RIKTLINJER

Riktlinjer för Informations-säkerhet

Fastställd av Välj ett objekt
Framtagen av regionstyrelseförvaltningen
Datum [Beslut/Publiceringsdatum]
Gäller 2023-2026
Ärendenr RS 2023/380
Version [1.0]

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

Innehållsförteckning

Informationssäkerhet

Information är en av Region Gotlands viktigaste tillgångar och hanteringen av den är en mycket viktig del i arbetet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i. Informationen kan till exempel vara talad, skriven eller tryckt på papper, elektronisk/digital eller förpackad i bild- film- eller ljudformat.

Definition

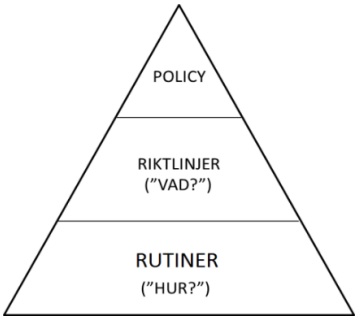
Informationssäkerhet handlar om att ge Region Gotlands informationstillgångar rätt skydd över tid och omfattar säkerhetsaspekterna:

- **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

Struktur styrande dokument

I *Informationssäkerhetspolicyn* fastställs synen på informationssäkerhet, övergripande mål och organisationens intention med informationssäkerhetsarbetet.

I detta dokument, *Riktlinjer för informationssäkerhet*, beskrivs vad som måste etableras för att uppfylla informationssäkerhetspolicyn.



Utifrån detta upprättas sedan *Rutiner*, som detaljerat redogör för hur exempelvis aktiviteter och säkerhetslösningar ska utformas och tillämpas, för att informationssäkerhetspolicyn och riktlinjerna ska följas. Informationssäkerhet ska vara en naturlig del i Region Gotlands verksamhet och kan påverka andra styrande dokument.

Mål för informationssäkerhetsarbetet

Målet för informationssäkerhetsarbetet i Region Gotland är:

- att informationssäkerhetsarbetet ska vara riskbaserat och bedrivas enligt standardfamiljen SS-ISO/IEC 27000, vilket kontrolleras genom revision,
- att informationssäkerheten ska vara en integrerad del i Region Gotlands verksamhetsutveckling och objektförvaltningsmodell, vilket kontrolleras genom revision,
- att alla förtroendevalda, medarbetare och externa utförare ska vara medvetna om informationssäkerhetsfrågornas betydelse samt ha kunskaper om vad som gäller i Region Gotland, och

- att medborgare ska i sin insyn och delaktighet i Region Gotlands verksamhet uppleva omtanke, förtroende, och delaktighet.

Organisation av säkerhetsarbetet

Ansvaret för informationssäkerhet är kopplat till det delegerade verksamhetsansvaret. För att säkerställa informationssäkerheten inom Region Gotland ska det på alla nivåer finnas en organisation och resurser, som aktivt och systematiskt förebygger risker och föreslår konkreta åtgärder för att undanröja olika hot.

Intern organisation

Regionfullmäktige uttrycker principer och viljeinriktning genom att fastställa Region Gotlands *Informationssäkerhetspolicy*.

Regionstyrelsen har det yttersta ansvaret för Region Gotlands informationssäkerhetsarbete. Regionstyrelsen utarbetar, förvaltar, fastställer och följer upp *Riktlinje för informationssäkerhet.* Regionen är att anse som en verksamhetsutövare avseende säkerhetsskydd enligt säkerhetsskyddslagen (2018:585).

Regionstyrelseförvaltningen ska stödja regionstyrelsen i att samordna och följa upp Region Gotlands informationssäkerhetsarbete. Regionstyrelseförvaltningen ska möjliggöra en
säker informationshantering och informationsförvaltning.

Varje nämnd ansvarar för att informationssäkerhetspolicy och riktlinjer för informationssäkerhet efterföljs och inarbetas i den egna verksamhetens lokala handlingsplaner och rutiner. Detta ska vara en naturlig del i verksamhetsutveckling, förvaltning och uppföljning.

Förvaltningarna ansvarar för att informationssäkerhetspolicy och riktlinjer för informationssäkerhet efterföljs och inarbetas i den egna verksamhetens lokala handlingsplaner och rutiner. Detta ska vara en naturlig del i verksamhetsutveckling, förvaltning och uppföljning. Informationssäkerhetsarbetet samordnas via Regionstyrelseförvaltningen.

