Danderyds sjukhus

Caroline Hällsjö Sander

TJÄNSTEUTLÅTANDE

ASN 2026-0812

Akutsjukhusnämnden

Ärenderubrik

Förvaltningens förslag till beslut
Förvaltningen föreslår att akutsjukhusnämnden beslutar följande.

> Förvaltningarnas tjänsteutlåtande utgör akutsjukhusnämndens yttrande på Regionrevisorernas rapport 13/2025 – Omhändertagande av CERT-rekommendationer, RK 2025-0063.

Sammanfattning
Regionrevisorerna har överlämnat rapport 13/2025 – Omhändertagande av CERT-rekommendationer för yttrande senast 2026-03-27.

Revisorernas samlade bedömning är att Danderyds sjukhus omhändertar rekommendationer från CERT men att det finns brister i processerna. Det saknas även formaliserad uppföljning av såväl incident som åtgärd.

Vidare konstateras att det saknas en samlad bild över vilka IT-system som används och att flera lokala system saknar systemägare och förvaltning, vilket riskerar att försena åtgärder vid identifierade störningar.

Bakgrund
Revisionskontoret har granskat it-säkerhetsarbetet i regionens nätverksmiljö med fokus på hantering av rekommendationer om skyddsåtgärder. Syftet med granskningen är att bedöma om akutsjukhusnämnden och fastighets- och servicenämnden har en till-räcklig styrning och kontroll för att säkerställa att CERT:s identifierade it-relaterade risker åtgärdas i tid. Detta för att minimera eller eliminera potentiella hot mot regionens digitala informationsmiljö.

Förvaltningens yttrande
Revisorernas samlade bedömning är att Danderyds sjukhus omhändertar rekommendationer från CERT men att det finns brister i processerna. Det saknas även formaliserad uppföljning av såväl incident som åtgärd.

Den nya cybersäkerhetslagen (CSL) och Regionens nya informationssäkerherhetsriktlinje blev gällande från den 15 januari 2026. Som en konsekvens av CSL förväntas myndigheten för civilt försvar (MCF)

att utfärda föreskrifter avseende hantering av incidenter under H1 2026. Utifrån lagen och kommande föreskrifter så ses Region Stockholm som vårdgivaren, inte respektive förvaltning. Detta innebär att eventuella incidenter som måste rapporteras till myndigheten måste göras av Regionen vilket kommer ha en direkt påverkan på incidenthanteringsprocesserna.

Ett arbete avseende dessa processer har påbörjats tillsammans med regionledingskontoret (RLK) och övriga vårdverksamheter inom regionen. Detta arbete kommer fortsätta under 2026 då det finns ett beroende på myndigheternas kommande föreskrifter. Incidenthanteringsarbetet ska ses från ett bredare perspektiv där CERT är en delkomponent och där även andra leverantörer som Serviceförvaltningen (SF), Locum och andra tredjepartsleverantörer ingår.

Det finns ett internt behov att se över incidenthanteringsfunktionen (IM) och hur den ska fungera framåt inom Danderyds sjukhus (DS), dels för att närma sig "best practice" och även för att kunna möta kraven som ställs i de externa regelverken.

Vidare konstateras att det saknas en samlad bild över vilka IT-system som används och att flera lokala system saknar systemägare och förvaltning, vilket riskerar att försena åtgärder vid identifierade störningar.

Säkerhet måste ses från ett holistiskt perspektiv och inte bara omfatta hårdvara och operativsystem i serviceförvaltningens datacenter. IT-infrastrukturen som används av Danderyds sjukhus är splittrad mellan flera organisationer såsom, DS, SF, Locum samt externa tredjeparts leverantörer. Denna komplexitet skapar möjliga sårbarheter i verksamheten genom sämre visibilitet och otydligt ansvar.

Ett arbete har initierats med att lägga upp system och applikationer, samt att identifiera systemägare och handläggare (förvaltare) där dessa inte är kända, i regionens nya system för informationssäkerhet och dataskydd (IRIS). Detta arbete påbörjades i samband med att Regionledningskontorets lanserade den nya plattformen i november 2025 och omfattar initialt system som ägs av DS och är installerade på servrar som SF ansvarar för.

Det kommer även finnas system och applikationer som inte ligger hos SF eller förvaltas av sjukhusets centrala förvaltningsorganisation. Dessa kan levereras i form av molntjänster, alternativt är lokalt installerade ute i

verksamheten, och informationen om sådana system och deras förvaltning kan vara bristfällig. Arbetet med verksamhetens system och applikationer ska ses som en kontinuerlig aktivitet, men grundarbetet att få in kända system i IRIS kommer att ske huvudsakligen under 2026.

I enighet med revisorernas samlade bedömning så finns det brister i vissa IT- och incidenthanteringsprocesser inom Danderyds sjukhus. Verksamheten avser att fortsätta utveckla ledningssystemet för informationssäkerhet i linje med de nya lagar och förordningar som introduceras under 2026 och med hjälp av regionens riktlinjer och metodstöd, något som kommer leda till förbättrad sårbarhetshantering och reducerad verksamhetsrisk.

Ekonomiska konsekvenser
Yttrandet medför inga ekonomiska konsekvenser.

Caroline Hällsjö Sander
Sjukhusdirektör

Beslutsunderlag

1. Regionrevisorernas missiv 2026 01 22: “Omhändertagande av CERT-rekommendationer”, RK 2025 0063
2. Regionrevisorernas rapport 13/2025: “Omhändertagande av CERT-rekommendationer”, RK 2025-0063

Skickas till

1. Regionrevisorerna

Godkänt av Caroline Hällsjö Sander, 2026-03-02