REGION KRONOBERG

Svar på revisionsrapport – Granskning av Region Kronobergs informationssäkerhet

Ordförandens förslag till beslut

Regionstyrelsen godkänner svar på revisionsrapport Granskning av Region Kronobergs informationssäkerhet samt överlämnar svaret till regionfullmäktige.

Sammanfattning

Regionfullmäktiges förtroendevalda revisorer har överlämnat rapporten Granskning av Region Kronobergs informationssäkerhet till regionstyrelsen.

Den samlade bedömningen är att regionstyrelsen har säkerställt att:

- Det finns en tillräcklig intern styrning, uppföljning och kontroll som säkerställer ett ändamålsenligt systematiskt arbetssätt med informationssäkerheten i regionen. Detta sker framför allt genom den utvecklade och beslutade styr- och samverkansmodellen, som skapar förutsättningar för ett effektivt arbete och god relation mellan de enheter som äger sakfrågorna och verksamheterna som ska följa beslutade riktlinjer. Region Kronoberg arbetar också enligt ISO 27000 vilket medför att det finns en struktur för utförande men också för regelbundna översyner som gynnar regionens arbete.

- Den interna kontrollen avseende regionens cybersäkerhet är tillräcklig. Region Kronoberg uppvisar ett aktivt arbete och samtidigt en medvetenhet kring att det finns krav på ständiga förbättringar. De framtagna utbildningarna kommer att stärka enskilda medarbetare och verksamheterna som helhet i att arbeta med informationssäkerhet.

- Region Kronobergs nuvarande (med vilket avses tidpunkten november 2023) tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå. Även här finns det kompetens och kunskap om sakfrågorna i regionen och det pågår ett ständigt arbete med att försöka minska riskerna som uppstår genom den mänskliga faktorn.

I granskningen framgår även att:

- Det systematiska informationssäkerhetsarbetet i Region Kronoberg följer standarden för ISO 27000, men det är inte ett mål för Region Kronoberg att bli certifierad.

- Bedömningen görs i granskningen att regionstyrelsen delvis säkerställt att det finns rutiner för kontroll av systembehörigheter som är ändamålsenliga.

- I granskningen noteras att uppföljningen på en övergripande politisk nivå är svag givet resultatet från protokollgranskningen.

Identifierade förbättringsområden

Granskningen har identifierat förbättringsområden. Regionstyrelsen

rekommenderas att:
• Trots tydliga förbättringar fortsätta följa upp Region Kronobergs arbete med informationssäkerhet.
• Skapa förutsättningar för att beslutade riktlinjer och rutiner är välkända i organisationen genom att hålla frågorna aktuella och relevanta så att informationssäkerhetsperspektivet finns med i alla delar av verksamheten.

Svar önskas från regionstyrelsen
Mot bakgrund av vad som framkommit i granskningen önskar revisorerna ett svar från regionstyrelsen med uppgift om tidsplan för eventuella planerade åtgärder samt redovisning av hittills vidtagna åtgärder som tillvaratar de förbättringsmöjligheter som föreslagits. För varje rekommendation som förslagits ska följande framgå:

- Hittills vidtagna åtgärder
- Eventuella planerade åtgärder
- Tidplan för eventuella planerade åtgärder
- Eventuella andra synpunkter

Revisorerna kommer i ett senare skede vilja ha en avstämning med styrelsen på hur arbetet har fortskridit avseende planerade åtgärder.

Rekommendationer och svar

Granskningen har identifierat följande förbättringsområden:

1. Trots tydliga förbättringar fortsätta följa upp Region Kronobergs arbete med informationssäkerhet.
2. Skapa förutsättningar för att beslutade riktlinjer och rutiner är välkända i organisationen genom att hålla frågorna aktuella och relevanta så att informationssäkerhetsperspektivet finns med i alla delar av verksamheten.

Rekommendation 1
Trots tydliga förbättringar fortsätta följa upp Region Kronobergs arbete med informationssäkerhet.