Roller och ansvar

Informationssäkerhetschefen har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet och ledningssystemet för informationssäkerhet (LIS) i regionen.

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

Signalskyddschefen har till uppgift att ansvara för ledning och samordning av signalskyddstjänsten.

Informationsägarna ansvarar för hur informationen får hanteras och av vem. Detta gäller när information bearbetas, lagras och transporteras. Informationsägarna ska minst årligen ansvara för att informationen informationsklassificeras enligt Region Gotlands informationsklassningsmodell samt ansvara för att riskanalyser genomförs minst årligen och vid större förändringar. Informationsägare är ytterst nämnden.

Objektägarna har övergripande ansvar för respektive informationssystem och dess användning. System ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov samt hur dess innehåll informationsklassificeras och resultatet av genomförda riskanalyser. Objektsägare fastställer systemsäkerhetsplan (krav på säkerhetsåtgärder) innan driftsättning samt förvaltningsplaner enligt Region Gotlands objektsförvaltningsmodell.

Dataskyddsombudet har en reviderande roll av skyddet kring personuppgifter och ska informeras då riskanalyser relaterat till dataskyddet sker för att säkerställa att tillräckliga skyddsåtgärder påförs. Dataskyddsombudet är kontaktperson mot Integritetsskyddsmyndigheten (IMY) samt mot medborgare.

Tjänsteman i beredskap (TiB) har mandat att aktivera hela eller delar av krisledningsstaben och är initialt stabschef i krisledningsstaben.

Chef/arbetsledare ansvarar för att inom respektive område uppmärksamma och åtgärda risker samt att policy, riktlinjer och rutiner efterlevs.

Informationsanvändare, (kan vara anställd, förtroendevald, utförare eller annan extern partner,) som i sin yrkesutövning hanterar information har ett ansvar för att informationssäkerheten upprätthålls, under och efter anställning eller åtagande, samt att rapportera incidenter.

Personalsäkerhet

Före anställning eller uppdrag

Vid rekrytering ska säkerhetsbestämmelserna beaktas. Platssökande ska kontrolleras på lämpligt sätt, särskilt om anställningen medför åtkomst till sekretessbelagda uppgifter eller på annat sätt omfattar säkerhetskritiska aktiviteter. Behovet av kontrollmoment ska analyseras innan rekryteringsprocessen påbörjas och kontrollerna stå i proportion till den berörda tjänsten.

Behörig att ta del av säkerhetsskyddsklassificerade uppgifter eller delta i säkerhetskänslig verksamhet är endast den som genomgått en säkerhetsprövning innan deltagande eller informationsåtkomst. Personen ska vidare ha relevanta kunskaper om säkerhetsskydd och nödvändiga befogenheter samt förstå och kvittera kraven på sekretess och tystnadsplikt.

Under anställning eller uppdrag

Alla anställda, förtroendevalda, utförare och konsulter ska löpande göras medvetna om sitt ansvar för informationssäkerheten. De ska också ges den kunskap i informationssäkerhet som behövs för att de ska kunna utföra sina uppdrag. All personal ska ha kunskap om offentlighetsprincipen och om offentlighets- och sekretesslagen (2009:400) samt i förekommande fall om säkerhetsskyddslagen (2018:585).

Avslut eller ändring av anställning eller uppdrag

Det ska finnas rutiner som styr avveckling/förändring av åtkomst till informationssystem för all personal både intern och extern.

När en anställning upphör ska den anställde påminnas om att sekretessreglerna gäller även efter anställningen.

När en anställning eller ett deltagande i den säkerhetskänsliga verksamheten upphör ska en ansökan om upphörande av registerkontroll meddelas Säkerhetspolisen samt ett avslutande säkerhetsprövningssamtal genomföras.

För personal med priviligierade behörigheter till informationssystem och där uppsägning från arbetsgivarens sida eller där övertalighet är aktuell ska behörigheterna för berörda personer omedelbart begränsas.

Hantering av tillgångar

Ansvar för tillgångar

Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är informationsägare och objektsägare. Tillgångens informationsklassificering och de regulatoriska krav, regler och avtal som tillgången omfattas av ska också ingå i förteckningen. Alla verksamheter ansvarar för att registrering sker och upprätthålls enligt rådande modell i för ändamålet avsett verktyg.

