att bidra till att regionens resurser och medel utnyttjas effektivt, vilket i sin tur möjliggör värdeskapande för regionens medborgare.
- Säkerställa att planerade aktiviteter och åtgärder inom området slutförs. Flera olika IT-säkerhetsrelaterade åtgärder tas upp i verksamhetsplan både för 2022 och 2023, exempelvis säkerheten i nätverksansluten hårdvara. Samtidigt noteras att aktiviteterna återkommande inte når den eftersträvade måluppfyllelsen.
- Fortsätta utvärdera och vara uppmärksam på behov av eventuella ytterligare resurser. Eventuella risker som ännu inte har identifierats kan medföra ett ökat behov av nya resurser och kompetenser.

Vi emotser senast den 10:e september 2024 en redovisning av vilka åtgärder som regionstyrelsen vidtagit eller avser vidta med anledning av granskningsresultatet samt en tidplan för åtgärderna.

För Region Jämtland Härjedalens revisorer

Jan Rönngren
Ordförande

Viveca Asproth
Vice ordförande

Bilaga
Revisionsrapport – Uppföljande granskning av IT-säkerhetsarbetet Rev/6/2023
Rapportsammandrag – Uppföljande granskning av IT-säkerhetsarbetet Rev/6/2023

Kopia till
Regiondirektören
Regionstabschef
IT-säkerhetsansvarig