GISLAVEDS KOMMUN

Styrdokument
Dokumenttyp: Riktlinjer
Beslutat av: Kommunstyrelsen
Fastställelsedatum inkl. dnr: 2026-01-14 §7, KS.2025.211
Gäller för: Kommunala förvaltningar
Ansvarig: (chef): Avdelningschef för verksamhetsstyrning och it
Revideras: Vid behov eller vart fjärde år
Följs upp: (enhet) Enheten för säkerhet, kunskap och analys

Riktlinjer för informations- och cybersäkerhet

2025-11-26

Innehållsförteckning

1 Inledning

Den här riktlinjen syftar till att konkretisera policy för informations- och cybersäkerhet samt ge vägledning i hur policyn ska tillämpas.

Riktlinjen gäller för all verksamhet inom kommunen och omfattar alla informationstillgångar som hanteras. Alla anställda, förtroendevalda och extern personal som hanterar information inklusive personuppgifter inom Gislaveds kommuns verksamheter omfattas av riktlinjen. Vissa funktioner har dock mer specifika uppgifter inom ramen för information- och cybersäkerhet vilket anges i riktlinjen.

Information- och cybersäkerhet är en del i kommunens lednings- och kvalitetsarbete och är en viktig del för att nå målen om en effektiv administration och förvaltning. Kommunen tar ansvar för sina informationstillgångar genom att arbeta strukturerat med informationssäkerhet i den egna verksamheten och ställa krav på upphandlade leverantörer.

Förutom policyn och riktlinjen finns även mer detaljerade rutiner, regler och metodstöd kring hur verksamheterna i Gislaveds kommun ska arbeta med informationssäkerhet. Nämnder och bolag kan ha behov av att ta fram egna styrdokument för sin specifika verksamhet.

2 Syfte

Syftet med Gislaveds kommun riktlinje för informationssäkerhet är att skapa förutsättningar för ett systematiskt och långsiktigt informationssäkerhetsarbete.

Riktlinjen omfattar alla informationstillgångar oavsett om de behandlas manuellt eller digitalt och oberoende av i vilken form eller miljö de förekommer.

Säkerhetsskyddsklassificerad information med betydelse för Sveriges säkerhet hanteras utanför denna riktlinje och regleras i Gislaveds kommun riktlinje för säkerhetsskydd.

3 Att arbeta systematiskt

Av Gislaveds kommun policy för informationssäkerhet framgår att det ska bedrivas ett systematiskt arbete med informationssäkerhet samt ett förebyggande arbete mot oönskade händelser.

Att arbeta systematiskt med informationssäkerhet innebär att arbeta förebyggande och att kontinuerligt anpassa skyddet för information utifrån organisationens behov och risker. Då finns även rätt information tillgänglig för rätt person vid rätt tidpunkt. Informationstillgångar behöver skyddas

utifrån sitt skyddsvärde och information ska inte hamna i orätta händer och missbrukas.

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Exempel på information kan vara i form av text, ljud, bilder eller film, och kan hanteras med stöd av it-utrustning, papper eller direkt av oss människor i form av tal.

Att information är korrekt som kommunen hanterar i relationer med kommuninvånare, företag och organisationer såväl som inom Gislaveds kommun utgör en grund för tillit och förtroende. Perspektivet med informationssäkerhet är en naturlig del vid utformning av våra arbetssätt och en del av vårt dagliga arbete.

3.1 Systematiskt informationssäkerhetsarbete

Metodstödet för Gislaveds kommun informationssäkerhetsarbete utgår från den etablerade standarden ISO 27000 serien som Myndigheten för civilt försvar rekommenderar. För att säkerställa att informationssäkerhetsarbetet har tillräcklig nivå i Gislaveds kommun är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt. Nedanstående fyra områden är viktiga för ett framgångsrikt och hållbart informationssäkerhetsarbete.

3.1.1 Identifiera och analysera

För att det systematiska informationssäkerhetsarbetet ska fungera måste informationssäkerhetsarbetet anpassas till kommunens olika verksamheter utifrån deras specifika krav.

