Rapportsammandrag
från Regionens revisorer

Diarienummer:
REV 39/2020

En granskning av
IT-säkerheten

Regionens revisorer har genomfört en granskning av regionens arbete med IT-säkerhet.

Ledningssystem finns
Det finns en övergripande styrning genom ett implementerat ledningssystem för informationssäkerhet där ansvarsfördelning och organisation framgår.

Efterlevnad av styrdokument
Den interna kontrollen avseende efterlevnaden av lagar, förordningar och interna regelverk för IT-säkerhet är bristfällig. Delar av det ansvar som utpekas i dokumenterad ansvarsfördelning uppfylls inte av avdelnings- och områdeschefer.

Sårbar organisation
Det finns risker att nuvarande organisation är sårbar då det vilar ett stort ansvar för både det strategiska arbetet och operativa arbetet på de nyckelpersoner som leder arbetet med informationssäkerhet och IT-säkerhet. Vid eventuella personal eller organisationsförändringar kan det leda till att kontinuitet och kunskap går förlorad.

Utbildning
Medarbetare har inte fått tillräcklig utbildning och därigenom den kunskap och medvetenhet som krävs för att efterleva de lagkrav och interna regler som finns för hantering av känslig information och informationstillgångar generellt.

Informationsklassning
Det saknas ett systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar. IT-säkerhetsåtgärder inrättas därmed till stor del utifrån den kunskap och förutsättningar som IT-enheten har. Detta riskerar att införda säkerhetsåtgärder inte står i relation till hur skyddsvärd information som den avser att hantera är.

Foto: Syda Productions/Mostphotos

Behörigheter och lösenord
De styrande och stödjande dokument som finns gällande behörigheter efterlevs inte i tillräckligt hög grad vilket påverkar regionens förmåga att säkerställa medborgarnas integritet avseende patientinformation i journalsystem.

Incidenthantering
Dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter saknas. I nuläget sker ingen övergripande sammanställning över inträffade incidenter så att dessa kan utvärderas och ligga till grund för regionens förbättringsarbete.

Aktivt arbete pågår
Regionen har ett aktivt arbete med IT-säkerhet genom vilket de har tillsett att det ska finnas säkerhetsåtgärder för att skydda regionens information inklusive lagrade patientdata. Flera åtgärder som exempelvis segmenterade nätverk och funktioner för övervakning har vidtagits.

Revisorernas skrivelse och revisionsrapport, se diariet: Rev/39/2020.

För information, kontakta:
Viveca Asproth, revisorernas ordförande
070-300 37 05
Leif Gabrielsson, Revisionsdirektör
063 - 14 75 28