RS § 293 Region Gotland – Organisation informations- och cybersäkerhet

Ärendenummer: RS 2026/1061
Paragraf föregående instans: AU § 166

Regionstyrelsens förslag till regionfullmäktige

- Dokument ”Förslag till organisation informations- och cybersäkerhet” fastställs.

Sammanfattning

Cybersäkerhetslag (2025:1506) och NIS2-direktivet syftar till att skapa en hög gemensam cybersäkerhetsnivå i hela Europeiska unionen. Lagstiftningen anger att ledningen ansvarar för att styra organisationens cybersäkerhetsarbete så att det bedrivs systematiskt och riskbaserat. Det man i lagen hänvisar till med begreppet ledning, är i regionens fall, regionstyrelsen.

I syfte att uppnå ett systematiskt arbetssätt behöver arbetet med informations- och cybersäkerhet drivas och samordnas centralt. Med anledning av detta behöver en struktur för hur beslutsfattande inom ramen för informationssäkerhet fastställas. I myndigheternas föreskrifter regleras att ledningen (regionstyrelsen) ska:

- besluta om mål, inriktning och resurser,
- fastställa roller och mandat och ansvar,
- säkerställa att organisationen har tillräcklig kompetens och tillräckliga resurser för att nå den säkerhetsnivå som krävs,
- säkerställa att organisationen vidtar tekniska, operationella och organisatoriska åtgärder för att hantera risker.

Arbetet med cybersäkerhet ska utgå ifrån ett allriskperspektiv. Åtgärderna ska vara proportionella och baserade på riskanalys.

Bedömning

I syfte att uppnå de krav som ställs på Region Gotland utifrån Cybersäkerhetslag (2025:1506) behövs beslut om hur strukturer för hur cyber- och informationssäkerhetsarbetet i Regionen ska organiseras. Idag styr varje nämnd själv hur arbetet ska bedrivas, vilket innebär att en gemensam struktur saknas och att nivån på säkerhet kan variera mellan nämnder. Lagstiftaren ser däremot regionen som en helhet som ska ha en gemensam styrning och struktur för arbetet, och där ledningen (regionstyrelsen) ansvar för att hur regionens informations- och cybersäkerhetsarbete samordnas och struktureras.

För att kunna uppnå ett sådant strukturerat arbetssätt behöver det finnas en central funktion som samordnar och utvecklar det strategiska och

regionövergripande arbetet. En sådan funktion ska även finnas för att informera och skapa beslutsunderlag till regionstyrelsen.

I dokumentet *"Förslag till organisation informations- och cybersäkerhet"* föreslås att denna funktion ska finnas på Regionstyrelseförvaltningen, i form av informationssäkerhetschef eller CISO (Chief information security officer). I dokumentet föreslås även en organisationsstruktur som ligger till grund för Region Gotlands informations- och cybersäkerhetsarbete.

Bedömning av konsekvenser i tvärperspektiv

1. Rättslig grund/rättsligt perspektiv

Cybersäkerhetslag, NIS2- direktiv.

2. Ekonomiskt perspektiv

Inom ramen för NIS2 och cybersäkerhetslagen kan brister i efterlevnad av lagstiftningen vara sanktionsgrundande. Sanktionerna kan uppgå till 10 mnkr.

3. Barnperspektiv

Ej aktuellt.

4. Jämställdhetsperspektiv

Ej aktuellt.

5. Landsbygdssäkring/geografiskt perspektiv

Ej aktuellt.

6. Klimat- och miljöperspektiv

Ej aktuellt.

Ärendets behandling under mötet
Ärendet föredras av Lisa Aurell Sandström, sakkunnig handläggare, regionstyrelseförvaltningen.

Ordförande ställer proposition på arbetsutskottets förslag och finner att det bifalls.

Beslutsunderlag
Förslag till organisation informations- och cybersäkerhet
Regionstyrelseförvaltningens tjänsteskrivelse 2026-08-03

Skickas till
Samtliga nämnder och förvaltningar