Resultatet från analyserna ska styra hur informationssäkerhetsarbetet ska utformas och bedrivas samt vilka säkerhetsåtgärder som behöver införas för respektive verksamhet.

3.1.2 Utforma

Utformningen av kommunens och verksamheternas mål, organisation, riskanalys, handlingsplan och klassningsmodell är viktigt för det långsiktiga arbetet med informationssäkerhet för hela kommunen. Mål, handlingsplan och riskanalysen kan underlätta informationssäkerhetsarbetet utifrån analysernas resultat.

Informationsklassning

Kommunens informationstillgångar behöver inventeras, värderas och klassificeras för att få rätt skydd. Klassningsmodellens roll är att skapa en kommunövergripande ram så klassning och skyddsnivåerna sker på ett likvärdigt sätt på informationstillgångarna.

Genom att klassa informationstillgångarna utifrån säkerhetsaspekterna kan skyddet anpassas och säkerställas för varje informationstillgång utifrån informationssäkerhet. Informationsklassningen syftar till att ge kommunens kritiska informationstillgångar tillräckligt skydd för att undvika överskydd och onödiga kostnader.

Kommunens samtliga informationstillgångar ska finnas förtecknade i det systemstöd som också ger en grund för klassificering, värdering och åtgärdsplan utifrån informationssäkerhet.

Kommunen använder klassningsmodell från Sveriges Kommuner och Regioner (SKR) som bygger på den internationella standarden ISO 27000 som också Myndigheten för civilt försvar använder. Genom att följa internationella och nationella riktlinjer underlättar kommunen för externa aktörer att värdera informationstillgångarna likvärdigt ur säkerhetsperspektiven tillgänglighet, riktighet och konfidentialitet.

Klassificering av information

Klassificering av information är en grundläggande aktivitet som görs för att kunna identifiera och rekommendera det nödvändigt skydd för informationstillgångar och resurser. Det är informationen som är skyddsobjektet, dvs. det som ska skyddas. Dock kan överklassificering medföra onödiga åtgärder med ytterligare kostnader till följd.

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

Vid klassificering av information ska det bedömas vilken negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ får inom följande fyra kravområden

- Konfidentialitet - innebär informationen kan åtkomst begränsas (benämndes tidigare för sekretess men standarden har ändrats för att inte förväxla begreppet med sekretess i juridisk mening)
- Riktighet - innebär informationen ska vara tillförlitlig, korrekt och fullständig
- Tillgänglighet - innebär informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.

3.1.3 Använda

Det systematiska informations- och cybersäkerhetsarbetet ska fungera i det vardagliga arbetet, vilket förutsätter att aktiviteter från handlingsplan och mål efterlevs enligt uppdrag, roller och ansvar. Medarbetare och förtroendevalda utbildas och hanterar informationstillgångarna efter kommunens rutiner som kopplas till riktlinjen för informations- och cybersäkerhet.

3.1.4 Följa upp och förbättra

Krav på informationshantering ändras konstant genom teknisk utveckling, förändrade hotbilder och organisationsförändringar. För att det systematiska informations- och cybersäkerheten ska utvecklas och nå framgång behöver arbetet följas upp och rapporteras.

Informationssäkerhetssamordnare ska rapportera arbetet med informationssäkerhet till kommunstyrelsen och kommunledningsgruppen.

4 Organisation, ansvar och roller

Organisationen utgör den arbetsstruktur som gäller i Gislaveds kommun. Syftet är att skapa ett effektivt och strukturerat informationssäkerhetsarbete, både övergripande och på verksamhetsnivå.

Kommunens strategiska arbete med informations- och cybersäkerhet omfattar planering, prioritering, målformulering och uppföljning av säkerhetsarbetet. Detta arbete utförs i samverkan mellan relevanta funktioner inom avdelningen för verksamhetsstyrning och it, och andra kompetenser kan involveras vid behov. På avdelningen finns kommunens informationssäkerhetssamordnare. Avdelningen ger stöd till förvaltningarnas operativa arbete.

