TN § 247 Revisionsrapport. Granskning av informations- och cybersäkerhet

Ärendenummer: TN 2023/3267
Paragraf föregående instans: TN AU § 205

Tekniska nämndens beslut

Tekniska nämnden ställer sig bakom rekommendationerna i rapporten.

Sammanfattning

KPMG har på uppdrag av Region Gotlands förtroendevalda revisorer genomfört en granskning av regionens arbete för att upprätthålla en god informations- och cybersäkerhet. Uppdraget ingår i revisionsplanen för år 2023. Syftet med granskningen har varit att bedöma om regionstyrelsen, hälso- och sjukvårdsnämnden, socialnämnden och tekniska nämnden har säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

I rapporten rekommenderas tekniska nämnden att:

• Säkerställa att objektsförvaltningsmodellen och dess aktiviteter implementeras fullt ut.

• Utvärdera behov av resurser i syfte att kunna etablera ett systematiskt informationssäkerhetsarbete som uppnår krav i NIS-direktivet.

• Se över behov av förvaltningsspecifika rutiner för informationssäkerhetsarbetet.

• Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.

• Säkerställ att utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.

• Följa upp informationssäkerhetsarbetet i syfte att kunna fatta beslut om målhandlingsplan för erforderliga åtgärder

Bedömning

Arbetet med att implementera objektsförvaltningsmodellen pågår och beräknas vara genomfört under 2024. Därefter påbörjas den årliga översynen av klassningar, planer och riskanalyser. Samtliga punkter hanteras i det löpande arbetet enligt objektsförvaltningsmodellen.

Det systematiska säkerhetsarbetet kan säkerställas och följas upp i samband med ledningsgruppsmöten och arbetsplatsträffar som fast punkt på dagordningen. Arbete har inletts men behöver struktureras.

Resurser finns för det systematiska arbetet. Information klassas, risker analyseras och handlingsplaner med olika åtgärder tas fram. Men verksamheten blir inte säkrare av en riskbedömning utan först när handlingsplanen är genomförd. När det gäller tekniska åtgärder saknas ofta kompetens inom verksamheten, och med flera parter involverade blir genomförandet ofta komplicerat och tidskrävande. De lösningar som önskas är inte alltid kompatibla med Region Gotlands övriga nuvarande system och policies.

Efter att åtgärden väl är genomförd behöver vi bli bättre på att efterleva och följa de nya säkerhetsrutinerna. Samtidigt som vi inför ny teknik och nya arbetssätt måste vi frångå det gamla. För detta kommer utbildningsinsatser att behövas. Men innan utbildningsinsatser planeras behövs utbildningsmaterial.

Grund för utbildningsmaterial om informationssäkerhet rent allmänt bör tas fram gemensamt inom Region Gotland i syfte att kvalitetssäkra utbildningen. Men framförallt behövs specifik utbildning inom de verksamheter som omfattas av NIS-direktivet eller hanterar annan information av högre skyddsvärde. Medarbetarna behöver veta hur de ska hantera informationen på rätt sätt och förstå varför detta är viktigt. Det är tänkbart att det i vissa fall kommer att krävas dokumenterad genomgången utbildning innan medarbetarna får tillgång till vissa system och dess information.

Informationssäkerhetsarbetet är tänkt att följas upp i och med den årliga översynen av informationsklassningar, förvaltningsplaner och riskanalyser, enligt Region Gotlands objeksförvaltningsmodell.

Ärendets behandling under mötet
Ärendet föredrogs av förvaltningschef Patric Ramberg.

Arbetsutskottets förslag till tekniska nämnden
Tekniska nämnden ställer sig bakom rekommendationerna i rapporten.

Beslutsunderlag
Missiv och rapport, Granskning av informations- och cybersäkerhet, 2023-09-21
TKF tjänsteskrivelse 2023-10-25

Skickas till
Regionstyrelsen ref RS 2023/1887