POLICY

Informations-säkerhetspolicy

Fastställd av regionfullmäktige
Framtagen av regionstyrelseförvaltningen
Datum 2023-06-19
Gäller 2023-2026
Ärendenr RS 2023/380
Version 1.0

Informationssäkerhetspolicy

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

Bakgrund och 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, landstingsuppgifter 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.

Definition

Informationssäkerhet handlar om att ge Region Gotlands informationstillgångar rätt skydd över tid och omfattar säkerhetsaspekterna:

- **Konfidentialitet** - egenskap hos informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer
- **Riktighet** - egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring
- **Tillgänglighet** - egenskap hos informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer
- **Spårbarhet** - entydig härledning av utförda aktiviteter

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

Omfattning

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

Lagar med direkt eller indirekt påverkan på åtgärder eller krav rörande informationssäkerhet som rör regionen kan nämnas bland annat

- säkerhetsskyddslagen (2018:585),
- lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS),
- EU:s allmänna dataskyddsförordning (EU/2016/679)(GDPR),
- registerförfattningar som till exempel 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).

Relaterade dokument

I detta dokument, *Informationssäkerhetspolicy,* fastställs synen på informationssäkerhet, övergripande mål och organisationens intention med informationssäkerhetsarbetet. I dokumentet *Riktlinjer för informationssäkerhet* beskrivs vad som måste etableras för att uppfylla informationssäkerhetspolicyn. Sammantaget är detta Region Gotlands styrdokument för informationssäkerhetsarbete på en strategisk nivå. Utifrån dessa styrande dokument skapar nämnder och förvaltningar rutiner på en taktisk och operativnivå.

Ansvar

Ansvaret för Region Gotlands informationssäkerhetsarbete ska följa det normala delegerade verksamhetsansvaret på alla nivåer.

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

Regionstyrelsen har det yttersta ansvaret för Region Gotlands informationssäkerhetsarbete och fastställer *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.

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.

Alla medarbetare har ett ansvar för att informationssäkerheten upprätthålls samt att rapportera incidenter.

Inriktning

Informationssäkerhetsarbete i Region Gotland 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, och
- att arbete med informationssäkerhet är en naturlig del i verksamheten.