Det operativa informationssäkerhetsarbetet genomförs i förvaltningarna. Fokus ligger på genomförande av informationsklassning, riskanalyser, uppföljning, incidenthantering och andra praktiska moment som rör informationssäkerhet.

4.1 Organisation för informationssäkerhet

Kommunstyrelsen fastställer riktlinjen för informationssäkerhet och dataskydd. I sin ledningsfunktion ingår att kommunstyrelsen ska ha uppsikt över övriga nämnders verksamhet (uppsiktsplikten). Kommunstyrelsen är arkivmyndighet och ska som sådan utöva tillsyn beträffande arkivbildning samt arkivvården i kommunen.

Respektive nämnd är ansvarig för den information det vill säga informationsägare och är därmed riskägare. Nämnden är personuppgiftsansvarig för de personuppgifter som hanteras i dess verksamhet. Nämnden ska kunna rapportera status kring sin hantering av information till kommunstyrelsen. Nämnden ska enligt 6 kap. 6 § kommunallagen (2017:725) se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten.

Kommundirektör ansvarar för att informations- och cybersäkerhetsarbetet bedrivs enligt styrdokumenten och beslutar om de övergripande rutinerna som rör informations- och cybersäkerhet.

Förvaltningschefer är ansvariga för informationssäkerheten inom respektive verksamhet. Förvaltningschefen ska säkerställa att förvaltningens informationssäkerhetsarbete bedrivs enligt gällande policy och riktlinjer samt avsätta tillräckliga resurser för att nå en tillräcklig nivå av informationssäkerhet. Förvaltningschefen ska även kunna rapportera status på arbetet till berörd nämnd, kommundirektören, informationssäkerhetssamordnare i Gislaveds kommun. Det är förvaltningschefen ytterst som tillsätter resurser som ska läggas på informationssäkerhet.

Dataskyddsombud (DSO) ansvarar för att granska efterlevnaden av dataskyddsförordningen i Gislaveds kommun nämnder. Dataskyddsombudet ansvara för att rapportera brister och förbättringsåtgärder till varje respektive nämnd.

Kommunstyrelseförvaltningen - Avdelningen för verksamhetsstyrning och it har det övergripande ansvaret för att samordna och leda kommunens arbete med informationssäkerhet. Ansvarsområdet omfattar både administrativ och teknisk informationssäkerhet, inklusive dataskydd, it-säkerhet och cybersäkerhet. Avdelningen ger stöd och hjälp till nämnderna genom att initiera utbildningar, gemensamma processer och rutiner, genomför revisioner inom informations- och cybersäkerhet och rapporterar till kommunstyrelsen.

Tjänsteägare är den person som har det övergripande ansvaret för ett it-system. It-systemet hanterar alltid en eller flera informationsmängder. Tjänsteägare ansvarar för leverans av ett system eller tjänst samt säkerställer att det finns ekonomiska och personella resurser. Tjänsteägare tillsammans med informationsägare ställer krav på tjänsteleverantörer och driftoperatörer.

Tjänsteförvaltare förvaltar systemet på uppdrag av tjänsteägare, det vill säga inom givna ekonomiska ramar och fastställd förvaltningsplan. Tjänsteförvaltare har det funktionella ansvaret för systemet. För större system kan en tjänsteförvaltare ha hjälp av en it-säkerhetsansvarig.

Medarbetare och förtroendevalda hanterar kommunens informationstillgångar och har ett ansvar att följa kommunens policy för informationssäkerhet och underliggande styrdokument. De har också ansvar för att uppmärksamma fel och brister i informationshantering, utrustning och informationsinnehåll samt för att rapportera brister och incidenter i enlighet med fastställda rutiner.

