

Datum

2018-05-30

Vår beteckning

RV180445

Er beteckning

Regionens revisorer

YTTRANDE ÖVER REVISIONSRAPPORTEN GRANSKNING AV INFORMATIONSSÄKERHET

Regionens revisorer har överlämnat sin granskningsrapport "Granskning av informationssäkerhet" till regionstyrelsen för yttrande. Granskningen syftar till att bedöma om Region Västmanland på en övergripande nivå har ett ändamålsenligt arbete med informationssäkerhet.

Revisorernas uppfattning är att regionstyrelsen till viss del har uppfyllt kontrollmålen. Regionen bedöms sammantaget arbeta aktivt med informationssäkerhet, men förbättringsmöjligheter finns för att nå ett fullt ut tillfredsställande arbete.

Nedan följer beskrivning och kommentarer till synpunkter som lyfts fram i rapporten.

I rapporten framhålls att regionens informationssäkerhetspolicy bör ses över och revideras med lämpliga intervall. Styrelsen delar revisorernas uppfattning och har för avsikt att revidera policyn och överlämna det uppdaterade dokumentet till det nyvalda regionfullmäktige för fastställande under år 2019.

Revisorerna rekommenderar att samtliga principer för informationssäkerhetsarbetet som nämns i policyn omsätts i riktlinjer. De principer som avses är bland annat att all information ska vara kopplad till en ägare, att åtkomst till information ska ges enligt klart definierade principer och att informationssäkerhetsaspekter ska beaktas vid upphandlingar och inköp. Avsikten är självfallet att samtliga principer ska omsättas i riktlinjer. Inom samtliga områden som tas upp i rapporten pågår arbete med framtagande av riktlinjer och instruktioner.

Vidare påtalar revisorerna att samtliga åtgärds mål som definieras i informations-säkerhetsstandarden SS-ISO/IEC 27001 inte omsätts i riktlinjer. I det arbete som bedrivs har dessa åtgärds mål brutits ner i de drygt 100 säkerhetsåtgärder som nämns i Bilaga A till standarden. Av dessa återstår f.n. 20 stycken att analysera och hantera.

Revisorerna påtalar i rapporten brister i styrande dokument och rutiner vad gäller personalsäkerhet. Här vill regionstyrelsen peka på ett stort antal styrande dokument i ledningssystemet som rör t.ex. obligatoriska bakgrundskontroller inför anställning av ny personal¹. Enligt styrelsens uppfattning finns tydliga processer. Däremot instämmer styrelsen i bedömningen att uppföljningen av desamma kunde vara tydligare.

I rapporten efterlyses en analys enligt säkerhetsskyddslagen. Avsikten med en sådan är att identifiera information som kan ha bäring på rikets säkerhet. Under ledning av

¹ Riktlinjerna som avses är bl.a. dokument nr 4520 som övergripande beskriver rekrytering, nr 32045 som behandlar anställning av legitimerad personal. Vidare finns riktlinje 23168 som övergripande styr rekrytering av medarbetare samt dokument nr 23350 som hanterar rekrytering av chefer

Datum

2018-05-30

Vår beteckning

RV180445

regiondirektören genomfördes en sådan analys i december 2017. En sammanfattande säkerhetsskyddsplan kommer färdigställas för fastställande av styrelsen under hösten 2018.

Rapporten innehåller en skrivning om att det skulle finnas ett "glapp i informationskedjan" mellan IT och informationssäkerhet. Styrelsen ser tvärtom att samarbetet är fullt ut fungerande. Täta kontakter förekommer bland annat inom ramen för den systematiska säkerhetsorganisationen och inom regionens systemförvaltningsorganisation.

De synpunkter som i övrigt framkommit i rapporten kommer att vara vägledande i det fortsatta utvecklingsarbetet inom området.

FÖR REGION VÄSTMANLAND



Denise Norström

Regionstyrelsens ordförande



Anders Åhlund

Regiondirektör