Informationsklassificering

Information ska informationsklassificeras så att alla informationstillgångar och informationsbehandlingsresurser ges rätt skydd.

Informationen ska informationsklassificeras utifrån den funktion och dess betydelse för verksamheten som den har och de konsekvenser det medför om informationen skulle hanteras felaktigt, försvinna, hamn i orätta händer etc.

Vid bedömning används följande fyra konsekvensnivåer:

- Försumbar skada
- Måttlig skada - ex minskad förmåga att genomföra verksamhetens uppgifter, men effektiviteten är påvisbart reducerad
- Betydande skada - ex tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, samt förlust av skapat förtroende
- Allvarlig skada - ex massiv informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, samt fara för liv och hälsa

Information som innehållet säkerhetsskyddsklassificierade uppgifter ska säkerhetsskyddsklassificeras enligt nedan.

Säkerhetsskyddsklassificering

Säkerhetsskyddsklassificerade uppgifter som rör säkerhetskänslig verksamhet eller uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet.
Vid bedömning används följande fyra säkerhetsskyddsklasser:

- Begränsat hemlig (BH) vid endast ringa skada för Sveriges säkerhet

- Konfidentiell (K) vid en inte obetydlig skada för Sveriges säkerhet
- Hemlig (H) vid en allvarlig skada för Sveriges säkerhet
- Kvalificerat hemlig (KH) vid en synnerligen allvarlig skada för Sveriges säkerhet

Bedömning av informationssäkerhetsrisker

Kontinuerliga och systematiska risk- och sårbarhetsanalyser ska genomföras i alla verksamheter. Syftet är att minimera sannolikhet eller konsekvens för att risker inträffar samt ge underlag till hur kriser ska hanteras i verksamheten. Riskreducerande åtgärder ska skyndsamt vidtas samt även kravställas vid anskaffning.

Hantering av lagringsmedia

Rutiner ska finnas för att förhindra obehörigt röjande, modifiering, avlägsnande eller förstörelse av information som lagras på media. Rutinen ska också beskriva hur media avvecklas på ett säkert sätt.

Styrning av åtkomst

Hantering av användares åtkomst

Åtkomst till information och informationssystem ska styras utifrån verksamhetens behov och säkerhetskrav. Den som har behov av tillgång till viss information för att kunna utföra sina uppdrag ska tilldelas åtkomsträttigheter. All åtkomst ska vara behovsbaserad utifrån ansvars- och arbetsområde.

Det ska finnas formella processer för registrering, avregistrering av användare samt tilldelning av åtkomsträttigheter till alla informationssystem och tjänster. Alla användare ska ha en individuell användaridentitet som ska vara unik över tid. Tilldelning av konfidentiell autentiseringsinformation, som till exempel lösenord eller PIN-koder, ska styras genom en formell hanteringsprocess.

Tilldelning av priviligierade åtkomsträttigheter ska begränsas och styras så att de bara omfattar de uppdrag som användaren har utbildning, ansvar och befogenheter att utföra. Priviligierade åtkomsträttigheter ska tilldelas med användning av annan användaridentitet (it-konto) än den som utnyttjas i den normala verksamheten.

Ägare av informationstillgångar ska minst årligen granska användarnas åtkomsträttigheter.

Användaransvar

Användare ska informeras om deras ansvar för att skydda autentiseringsinformation som till exempel lösenord, PIN-koder mm.

Styrning av åtkomst

Tillgång till information och systemfunktioner ska tillåtas i enlighet med ägarens krav på styrning av åtkomst. Dessa krav ska utgå ifrån regulatoriska krav, informationsklassning och risk.

Fysisk och miljörelaterad säkerhet

Nivån på det fysiska skyddet ska stå i proportion till värdet av tillgångarna och resultatet av informationsklassificeringen och de återkommande riskanalyserna som genomförs som en del av objektsförvaltningen. Värdet på informationen är konstant oavsett om informationen befinner sig i vila eller är under transport.

Säkra utrymmen

Fysiska avgränsningar ska användas för att skydda utrymmen som innehåller skyddsvärd information.

Säkra utrymmen ska skyddas genom lämpliga säkerhetsåtgärder för att säkerställa att endast behörig personal får tillträde. Samma krav gäller information som finns hos extern part.

Utrustning

Utrustning ska placeras och skyddas för att minska riskerna för miljörelaterade hot och faror samt möjligheter för obehörig åtkomst.

