POLICY

Informations-säkerhetspolicy

Fastställd av regionfullmäktige
Framtagen av regionstyrelseförvaltningen
Datum 2025-12-10
Gäller 2026-2030
Ärendenr RS 2025/1981
Version [1.0]

Informationssäkerhetspolicy

Innehåll

1. Om Informationssäkerhetspolicyn 2
1.1 Syfte 2
2. Definitioner 2
2.1 Informationstillgångar 2
2.2 Informationshantering 3
2.3 Informationssäkerhet 3
3. Mål och Principer 3
4. Arbetssätt 4
5. Uppföljning 5
6. Ansvar 5
7. Regulatoriska krav 7
8. Relaterade dokument 7

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

1. Om Informationssäkerhetspolicyn

Denna policy gäller för Region Gotland samt bolag som hel- eller majoritetsägda av Region Gotland.

I de fall extern part hanterar Region Gotlands information ska denne genom avtal eller liknande förbindas att följa motsvarande krav på hantering av information som gäller för regionen.

Informationssäkerhetspolicyn beskriver Region Gotlands övergripande mål och principer med informationshantering och informationssäkerhet. Policyn konkretiseras i de dokument som redovisas i avsnittet ”Relaterade dokument”.

Region Gotland förnyar och kompletterar regelbundet sitt informationssäkerhetsarbete för att möta nya regulatoriska krav samt nationella riktlinjer från MSB.

Informationssäkerhetspolicyn fastställs av regionfullmäktige och anger, på en övergripande nivå, Region Gotlands grundläggande synsätt och viljeinriktning gällande arbete med informationssäkerhet.

1.1 Syfte

Medborgarna ska stå i centrum för Region Gotlands verksamhet och de gemensamma värderingarna omtanke, förtroende och delaktighet ska genomsyra arbetet.

Region Gotland har i huvudsak tre uppdrag: kommunala uppgifter, Regionala uppgifter och det Regionala utvecklingsansvaret. I uppdragen hanteras viktiga samhällstjänster och Regionens information är därför en kritisk del i Sveriges och samhällets informationssäkerhet. För att säkerställa en robust, flexibel och uthållig verksamhet som har allmänhetens förtroende är det av stor betydelse att informationssäkerhetsarbetet är prioriterat och bedrivs metodiskt och långsiktigt. Denna policy syftar till att ge vägledning för beslut, prioriteringar och styrning inom informationssäkerhet.

2. Definitioner

Information är en av Region Gotlands viktigaste tillgångar och hanteringen av den är en mycket viktig del i arbetet.

2.1 Informationstillgångar

Med informationstillgångar avses all information som ägs av Region Gotland, oavsett om den behandlas manuellt eller digitalt och oberoende av dess form eller miljön den förekommer i.

Informationen rör exempelvis personal, tjänster, ekonomi och omgivning med medborgare, näringsliv och civila samhället.

Information kan vara i såväl fysisk som digital form och förmedlas via

exempelvis text, ljud, bilder eller film. Information kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

2.2 Informationshantering

Region Gotland ska i enighet med offentlighetsprincipen uppnå och upprätthålla en informationshantering som säkerställer långsiktigt bevarande, förvaltande och tillgängliggörande av information.

Informationshantering är ett samlingsbegrepp för hur Region Gotland förhåller oss till information som tillgång, exempelvis hur Region Gotland genererar, behandlar, förmedlar, kvalitetssäkrar och skyddar information.

Informationshanteringen ska bidra till en effektivare och öppnare regional organisation som på bästa sätt tar tillvara medborgarnas intressen.
Ett medvetet agerande vad gäller Region Gotlands informationshantering ska leda till att medarbetare och politiker tar ansvar för dåtid, nutid och framtid.

Informationshantering omfattar fyra områden – informationsförvaltning, informationsförsörjning, informationssäkerhet och dataskydd.

- **Informationsförvaltning** handlar om att hålla informationen ordnad, beskriven och strukturerad.
- **Informationsförsörjning** handlar om att säkerställa tillgång till information.
- **Informationssäkerhet** handlar om att skydda information.
- **Dataskydd** handlar om skyddet för den personliga integriteten vid behandling av personuppgifter.

2.3 Informationssäkerhet

Informationssäkerheten är en integrerad del i Region Gotlands ledningssystem och syftar till att ge Region Gotlands informationstillgångar rätt skydd över tid. Informationssäkerhet bygger på säkerhetsaspekterna:

- **Konfidentialitet** – Att informationen inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.
- **Riktighet** – Att det går att lita på att informationen är korrekt.
- **Tillgänglighet** – Att informationen finns tillgänglig när den behövs, för den som har behörighet att ta del av den.
- **Spårbarhet** – Förmågan att dokumentera och kontrollera vem som gjort vad, när och under vilka förutsättningar, i relation till informationen.

3. Mål och Principer

Att informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet bevaras så att rätt personer får tillgång till rätt information vid rätt tillfälle, nu

och i framtiden, är målet för en väl fungerande informationssäkerhetstrategi. Informationshanteringen ska bidra till att Region Gotland når sin vision och sina mål och att krav i såväl författningar som avtal kan efterlevas.

Tillgången till allmänna offentliga handlingar är en förutsättning för allmänhetens insyn i den offentliga verksamheten och en demokratisk dialog i samhället.

