Styrdokument
Dokumenttyp: Program
Beslutat av: Kommunstyrelsen
Fastställelsedatum: 2021-11-24
Ansvarig: Informationssäkerhetssamordnare
Revideras: Vart 4:e år eller vid behov
Följas upp: Vartannat år

Handlingsprogram för informationssäkerhet

Dnr: 2021.156
2021-10-18

Innehållsförteckning

1 Bakgrund

Vi klarar idag i princip ingen verksamhet utan tillgång till våra informationsresurser. Störningar i våra mest kritiska system kan leda till allvarliga kriser och drabba enskilda och deras hälsa, innebära försenade utbetalningar och påverka förtroendet för förvaltning och service.

Information kan förekomma i många olika former. Oftast är den lagrad elektroniskt men information kan också finnas tryckt eller enbart nedskriven och yttras i en konversation. Oavsett form så omfattas detta program av samtliga informationstillgångar oberoende om den behandlas manuellt eller med informationsteknologi.

Informationssäkerhet 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. Detta program tydliggör kommunens övergripande principer och förhållningssätt för arbetet med informationssäkerhet.

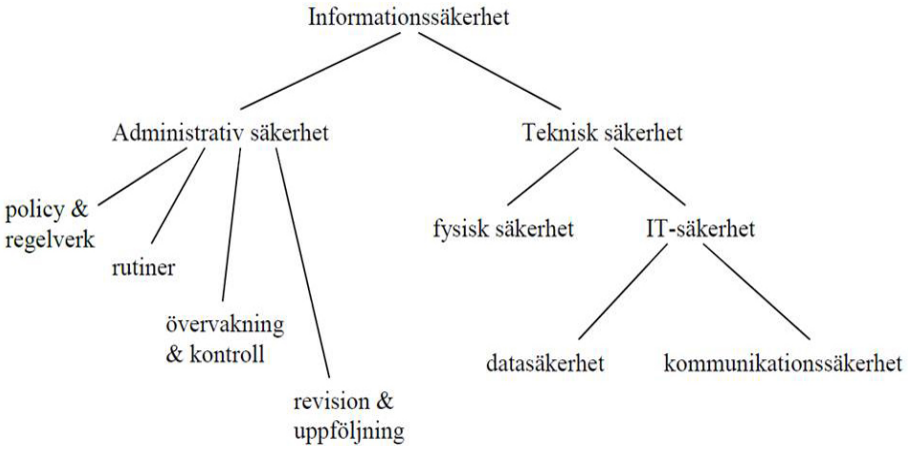
2 Informationssäkerhet

Informationssäkerheten omfattar kommunens alla informationstillgångar. Informationssäkerhet är ett samling begrepp för all säkerhet som har anknytning till hur information hanteras. Begreppet omfattar inte enbart information som bearbetas eller hanteras i IT-system utan alla förekommande former av information till exempel kunskap, kompetens, rutiner, dataöverföring oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i.

Informationssäkerhet, säkerhet vid hantering av information för önskad

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

- *Spårbarhet* - innebär att specifika aktiviteter som rör informationen kan spåras



2.1 Administrativ säkerhet

Administrativ säkerhet uppnås framför allt med hjälp av administrativa regler och rutiner. Administrativ säkerhet definieras i:

- *Policy och regelverk* – eller andra typer av styrdokument som beskriver vad som ska finnas och talar om vad man vill uppnå
- *Rutiner* – eller annat dokument som beskriver hur något ska göras och ansvarig för genomförandet
- *Övervakning och kontroll* - för att fortlöpande säkra informationen
- *Revision och uppföljning* – för att kontrollera hur informationen och arbetet med den hanteras

2.2 Teknisk säkerhet

Fysisk säkerhet

Fysisk säkerhet är skydd av data, system, kommunikationsvägar och tillhörande utrustning. Det fysiska skyddet ska samordnas med de skydd som krävs för datasäkerhet och kommunikationssäkerhet.

IT-säkerhet

IT-säkerhet indelas i:

- ***Datasäkerhet*** – skydd av data och system mot obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling.
- ***Kommunikationssäkerhet*** – implementera och upprätthålla säkerhetsåtgärder i syfte att förhindra eller försvåra avlyssning eller obehörig påverkan av information i kommunikationssystem.

2.3 Hantering av tillgångar

Samtliga informationstillgångar ska vara identifierade och förtecknade i informationshanteringsplaner och det ska framgå vem som är tjänsteägare och tjänsteförvaltare.