Driftsäkerhet

Driftsrutiner och ansvar

Driftsrutiner ska dokumenteras och göras tillgängliga för alla som behöver dem. Förändringar som påverkar informationssäkerheten ska hanteras på ett strukturerat sätt.

Konsumtion och av resurser ska övervakas samt analyseras så att nödvändig systemprestanda kan garanteras.

Skydd mot skadlig kod

Upptäckande, förebyggande och återställande säkerhetsåtgärder för att skydda mot skadlig kod ska finnas i kombination med att skapa medvetenhet hos medarbetare om risker med skadlig kod.

Säkerhetskopiering

Informationens och it-miljöns krav på konfidentialitet, riktighet och tillgänglighet ska bevaras genom väl utvecklade rutiner för säkerhetskopiering och återläsning och anpassas till verksamheternas krav på kontinuitet.

Loggning och övervakning

Kritiska och säkerhetsrelevanta händelser ska vara spårbara genom automatiska loggningsfunktioner som skyddas mot manipulation och obehörig åtkomst.

Tid

Tidskällan ska vara spårbar till den svenska nationella tidsskalan UTC(SP).

Styrning av driftsystem
Det ska finnas en rutin för att styra installation av driftsystem. Innan installation ska riskanalys ha genomförts och säkerhetskraven fastställts.

Hantering av tekniska sårbarheter
Genomsökning och analys av tekniska sårbarheter i Region Gotlands it-miljö ska ske löpande.

Sårbarheter ska analyseras och lämpliga åtgärder för att åtgärda sårbarheter eller minska riskerna ska genomföras. Motsvarande gäller även vid avtalsmässigt inköp av it-tjänster av extern part.

Överväganden gällande revision av informationssystem
Revisionsaktiviteter som omfattar verifiering av status på driftsystem ska planeras noggrant för att minimera störningar.

Kommunikationssäkerhet

Hantering av nätverkssäkerhet
Nätverk ska hanteras och styras för att skydda information i informationssystemen. Informationens värde styr säkerhetsmekanismer, tjänstenivåer och ledningskrav.

Avtal och överenskommelser reglerar närverkssäkerhetens utformning och tjänster oavsett om dessa tjänster tillhandahålls i egen eller annans regi.

Informationsöverföring
Formella rutiner och säkerhetsåtgärder ska vara införda för att skydda överföring av information oavsett metod. Säker överföring av verksamhetsinformation mellan organisationer och externa parter ska vara reglerad genom överenskommelser.

Kryptografiska säkerhetsåtgärder
Det ska finnas rutiner som beskriver när kryptologiska säkerhetsåtgärder ska användas för skydd av information. Dessa rutiner ska också beskriva de nivåer som ska användas beroende på informationens värde, risk samt giltighetstid för kryptologiska nycklar för hela deras livscykel.

Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras inom Region Gotlands förvaltningar och bolag ska detta ske enligt anvisning från säkerhetsskyddschef.

Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem som finns utom Region Gotlands kontroll ska uppgifterna skyddas med hjälp av kryptografiska funktioner som godkänts av Försvarsmakten.

Anskaffning, utveckling och underhåll av system

Säkerhetskrav på informationssystem

Krav som rör informationssäkerhet ska inkluderas i kraven för nya informationssystem eller förändringar av befintliga informationssystem. En riskanalys ska alltid föregå nyanskaffning och större förändringar. Detta gäller oavsett om informationssystemet eller tillämpningen levereras intern eller externt som någon form av molntjänst. För mer information och upphandling och införande se Region Gotlands införandeprocess och objektförvaltningsmodell.

Vid anskaffning ska gallring och arkivering vägas in och beaktas särskilt för att stötta informationens hela livscykel. Plan för avveckling ska finnas redan vid anskaffning av ett system. För mera information, läs Region Gotlands arkivreglemente med tillhörande informationshanteringsplan

Säkerhet i utvecklings- och supportprocesser

Det ska finnas rutiner som tillämpas vid systemutveckling inom organisationen. Systemförändringar inom utvecklingscykel ska styras genom användning av formella rutiner för ändringshantering. När driftmiljön ändras ska verksamhetskritiska tillämpningar granskas och testas för att säkerställa att det inte innebär negativ påverkan på verksamheten eller säkerheten.