5 Utbildning av medarbetare och förtroendevalda

Utbildning och kunskapsbehoven för varje målgrupp finns beskrivet i handlingsplanen som upprättas och justeras årligen. Årlig utbildning för medarbetare och för nyanställda inom kommunen beskriv mer detaljerat i utbildningsplanen för informations- och cybersäkerhet.

6 Incidentrapportering

En informationssäkerhetsincident innebär en händelse som kan eller har påverkat konfidentialitet, riktighet eller tillgänglighet av information. Alla som använder information inom organisationen måste rapportera säkerhetsbrister och incidenter. Exempel på sådana händelser kan vara obehörig åtkomst till lokaler, läckage av information, försvunnen information, delade lösenord eller skadlig kod i it-miljön. Informationssäkerhetsincidenter omfattar både tekniska och administrativa aspekter.

Informationssäkerhetssamordnare ansvarar för att rutiner finns för att upptäcka, analysera och rapportera säkerhetsincidenter. Rutinerna bör inkludera rapporteringsskyldighet, rapporteringsmetod, innehåll och mottagare. Lärdomar från incidenter bör användas för att förbättra säkerheten, exempelvis genom att investera i nya lösningar eller införa nya rutiner och kontroller.

Anmälan av informationssäkerhetsincidenter följer samma process som för it-säkerhetsincidenter. Processen omfattar mottagning, styrning, analys, återkoppling och vidarebefordran till ansvariga och berörda personer.

Vissa incidenter kräver snabb rapportering till tillsynsmyndigheter, så en bedömning av incidenten bör påbörjas omedelbart. Exempel på sådana incidenter är personuppgiftsincidenter enligt dataskyddsförordningen och incidenter som rör säkerheten i nätverk och informationssystem inom samhällsviktiga tjänster enligt NIS2-direktivet.

För personuppgiftsincidenter finns särskilda rutiner och stödmaterial för att bedöma om incidenten ska rapporteras till tillsynsmyndigheten. Den utsedda kontaktpersonen inom respektive verksamhet leder arbetet med incidentrapportering och tar vid behov kontakt med olika stödfunktioner enligt rutinen.

7 Kontinuitetsplanering

Kontinuitetsplaner ska upprättas och införas för de kritiska verksamhetsprocesserna för att säkerställa att identifierade viktiga funktioner kan återställas inom rimlig tid och att verksamheten har manuella rutiner för tiden under återuppbyggnadsarbetet.

Kontinuitetsplanen ska baseras på analys att konsekvenserna av störningar, allvarliga händelser, och extraordinära händelser med hänsyn till dess inverkan på verksamheten.

7.1 Efterlevnad och uppföljning

Chefer ska säkerställa att alla säkerhetsrutiner inom deras respektive ansvarsområden utförs korrekt för att upprätthålla informationens konfidentialitet, riktighet och tillgänglighet.

Vitala system och vitala delar i it-miljö, nätverk och tillhörande infrastruktur ska regelbundet kontrolleras att informationens konfidentialitet, riktighet och tillgänglighet upprätthålls.

Extern revision ska utföras på ett sådant sätt att informationens konfidentialitet, riktighet och tillgänglighet inte påverkas.

Kommunstyrelsen ska årligen få uppföljning som omfattar

- hantering av identifierade risker och status på vidtagna åtgärder,
- inträffade incidenter,
- planerade och genomförda utbildningar,
- interna kontroller, revisioner och förbättringsåtgärder,
- uppföljning av krav på leverantörer och andra externa parter som hanterar kommunens information eller it-tjänster,
- hotbild, beroenden och sårbarheter som påverkar kommunens informations- och cybersäkerhet.

Denna riktlinje ska följas upp i samband med den återkommande övergripande risk- och sårbarhetsanalysen.

8 Leverantörsrelationer

Gislaveds kommun är alltid informationsägare av sin information. Vid behov kan skyddsvärd information behöva lämnas ut för att leverantör ska kunna fullgöra sina åtaganden. Med leverantör avses alla fysiska och juridiska personer som Gislaveds kommun 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.