VÄSTRA GÖTALANDSREGIONEN
REVISIONSENHETEN

2022-12-14

Till regionstyrelsen, styrelsen för Regionhälsan, styrelsen för Skaraborgs Sjukhus och fastighetsnämnden

Granskning av informations- och cybersäkerhet (REV 2022-00120)

Revisionen har granskat regionens arbete med informations- och cybersäkerhet. Syftet med granskningen har varit att bedöma om nämnder och styrelser har en tillräcklig styrning och intern kontroll av informationssäkerhetsarbetet för att säkerställa att arbetet sker på ett ändamålsenligt sätt.

Granskningen omfattar regionstyrelsen, styrelsen för Regionhälsan, styrelsen för Skaraborgs Sjukhus och fastighetsnämnden.

Vår bedömning är att regionstyrelsen, inom ramen för sitt övergripande ledningsansvar, inte har etablerat en tillräcklig styrning av informations- och cybersäkerhetsarbetet. Vidare bedömer vi att styrelsen för Regionhälsan och fastighetsnämnden i huvudsak har en tillräcklig styrning inom området. Vi bedömer att Skaraborgs sjukhus inte har en tillräcklig styrning av arbetet och att arbetet i nuläget inte sker på ett ändamålsenligt sätt. Vi kan även konstatera att den interna kontrollen tillsammans med andra uppföljningsrutiner behöver stärkas hos samtliga granskade. Slutligen bedömer vi att regionstyrelsen brister i sitt övergripande ansvar för säkerhetsarbetet då den inte har tillsett att det finns regelbunden rapportering av informationssäkerhetsarbetet enligt gällande regelverk.

På nästa sida finns de rekommendationer som vi lämnar med anledning av granskningen.

Vi önskar få ett yttrande från er senast den 30 april 2023. Av yttrandet ska framgå vilka åtgärder som ni har gjort eller planerar att göra med anledning av de rekommendationer som vi lämnar. Yttrandet skickar ni till revision@vgregion.se.

Revisionsrapporten översänds för yttrande till regionstyrelsen, styrelsen för Regionhälsan, styrelsen för Skaraborgs Sjukhus och fastighetsnämnden samt för kännedom till regionfullmäktiges presidium och övriga nämnder och styrelser i regionen.

För revisorskollegiet,

Birgitta Eriksson,
ordförande

Krister Stensson,
vice ordförande

Rekommendationer

Revisionen rekommenderar regionstyrelsen – inom ramen för sitt övergripande ledningsansvar – att:

- revidera och komplettera ledningssystemet för informationssäkerhet (LIS) i enlighet med granskningens resultat, främst med avseende på:
  - de kompletterande riktlinjer, planer och rutiner som enligt tidigare beslut fattade av regionstyrelsen och regiondirektören upprättas.
  - gällande lagar, regler och nya krav inom området.
  - beskrivning av ansvar och roller på både strategisk och operativ nivå så att det överensstämmer med nuvarande organisation.
  - rutiner för uppföljning och kontroll.
- säkerställa att det regelbundet genomförs obligatoriska utbildningar i informationssäkerhet för medarbetare.
- förstärka uppföljning, intern kontroll och uppsikt av informationssäkerhets-arbetet för att säkerställa följsamhet till interna krav och gällande regelverk.
- etablera en årlig rapportering från samtliga nämnder och styrelser i syfte att ge styrelsen en samlad bild av regionens informationssäkerhet.

Revisionen rekommenderar regionstyrelsen, styrelsen för Regionhälsan, fastighets-nämnden och styrelsen för Skaraborgs Sjukhus att:

- upprätta förvaltningsspecifika rutiner avseende hantering av behörighet som kopplar an mot de regionövergripande riktlinjerna samt säkerställa att kontroller av tilldelade behörigheter genomförs.
- säkerställa att obligatoriska utbildningar som svarar mot verksamhetens behov genomförs och att deltagandet följs upp.
- upprätta kontinuitetsplaner för att säkerställa verksamhetens fortgående vid en eventuell incident samt säkerställa att dessa testas med regelbundenhet.
- vidta åtgärder i syfte att stärka uppföljningsarbetet samt upprätta former för kontinuerlig återrapportering till styrelse/nämnd av det informations-säkerhetsarbete som bedrivs.

Revisionen rekommenderar styrelsen för Skaraborgs Sjukhus att även:

- säkerställa att riskbedömning och informationsklassning genomförs av den information som hanteras inom styrelsens verksamhet.