För alla test- och utvecklingsmiljöer i Region Gotlands it-miljö ska det finnas utpekat ansvar. Dessa informationssystem ska på lämpligt sätt skyddas och säkras över hela livscykeln. Testdata bör vara anonymiserat.

Program för acceptanstester och relaterade kriterier ska fastställas för nya informationssystem, uppgraderingar och nya versioner.

Leverantörsrelationer

Informationssäkerhet i leverantörsrelationer

Region Gotland är alltid informationsägare av sin information. Vid behov kan skyddsvärd information behöva lämnas ut för att leverantör ska kunna fullgöra sina åtagande. Med leverantör avses alla fysiska och juridiska personer som Region Gotland har en affärsrelation med.

Avtal ska upprättas med varje leverantör som kan tillgå, behandla, lagra och kommunicera information eller som tillhandahåller infrastrukturkomponenter för organisationens information.

Avtal med leverantör ska innehålla krav på att hantera informationssäkerhetsrisker som är relaterade till försörjningskedjan för tjänster och produkter baserade på informations- och kommunikationsteknologi.

Informationssäkerhetskrav för att reducera riskerna förknippade med leverantörers åtkomst till organisationens tillgångar ska avtalas med leverantören och dokumenteras.

Personalsäkerheten för konsulter/entreprenörer ska regleras i enlighet med avsnittet för personalsäkerhet i denna riktlinje.

För behandling av personuppgifter ska det finnas ett personuppgiftsbiträdesavtal tecknat.

Om en leverantör kan få tillgång till säkerhetsskyddsklassificerade handlingar i klassen konfidentiell eller högre eller annan säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet ska ett säkerhetsskyddsavtal ingås. Innan ett förfarande som kräver säkerhetsskyddsavtal påbörjas ska en särskild säkerhetskyddsbedömning och en lämplighetsprövning genomföras. Säkerhetskyddsbedömningen och lämplighetsprövningen ska
dokumenteras.

Hantering av leverantörers tjänsteleverans

Region Gotland ska regelbundet övervaka, granska och genomföra revision av sina leverantörers tjänsteleveranser.

Hantering av informationssäkerhetsincidenter

Hantering av informationssäkerhetsincidenter och förbättringar

Incidenter, säkerhetshotande händelser och säkerhetsmässiga svagheter ska, utan dröjsmål, rapporteras och korrigerande åtgärder ska vidtas.

- Informationssäkerhetsincidenter, säkerhetsskyddsrelaterade incidenter, NIS-incidenter samt personuppgiftsincidenter ska ses som en del i ett ständigt lärande oavsett om de rapporteras till tillsynsmyndighet eller ej.
- Region Gotland ska ha ett system för rapportering av incidenter.
- Region Gotland ska ha en etablerad kontakt med Sveriges nationella Computer Security Incident Respons Team (CSIRT).

Respektive verksamhetsutövares säkerhetsskyddschef ska kontinuerligt informera Regionstyrelseförvaltningens säkerhetsskyddschef om händelser av vikt.

Informationssäkerhetsaspekter avseende hantering av verksamhets kontinuitet

Kontinuitet för informationssäkerhet

Kontinuiteten för informationssäkerheten ska planeras, implementeras och revideras som en integrerad del av hela organisationens system för kontinuitetshantering.

Efterlevnad

Vid oklarheter beträffande tillämpningen av detta regelverk ska varje anställd kontakta sin chef, informationssäkerhetschef eller i förekommande fall säkerhetsskyddschef. Vid överträdelse av regelverk för informationssäkerhet kommer detta att behandlas i enlighet med regionens personalpolicy.

Juridiska och affärsmässiga krav

Varje verksamhet lyder under en rad olika lagar och varje verksamhet behöver själva ha insikt i hur de berör den egna verksamheten t ex

- 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).

Granskning av informationssäkerhet

Region Gotlands tillvägagångssätt för att arbeta med och hantera informationssäkerhet ska med jämna mellanrum eller när betydande förändringar sker genomgå oberoende granskning. Respektive verksamhetsutövare ansvarar för att kontinuerligt identifiera brister och sårbarheter och genomföra förbättringar. Ansvaret omfattar även att regelbundet kontrollera och följa upp att den eventuellt säkerhetskänsliga verksamheten följer regelverket samt att utvärdera om skyddsåtgärderna ger avsedd effekt.

Säkerhetsskyddschefen ansvarar för att regelbundet följa upp och utvärdera säkerhetsskyddet i Region Gotland.