Till:
Regionfullmäktiges presidium

Till beaktande:
Regionstyrelsen
Hälso- och sjukvårdsnämnden
Hållbarhetsnämnden

Rapport – Granskning av informationssäkerhet

Revisionen har genomfört en granskning av regionens arbete med informationssäkerhet.

Vår samlade bedömning utifrån granskningens syfte är att regionstyrelsen, hälso- och sjukvårdsnämnden samt hållbarhetsnämnden endast delvis har säkerställt att informationssäkerhetsarbetet är systematiskt i enlighet med lagkrav och interna beslut.

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen att:

- Tillse att övergripande styrdokument för informationssäkerhet antas politiskt för att tydliggöra de förtroendevaldas viljeriktning och krav på förvaltningarnas arbete.
- Tillse att nuvarande ledningssystem för informationssäkerhet (LIS) utvärderas, kompletteras och struktureras i syfte att säkerställa tillämpning av regionens regelverk inom informationssäkerhet.
- Besluta om riktlinjer för regionens övergripande riskhantering och tillse att riskanalyser minst årligen genomförs med inriktning på informationssäkerhet.
- Utvärdera nuvarande personalsäkerhetsåtgärder för att bedöma om de är tillräckliga i syfte att etablera en säkerhetskultur i enlighet med beslutade riktlinjer för informationssäkerhet.
- Stärka styrningen av informationssäkerhetsarbetet där uppföljning och rapportering efterföljs av beslut om handlingsplaner för väsentliga och prioriterade förbättringsåtgärder.
- Utvärdera nuvarande it-säkerhetsåtgärder i relation till kommande lagkrav samt aktuella hot och risker, särskilt med beaktande på förmåga att upptäcka och hantera avvikelser i form av it-säkerhetshändelser.
- Säkerställa att uppföljning och rapportering genomförs i enlighet med beslutade rutiner samt tydliggöra krav på nämndernas ansvar för uppföljning och rapportering av informationssäkerhetsarbetet. I uppföljning bör kontroll av att de beslutade styrdokumenten efterlevs ingå.

Penneo dokumentnyckel: NKR2J-VM6ZA-GMXZY-XJ6GC-LM7HC-KXP69

Utifrån resultatet av vår granskning rekommenderar vi hälso- och sjukvårdsnämnden att:

- Slutföra arbetet enligt rutinen för processorienterad informationskartläggning (POIK).
- Efterfråga förtydligande över nämndens ansvar för uppföljning av det egna informationssäkerhetsarbetet.
- Efterfråga förtydligande över på vilka sätt informationsägaren ska involveras i analys och bedömning av informationssäkerhetsincidenter samt vilka krav som finns för när nämnden ska få kännedom om inträffade incidenter.
- Etablera regelbunden, minst årlig, uppföljning informationssäkerhetsarbetet så att nämnden ges förutsättningar att fatta beslut om inriktning och förstärkningar.

Utifrån resultatet av vår granskning rekommenderar vi hållbarhetsnämnden att:

- Tillse att samverkan och samsyn stärks internt mellan funktioner för informationssäkerhet och systemenhet samt även mellan systemenhet och avdelning för IT och verksamhetsutveckling.
- Efterfråga förtydligande över nämndens ansvar för uppföljning av det egna informationssäkerhetsarbetet.
- Efterfråga förtydligande över på vilka sätt informationsägaren ska involveras i analys och bedömning av informationssäkerhetsincidenter samt vilka krav som finns för när nämnden ska få kännedom om inträffade incidenter.
- Etablera regelbunden, minst årlig, uppföljning informationssäkerhetsarbetet så att nämnden ges förutsättningar att fatta beslut om inriktning och förstärkningar.

För Region Gävleborgs revisorer

Sven-Erik Lindestam
Ordförande

Petri Ritola
Vice ordförande

Penneo dokumentnyckel: NKR2J-VM6ZA-GMXZY-XJ6GC-LM7HC-KXP69

PENNEO

Signaturerna i detta dokument är juridiskt bindande. Dokumentet är signerat genom Penneo™ för säker digital signering. Tecknarnas identitet har lagrats, och visas nedan.

"Med min signatur bekräftar jag innehållet och alla datum i detta dokumentet."

SVEN-ERIK LINDESTAM
Undertecknare
Serienummer: 5a6f9a49415a71[…]52a1a47f8f71c
IP: 80.245.xxx.xxx
2025-11-20 10:16:00 UTC

PETRI JAAKKO RITOLA
Undertecknare
Serienummer: fb86137557d703[…]467d1f9ec74e1
IP: 83.227.xxx.xxx
2025-11-21 07:33:25 UTC

Penneo dokumentnyckel: NKR2J-VM6ZA-GMXZY-XJ6GC-LM7HC-KXP69

Detta dokument är undertecknat digitalt via **Penneo.com**. De signerade uppgifternas integritet är validerad med hjälp av ett beräknat hashvärde för originaldokumentet. Alla kryptografiska bevis är inbäddade i denna PDF, vilket säkerställer både autenticitet och möjlighet till framtida validering.

Detta dokument är försett med ett kvalificerat elektroniskt sigill. För mer information om Penneos kvalificerade betrodda tjänster, se **https://eutl.penneo.com**.

Så här verifierar du dokumentets äkthet:
När du öppnar dokumentet i Adobe Reader kan du se att det är certifierat av **Penneo A/S**. Detta bekräftar att dokumentets innehåll förblir oförändrat sedan tidpunkten för undertecknandet. Bevis för de enskilda undertecknarnas digitala signaturer bifogas dokumentet.

De kryptografiska bevisen kan kontrolleras med hjälp av Penneos validator, **https://penneo.com/validator**, eller andra valideringsverktyg för digitala signaturer.