Region Gävleborg

REVISORERNA

2021-12-20

Till
Regionfullmäktige

För kännedom
Regionstyrelsen

Uppföljande granskning – Informations- och cybersäkerhet

År 2019 genomfördes en granskning av Region Gävleborgs hantering av informations- och cybersäkerhet. Syftet med granskningen var att ge revisorerna ett underlag för bedömning av ändamålsenligheten i Region Gävleborgs IT-säkerhetsarbete i förhållande till de risker som regionen utsätts för. Den sammantagna revisionella bedömningen var att regionstyrelsen, i begränsad utsträckning, hade säkerställt att regionen hade ett ändamålsenligt arbete med att identifiera, prioritera och hantera säkerhetshot och incidenter som kan påverka regionens informations- och cybersäkerhet.

Region Gävleborgs revisorer har utifrån risk och väsentlighet bedömt det angeläget att följa upp tidigare granskning informations- och cybersäkherhetsarbetet. Granskningens syfte och revisionsfråga har varit att besvara om ändamålsenliga åtgärder vidtagits med anledning av 2019 års granskning.

Granskningsresultatet har bedömts utifrån skalan ”ej uppfyllt”, ”i begränsad utsträckning”, ”till övervägande del” eller ”helt uppfyllt”.

Efter genomförd granskning gör vid den samlade bedömningen att regionstyrelsen ***till övervägande del*** vidtagit ändamålsenliga åtgärder med anledning av 2019 års granskning. Vi kan konstatera att regionen vidtagit ett antal viktiga åtgärder sedan föregående granskning.

Vissa delar i granskningsrapporten är sekretessbelagd och texten svartmarkerad.

Med utgångspunkt från de iakttagelser och bedömningar som har framkommit i den uppföljande granskningen lämnar vi följande rekommendationer till regionstyrelsen:

- Fastställ dokumentet (rutinen) ”Livscykelhantering i Region Gävleborg”.
- Slutför och dokumentera den påbörjade processkartläggningen, med fokus på de återstående kärnprocesserna, då dessa torde ha högre prioritet än resterande stöd- och ledningsprocesser. Sammanställ processkartläggningen på ett sätt som skapar överblick och som underlättar uppföljning och styrning.
- Stärk arbetet med uppföljning av tidigare upphandlingar genom tydligt utpekat ansvar och genom stickprov samt ett dokumenterat systematiskt arbete relaterat till uppföljning.

- Förtydliga hur arbetet med området för informationssäkerhet ska följas upp, med tydliga mål och planer för hur detta ska ske.
- Slutför arbetet med utformandet av en övergripande kontinuitetsplan och säkerställ att arbetet med nedbrutna och anpassade planer för verksamheterna slutförs.
- Överväg att skapa ett dokumenterat rollbaserat utbildningspaket för olika personalgrupper inom organisationen.
- Överväg att utveckla dokumenterade rollbaserade eller individuella utbildningsplaner, vilka följs upp för att säkerställa att obligatoriska moment verkligen genomförts.
- Överväg att genomföra ytterligare medvetandehöjande kampanjer kring ransomware, phishing eller lösenordsbyte, gärna vid olika tidpunkter varje år.

Gävle 2021-12-20

För Region Gävleborgs revisorer

Olof Bengtsson
Ordförande

Sture Sandberg
Vice ordförande