Förslag till Organisation informations- och cybersäkerhet

Fastställd av regionfullmäktige
Framtagen av regionstyrelseförvaltningen
Datum 2026-09-21
Gäller tillsvidare
Ärendenr RS 2026/1061
Version [1.0]

Förslag till Organisation informations- och cybersäkerhet

Inledning

Syftet med cybersäkerhetslagen (2025:1506) är att skapa en hög gemensam cybersäkerhetsnivå i hela den Europeiska unionen. Ledningen ansvarar för att styra organisationens cybersäkerhetsarbete så att det bedrivs systematiskt och riskbaserat. Med begreppet ledning avses regionstyrelse.[1]

Ledningen ska besluta om mål, inriktning och resurser, fastställa mandat och se till att organisationen har tillräcklig kompetens och tillräckliga resurser för att nå den säkerhetsnivå som krävs.[2] Arbetet med informations- och cybersäkerhet ska utgå ifrån ett allriskperspektiv.

Ledningen ansvarar även för att säkerställa att organisationen vidtar tekniska, operationella och organisatoriska åtgärder för att hantera risker. Åtgärderna ska vara proportionella och baserade på riskanalys.

Mål och inriktning

Region Gotland ska upprätta ett systematiskt och riskbaserat arbetssätt enlighet med gällande lagstiftning. Arbetet ska inte hanteras som ett separat spår, utan som en naturlig del av verksamhetsstyrningen.
Med systematiskt och riskbaserat avses arbete som bedrivs med stöd av interna regler och arbetssätt för att upprätta, genomföra, driva, övervaka, kontrollera, underhålla och utveckla organisationens cybersäkerhet utifrån risk.

[1] Regeringens proposition 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag,
[2] Cybersäkerhetslagen för ledningen – Nationellt cybersäkerhetscenter

Region Gotland
Besöksadress Visborgsallén 19
Postadress SE-621 81 Visby
Telefon +46 (0)498 26 90 00
E-post regiongotland@gotland.se
Org nr 212000-0803
Webbplats www.gotland.se

Styrdokument

Styrdokumentet Informationssäkerhetspolicy Region Gotland fastställdes i december 2025 av regionfullmäktige. I detta dokument föreslås att även dokumentet Riktlinjer för informationssäkerhet Region Gotland ska vara regionövergripande i syfte att uppfylla cybersäkerhetslagens krav på ett systematiskt arbetssätt, och därmed fastställas av regionfullmäktige. Region Gotlands Riktlinjer för informationssäkerhet är i dagsläget under omarbetning. Beslut om framtida eventuella ändringar i dokumentet Riktlinjer för informationssäkerhet föreslås delegeras till regionstyrelsen i syfte att inte i onödan belasta regionfullmäktige och få framdrift i förändringsarbetet.

Kommentar [KN1]: Detta stycke rör ett förslag till delegering av framtida ändringar i ett annat styrdokument. Ett sådant förslag bör läggas fram i samband med att riktlinjerna ska beslutas och fyller ingen direkt funktion här.

Roller och mandat

Ledningen (regionstyrelsen) ansvarar för att tydliggöra roller och ansvar i organisationen i syfte att säkerställa att all information och alla system har ägare som tar ansvar för säkerheten utifrån sina roller. Ledningen ska dessutom säkerställa att det finns en funktion som samordnar cybersäkerhetsarbetet och ger ledningen det underlag de behöver, exempelvis en CISO eller informationssäkerhetschef.

CISO alt. Informationssäkerhetschef

Funktionsbeskrivning

- Har det övergripande ansvaret att leda och samordna arbetet med informationssäkerhet på strategisk nivå.
- Underställd regionstyrelse i informationssäkerhetsfrågor.
  Ansvarar för rapportering och beslutsunderlag till regionstyrelse och KLG och förvaltningsledning.
- Ansvarar för framtagande, förvaltande och efterlevnad av policy, riktlinjer och årshjul.
- Planerar och samordnar regiongemensamma aktiviteter och planer som exempelvis övnings- och utbildningsplaner.
  Fungerar som länk mellan regionens ledning och verksamhet (via exempelvis nätverk).
  Kravställande gentemot IT och Digitaliseringsavdelningen.
  Rådgivande och stödjande gentemot verksamheten.
- Kontaktperson gentemot myndigheter och externa parter i informationssäkerhetsfrågor.
- Ansvarar för myndighetsrapportering vid incidenter.

Mandat

- Att kravställa vid till exempel utvecklingsprojekt.
- Att utföra intern granskning och kontroll av att styrdokument efterlevs.
- Att rapportera interna brister i efterlevnaden av styrdokument.
- Att godkänna eventuella undantag från styrdokument, alternativt yttra sig inför eventuella undantag.
- Att godkänna specifika informationssäkerhetslösningar (det vill säga tolka ifall de uppfyller styrdokument), alternativt yttra sig inför godkännande.
- Att stoppa aktiviteter som strider mot styrdokument, alternativt att rapportera aktiviteter som strider mot styrdokument.

