Revisorerna

Region Gotland

2023-09-21

Till:
Regionstyrelsen, hälso- och sjukvårdsnämnden, socialnämnden och tekniska nämnden

För kännedom:
Regionfullmäktige

Granskning av informations- och cybersäkerhet

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 revisionsrapporten som bifogas framgår väsentliga iakttagelser. Utifrån våra iakttagelser och vår bedömning rekommenderar vi regionstyrelsen att:

- Se över organisationsstrukturen avseende informationssäkerhetschefens roll och placering i regionen.
- Säkerställa att objektsförvaltningsmodellen och dess aktiviteter implementeras fullt ut.
- Säkerställa att riskbedömning och informationsklassning genomförs för informationstillgångar samt att dessa ligger till grund för åtgärds- och handlingsplaner för identifierade säkerhetsåtgärder.
- Säkerställ att regionövergripande utbildningsinsatser genomförs samt att medarbetarnas medverkan följs upp.
- Säkerställ att övervakning av it-system sker i tillräcklig utsträckning samt att säkerhetshändelser loggas.
- Säkerställ att inträffade incidenter analyseras i syfte att identifiera eventuella åtgärder som behöver vidtas.
- Följa upp informationssäkerhetsarbetet både på förvaltningsnivå och regionövergripande nivå i syfte att kunna fatta beslut om mål-handlingsplan för erforderliga åtgärder.

Vidare rekommenderar vi hälso- och sjukvårdsnämnden 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 mål-handlingsplan för erforderliga åtgärder.

Vi rekommenderar även socialnämnden att:

- 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 mål-handlingsplan för erforderliga åtgärder.

Slutligen rekommenderar vi 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 mål-handlingsplan för erforderliga åtgärder.

Vi emotser styrelsens och nämndernas yttrande till våra iakttagelser och rekommendationer i bifogad rapport senast 2023-12-04.

De förtroendevalda revisorerna i Region Gotland,

Barbro Hejdenberg Ronsten
Ordförande