För att Region Gotland ska nå målen med informationssäkerhet ska arbetet vila på följande principer:

- **Öppenhet**, vilket förutsätter att Region Gotland vilar på en grund av informationsförvaltning, informationssäkerhet och dataskydd och därmed säkerställer handlingsoffentligheten.
- **Integrerad informationshantering**, som en naturlig del av verksamhetens ordinarie processer.
- **Riskbaserat, proaktivt och systematiskt arbetssätt** där informationssäkerheten i ett tidigt skede tas med i verksamhetsplanering, verksamhetsutveckling och projekt. Det innebär även att Region Gotland kontinuerligt följer upp, utvärderar och förbättrar regionens informationssäkerhetsarbete.
- **Incidenthantering** där avvikelser och incidenter som inträffar ska hanteras på ett strukturerat och ordnat sätt.
- **Etablerade arbetssätt**, där arbete med informationshantering ska bygga på relevanta standarder och andra tillförlitliga arbetssätt.
- **Kommunikation och stöd**. Stödmaterial, rutiner och regelverk ska vara väl kommunicerade och förankrade i verksamheten för att skapa förutsättningar för en väl fungerade informationshantering.
- **Förtroende- och trygghetsskapande** genom robust, säker och tillförlitlig hantering av information
- **Personlig integritet**. Region Gotland värnar om, samt skyddar den personliga integriteten med hänsyn till den enskildes friheter och rättigheter.

4. Arbetssätt

Informationssäkerhetsarbetet i Region Gotland ska kännetecknas av:

- att kunskap finns om hur informationssäkerheten säkerställs
- att krishanteringsförmågan fortlöpande analyseras och upprätthålls
- att alla informationstillgångar klassificeras
- att hotbilden mot informationstillgångar fortlöpande analyseras

- att händelser som kan leda till negativa konsekvenser förebyggs

5. Uppföljning

Statusen för informationshanteringen ska regelbundet följas upp och rapporteras till objektsägarna, i enlighet med regionens objektsförvaltnings-modell.

Uppföljningen ska ge en bild av hur arbetet med informationshanteringen fungerar och vilka brister som behöver åtgärdas, samt för att kontinuerligt utveckla och revidera informationssäkerhetsarbetet. Utöver den regelbundna rapporteringen kan särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, motivera ytterligare rapporteringar.

Uppföljningen är en egenkontroll för objektssägaren och skiljer sig från den tillsyn över att nämnder och kommunala bolag följer arkivlagen som kommunstyrelsen utövar i egenskap av arkivmyndighet.

6. Ansvar

Efterlevnad av denna policy och tillhörande riktlinjer ska följas upp minst årligen genom revision och stickprov på samtliga nivåer. Avvikelser ska dokumenteras och åtgärdas.

Regionfullmäktige uttrycker principer och viljeinriktning genom att fastställa Region Gotlands informationssäkerhetspolicy.

Regionstyrelsen har det yttersta ansvaret för Region Gotlands informationssäkerhetsarbete och fastställer dokumentet ”Riktlinje för informationssäkerhet”. Regionstyrelsen äger och ansvarar för Regiongemensam infrastruktur, tjänster, system och applikationer.

Informationssäkerhetschefen arbetar på uppdrag av regiondirektören. Informationssäkerhetschefen har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet och ledningssystemet för informationssäkerhet (LIS) i
regionen. Informationssäkerhetschefen ska även samordna anpassning till NIS2 och fungera som kontakt mot nationella cybersäkerhetsmyndigheter.

Säkerhetsskyddschefen arbetar på uppdrag av regiondirektören. Säkerhetsskyddschefen ska leda och samordna säkerhetsskyddsarbetet samt kontrollera det egna säkerhetsskyddet av regionens säkerhetsskyddsklassificerade uppgifter.

Nämnder och förvaltningar äger och ansvarar för egen verksamhetsspecifik infrastruktur, tjänster, system och applikationer och tillsätter informations- och objektägare för dessa.

Chefer ansvarar för att medarbetare har rätt kunskap och förutsättningar för att upprätthålla informationssäkerhetsarbetet.

Alla medarbetare har ett ansvar för att informationssäkerheten upprätthålls

samt att rapportera incidenter.

7. Regulatoriska krav

Lagar som direkt eller indirekt påverkar informationssäkerhetsåtgärder eller -krav för regionen inkluderar bland annat följande:

- Säkerhetsskyddslagen (2018:585),
- lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS),
- Europaparlamentets och rådets direktiv (EU 2022/2555) om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, Cybersäkerhetslagen/Nya regler om Cybersäkerhet (SOU2024:18)[1]
- EU:s allmänna dataskyddsförordning (EU/2016/679) (GDPR),
- registerförfattningar som exempelvis patientdatalagen (2008:355) (PDL),
- offentlighets- och sekretesslagen (2009:400) (OSL),
- arkivlagen (1990:782), och
- lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap samt till dessa hörande författningar såsom förordningar och föreskrifter (LEH).

8. Relaterade dokument

I detta dokument, ”Informationssäkerhetspolicy”, fastställs synen på informationssäkerhet, övergripande mål och organisationens intention med informationssäkerhetsarbetet. Övriga relaterade dokument:

- Riktlinjer för informationssäkerhet – beskrivning av vad som måste etableras för att uppfylla informationssäkerhetspolicyn.
- Objektsförvaltningsmodell - beskrivning av ansvar och roller i informationshanteringsarbetet.
- Netikett – Riktlinjer för IT-användning
- Riktlinjer för anställda som använder egna IT-verktyg och tjänster
- Informationshanteringsplan – Riktlinjer för lagring, gallring och arkivering av information

Sammantaget är detta Region Gotlands styrdokument för informationssäkerhetsarbete på en strategisk nivå. Utifrån dessa styrande dokument skapar nämnder och förvaltningar rutiner anpassade för den specifika verksamheten.

[1] Fastställd lag finns i nuvarande läge inte antagen. Denna beräknas fastställas i januari 2026 och baseras på nämnda föreskrifter.