Informationssäkerhetsspecialist alt. samordnare

Funktionsbeskrivning

- Arbetar strategiskt och operativt med informationssäkerhet. Det är av vikt att denna funktion finns i samtliga förvaltningar, vid behov inom flera avdelningar eller enheter.
- Stödjer CISO alt. informationssäkerhetschef, bidrar vid framtagande, förvaltning och tillämpning av policyer, riktlinjer och styrdokument samt vägleder regionens förvaltningar i hur krav, exempelvis enligt NIS2 och cybersäkerhetslagen och andra regelverk, kan integreras i befintliga processer.
- Driver regiongemensamma utbildnings- och informationsinsatser inom informationssäkerhet samt arbetar med att stärka förvaltningarnas egen förmåga att arbeta med frågorna.
- Deltar i Region Gotlands Nätverk för informationssäkerhet.
- Fungerar som stöd i informationssäkerhetsfrågor och löpande ärenden som uppstår i verksamheten, exempelvis informations- och cybersäkerhetsincidenter, informationsklassning och risk- och sårbarhetsanalyser.
- Samverkar med andra centrala funktioner och nätverk inom förvaltningarna och IT- och Digitaliseringsfunktion i frågor som rör informations- och cybersäkerhet.

Nätverk Informationssäkerhet
Befintlig arbetsgrupp AG-Infosäk föreslås att göras om till Nätverk för informationssäkerhet. Syftet med detta är att möjliggöra vägar mellan ledning och verksamhet. Regionstyrelsen ger inriktning och uppdrag till CISO alt. informationssäkerhetschef som i nätverket som hanterar frågorna. Nätverket tar fram underlag för beslut och rapportering gentemot både verksamhet och ledning.

Ansvar

Regionfullmäktige – Beslutar om policy, regionövergripande riktlinje samt regionövergripande budget

Regionstyrelse – Beslutar om mål, inriktning och resurser. Fastställer roller och mandat. Informerar sig om resultat av risk och sårbarhetsanalyser, incidenter och omvärldsläge. Beslutar om nivå på riskaptit och säkerhetsåtgärder. Föredrar budgetbehov för regionfullmäktige.

CISO alt. Informationssäkerhetschef – Befattningen är placerad på Regionstyrelseförvaltningen, och rapporterar till regionstyrelse och KLG. Leder och samordnar Region Gotlands övergripande informationssäkerhetsarbete på strategisk nivå. Fungerar som länk mellan, och samverkar med regionstyrelse, KLG/förvaltningsledning och verksamhet. Leder Nätverk för informationssäkerhet.

KLG och Förvaltningsledning – Säkerställer resurser och kompetens i respektive verksamhet. Ansvarar för att informationssäkerhetsarbetet drivs i enlighet med policyer, riktlinjer objektsförvaltningsmodell och av regionstyrelsen fattade beslut.

Förvaltningar
Utser eller rekryterar förvaltnings- eller avdelningsspecifika informationssäkerhetsspecialister/samordnare. Ansvarar för att fattade beslut implementeras och följs upp, samt arbetar proaktivt med risk- och sårbarhetsanalys. Samverkar med CISO alt. informationssäkerhetschef. Driver förvaltningsspecifika frågor i Nätverk för informationssäkerhet. Återrapporterar incidenter, resultat av analyser och uppföljning till CISO alt. informationssäkerhetschef

Gränsdragning mellan IT och Informationssäkerhet

För att säkerställa att informationssäkerheten förblir en strategisk fråga snarare än en teknisk, är en gränsdragning mellan de båda funktionerna viktig. CISO alt. informationssäkerhetschefen bör därför vara kravställande gentemot IT- och digitaliseringsorganisationen, vilken fokuserar på att skydda IT-system och tillgångar, inklusive hårdvara, mjukvara och nätverksinfrastruktur och är en delmängd av cybersäkerheten.

Budget

En del i ledningens arbete är enligt cybersäkerhetslagen att fastställa budget och resurser för informationssäkerhetsarbetet. Kommunallagen (SFS 2017:725, 2 kap. 1 §) anger att beslut om budgetfrågor skall fattas i regionfullmäktige, vilket i praktiken innebär att regionstyrelsen ansvarar för att lägga fram förslag på budget för cybersäkerhetsarbetet, baserat på verksamhetens behov.

Informationssäkerhetsarbetet är regionövergripande och placering av, och storlek på budget behöver anpassas efter detta. Med Region Gotlands gap-analys och handlingsplan som grund är det tydligt att informationssäkerhetsarbetet är kostnadsdrivande, både vad gäller resurser och tekniska åtgärder. Det är därför viktigt att beslut fattas kring hur kostnader för detta arbete ska fördelas.

Budget och statliga medel för informations- och cybersäkerhetsfrågor bör placeras centralt på regionstyrelseförvaltningen, för att kunna användas och äskas av såväl informations- som IT-säkerhetsfunktionerna. Detta för att medel inte ska kunna prioriteras om hos de båda funktionerna. Därtill behöver ökade personalresurser säkerställas för att kunna omhänderta regionövergripande åtgärder och insatser.

Relaterade dokument

Cybersäkerhetslag (2025:1506) | Sveriges riksdag

Cybersäkerhetsförordning (2025:1507) | Sveriges riksdag

Cybersäkerhetslagen för ledningen

Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag