region västerbotten

REVISORERNAS BEDÖMNINGAR

2022-09-30

REV 45–2021
REV 46-2021

Regionstyrelsen
Hälso- och sjukvårdsnämnden

Brister i arbetet med IT- och informationssäkerhet

Uppföljning av tidigare granskningar av IT- och informationssäkerhet visar att oroande brister kvarstår:

- Riktlinjer och regler behöver uppdateras. Det finns inte rutiner för hur olika styrdokument ska uppdateras. Vissa styrande dokument saknas helt. Det saknas också system och rutiner för att utbilda medarbetare i regionen om regler för IT- och informationssäkerhet.
- Det saknas en tillräckligt utvecklad organisation för arbetet med informationssäkerhet i regionen. Det finns en informationspolicy och vissa övergripande styrdokument. Det finns dock inget övergripande dokument som beskriver hur dataskyddsarbetet ska organiseras. Det saknas också en analys av vilka resurser och stöd som behövs till informationssäkerhetsansvarig och dataskyddsombud i dataskyddsarbetet.
- Uppföljningen och kontrollen av att regler och rutiner för IT- och informationssäkerhet följs är svagt utvecklad. Det förekommer sporadiska kontroller bland verksamheterna. Det saknas dock centrala granskningsplaner och kontrollfunktioner. Det finns heller inga naturliga rapporteringsvägar till regionstyrelsen och hälso- och sjukvårdsnämnden om IT- och informationssäkerhetsarbetet.

Det är angeläget att regionstyrelsen och hälso- och sjukvårdsnämnden stärker styrningen och kontrollen över regionens IT- och informationssäkerhetsarbete. I flera tidigare granskningar har revisorerna framfört behov av att stärka IT- och informationssäkerhetsarbetet (Nr 23/2010, 17/2014, 18/2015, 3/2017, 14/2017 och 3/2018). I tider när IT-intrång och cyberbrottslighet är en stor risk är det extra viktigt att regionen har ett tillräckligt säkerhetsarbete. Brister i IT- och informationssäkerheten kan få stora negativa konsekvenser.

Revisorerna har enhälligt ställt sig bakom dessa bedömningar och slutsatser. I en bilaga lämnar revisorerna rekommendationer till regionstyrelsen och hälso- och sjukvårdsnämnden. Revisorerna lämnar denna skrivelse och underliggande rapporter (1/2022 och 2/2022) till regionstyrelsen och hälso- och sjukvårdsnämnden för yttrande. Yttrande med uppgifter om verkställda och planerade åtgärder ska lämnas till revisionskontoret senast den 18 januari 2023.

För regionens revisorer

Edward Riedl
Ordförande

Bert Öhlund
Vice ordförande

Revisorernas rekommendationer

Informations- och IT-säkerhet (1/2022)

- Se över organisationen för arbetet med IT- och informationssäkerhet. Säkerställ en tydlig ansvarsfördelning.
- Inför en standardiserad process för att identifiera risker inom IT- och informationssäkerhet.
- Säkerställ att styrdokument är aktuella över tid och kända bland verksamheterna. Säkerställ att anställda får tillräcklig utbildning inom IT-och informationssäkerhet.
- Säkerställ tillräcklig uppföljning och kontroll av verksamheternas arbete med IT och informationssäkerhet och att policyer, riktlinjer och rutiner följs.

Efterlevnad av GDPR (2/2022)

- Tydliggör hur dataskyddsarbetet ska organiseras och genomföras i regionen. Dataskyddsarbetet bör utgå från ett övergripande styrdokument för GDPR, tydlig ansvarsfördelning och dokumenterade rollbeskrivningar. Tydliggör vilket stöd och vilka resurser som finns för informationssäkerhetsansvarig och dataskyddsombud.
- Säkerställ att styrdokument är aktuella över tid och kända bland verksamheterna. Säkerställ att anställda har tillräcklig kunskap i dataskyddsarbetet genom regelbundna utbildningar.
- Säkerställ tillräcklig uppföljning och kontroll av verksamheternas hantering av personuppgifter och att policyer, riktlinjer och rutiner följs.

Instruktioner för yttrande

Det ska vara enkelt att utläsa vilka åtgärder som styrelsen eller nämnden vidtagit eller planerar att vidta. Tänk därför på detta när ni svarar:

- Lämna ett svar för varje rekommendation som revisorerna lämnat. Det ska finnas en tydlig koppling mellan rekommendationerna och de åtgärder som vidtagits eller planeras vidtas.
- Svara så konkret som möjligt. Ange gärna hur åtgärderna ska genomföras, vem som ska genomföra dem och när.
- Om styrelsen eller nämnden inte tänker vidta några åtgärder, motivera varför.
- Om styrelsen eller nämnden inte kan svara på utsatt tid, kontakta undertecknad.

Vid frågor kontakta

Petter Bergner
Revisionskontoret
090-785 73 72
petter.bergner@regionvasterbotten.se

UNDERSKRIFTSSIDA

Detta dokument har undertecknats med elektroniska underskrifter:

NAMN:	BERT ÖHLUND
TITEL, ORGANISATION:	Vice ordförande, Revisorerna i Region Västerbotte
IDENTIFIKATIONSTYP:	Svensk e-legitimation
IDENTIFIKATIONS-ID:	_0775f63f4651b14f976b1a4fe50e593386
DATUM & TID:	2022-10-03 09:18:15 +02:00

NAMN:	EDWARD RIEDL
TITEL, ORGANISATION:	Ordförande, Revisorerna i Region Västerbotten
IDENTIFIKATIONSTYP:	Svensk e-legitimation
IDENTIFIKATIONS-ID:	_097d20985ae86c0a4981e1891c5ecbb273
DATUM & TID:	2022-10-04 16:18:28 +02:00

Certifierad av Comfact Signature
Accepterad av alla undertecknare
2022-10-04 16:18:35 +02:00
Ref: 49780SE
www.comfact.se

Validera dokumentet | Användarvillkor