Regionstyrelsens svar
Att följa upp Region Kronobergs informationssäkerhetsarbete är ett arbete som bedrivs kontinuerligt genom regionens systematiska informationssäkerhetsarbete. Arbetet bedrivs enligt ISO27000 för att säkerställa att regionen kontinuerligt följer upp och styr informationssäkerhetsarbetet för att uppnå ständiga förbättringar. Detta gör regionen bland annat genom att:

- Arbeta enligt Ledningssystemet för Informationssäkerhet som är infört på Säkerhetsenheten enligt ISO 27 000.
- Följa ett årshjul för systematiskt informationssäkerhetsarbete.
- Följa upp ett antal KPI (mätetal) varje kvartal.
- Samverka aktivt med IT och med övriga verksamheter.

- Följa upp och analysera inkomna avvikelser i Synergi kopplade till informationssäkerhet och dataskydd.

Planerade åtgärder:

- Enligt beslut i regionstyrelsens internkontrollplan ska personuppgiftsincidenter rapporteras till varje nämnd en gång/år. Denna rapportering kan ske genom föredragning på sammanträde eller genom utskick av sammanställd information. Samtliga nämnder kommer under september månad att få möjlighet att antingen ta del av en föredragning eller få underlag utsänt kopplat till personuppgiftsincidenter.
- MBS:s nationella undersökning Infosäkkollen ska fyllas i och skickas in senast 6 september. Infosäkkollen ger MSB en bild över informations- och cybersäkerhetsarbetet på nationell nivå och ger också Region Kronoberg en möjlighet att ta temperaturen på regionens pågående arbete och ger regionen möjlighet att kunna styra arbetet för att ytterligare förbättra regionens informationssäkerhetsarbete.

Rekommendation 2
Skapa förutsättningar för att beslutade riktlinjer och rutiner är välkända i organisationen genom att hålla frågorna aktuella och relevanta så att informationssäkerhetsperspektivet finns med i alla delar av verksamheten.

Regionstyrelsens svar
Att hålla informationssäkerhetsfrågor relevanta och aktuella och att se till att informationssäkerhetsperspektivet finns med i alla delar av verksamheten handlar främst om att bygga en stark säkerhetskultur i Region Kronoberg. Att bygga en säkerhetskultur gör regionen kontinuerligt på olika sätt, exempelvis genom utbildning, föredragningar på APT och verksamhetsmöten och genom kommunikation av viktiga frågor i olika kanaler.

För närvarande finns ett antal åtgärder som ska vidtas för att ytterligare stärka regionens säkerhetskultur:

- Utbildningen Säkert Beteende som finns på kompetensportalen ska göras obligatorisk för samtliga medarbetare. Beslutet ska fattas inom kort och regionen beräknar att utbildningen ska publiceras i ny version i september.
- En kommunikationsplan håller på att utarbetas tillsammans med kommunikationsavdelningen för att säkerställa att regionen kontinuerligt håller frågorna levande och relevanta. I kommunikationsplanen kommer regionen att specificera hur kommunikationen sker med våra verksamheter, vilka budskap som ska lyftas och i vilka kanaler. Kommunikationsplanen kommer att finnas färdig i en första version under hösten 2024.
- Oktober är EU:s informationssäkerhetsmånad. Under oktober 2024 kommer informationssäkerhet att ha ett extra fokus i Region Kronoberg genom olika typer av aktiviteter som tillsammans knyter ihop vår utbildning Säkert Beteende och våra andra satsningar på exempelvis

informationsklassning, registerförteckning och säker hantering av den egna arbetsdatorn.

Henrietta Modig Serrate (S)
Regionstyrelsens ordförande

Bilagor

- Revisionsrapport Granskning av Region Kronobergs informationssäkerhet
- Svar på revisionsrapport – Granskning av Region Kronobergs informationssäkerhet, daterat 2024-05-08