Alla verksamheter och system är utsatta för risker. Risk- och sårbarhetsanalyser ska identifiera tänkbara störningar, allvarliga händelser samt extraordinära händelser. Arbetet syftar till att skapa robusta system samt identifiera och analysera skyddsvärda informationstillgångar. Arbetet ska fokusera på förebyggande insatser och konkreta skyddsåtgärder för människor, egendom och miljö.

2.4 Klassificering av information

Klassificering av information är en grundläggande aktivitet som bör göras för att kunna identifiera och rekommendera de nödvändiga skydden för informationstillgångar och resurser. Det är informationen som är skyddsobjektet, det vill säga det som ska skyddas. Dock kan överklassificering medföra onödiga åtgärder med ytterligare kostnader som 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 etcetera.

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, tillgänglighet*, *riktighet* och *spårbarhet.* Vid bedömningen används de fyra konsekvensnivåer: *Allvarlig, Betydande, Måttlig* och *Försumbar*. Mer information kring konsekvensnivåerna finns i *riktlinjer för klassificering av information*.

3 Roller och ansvar

Detta kapitel beskriver de centrala rollerna i informationssäkerhetsarbetet inom kommunen. Men alla som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls samt att rapportera incidenter.

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhetsarbete och fastställer *Program för informationssäkerhet.* Kommunstyrelsen ska även se till att nämnderna ges vägledning genom att

styra arbetet via informationssäkerhetssamordnaren, samt att avsätta medel för arbetet.

Kommundirektör har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet i kommunen.

Den centrala **informationssäkerhetssamordnaren** är direkt underställd kommundirektören och har det operativa ansvaret för samordning av informationssäkerhetsarbetet. Samordnaren ska se till att programmet efterlevs och ge stöd och hjälp till nämnderna genom att initiera utbildningar, rutiner samt övriga aktiviteter.

Dataskyddsombudet är en tillsynsfunktion som granskar tillämpningen av regelverk, instruktioner och avtal men är också en stödfunktion med uppgift att sprida kunskap och information. Dataskyddombudet ser till att personuppgifter behandlas enligt gällande lagstiftning och påpekar eventuell brister till kommunstyrelsen samt vid behov direkt till Integritetsskyddsmyndigheten (IMY).

Mer information kring organisation och ansvar finns i *IT-regler Förvaltning Bas.*

4 Tillämpning

Varje behandling av personuppgifter ska ske med hänsyn till den enskildes personliga integritet och rättigheter.

För att uppfylla målsättningen med Gislaveds kommuns informationssäkerhet och för att kunna styra och leda arbetet med informationssäkerhet, har kommunen valt att införa ett systematiskt informationssäkerhetsarbete. Arbetet ska följa Myndigheten för Samhällsskydd och Beredskaps (MSB) rekommendationer för kommuners informationssäkerhet samt kraven i informationssäkerhetsstandarden ISO/IEC 27001.

4.1 Personalresurser och säkerhet

Alla anställda, uppdragstagare och utomstående användare ska förstå sitt ansvar. Det ska säkerställas att dessa är lämpliga för de roller de anses ha i syfte att minska risken för stöld, bedrägeri eller missbruk av resurser. Det ska också säkerställas att de är medvetna om hot och problem som rör informationssäkerhet samt är rustade för att följa kommunens regelverk för informationssäkerhet när de utför sitt normala arbete och för att minska risken för mänskliga fel.

När anställda, uppdragstagare och utomstående användare lämnar kommunen eller ändrar anställningsförhållande ska det ske på strukturerade och säkert sätt.

4.2 Fysisk och miljörelateradsäkerhet

Nivån på det fysiska skyddet ska stå i proportion till resultatet av informationsklassificeringen och de återkommande riskanalyserna.

Utrustning ska skyddas mot förlust, skada, stöld eller skadlig påverkan på tillgångar och avbrott i kommunens verksamhet

4.3 Kommunikation och drift

Kommunen ska ha en korrekt och säker drift av all IT-miljö, nätverk och tillhörande infrastruktur så att informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet upprätthålls.

Risken för systemfel ska minimeras och systemintegriteten för programvara och riktighet i information ska säkerställas genom tydliga förvaltningsmodeller och adekvata tekniska skydd mot exempelvis skadlig kod.

Informationens och IT-miljöns riktighet respektive systemintegritet och tillgänglighet ska bevaras genom väl utvecklade rutiner för säkerhetskopiering och återläsning.

De ska finnas tydliga rutiner som hindrar att information på flyttbart och avvecklat media avslöjas.

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

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

Alla administratörer ska ha individuella användaridentiteter. Användare ska hantera sina inloggningsuppgifter på ett sätt så att obehörig åtkomst undviks.

4.4 Anskaffning, utveckling, underhåll och avveckling av system

Alla system inom kommunen ska ha tillräckliga skydd så att informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet upprätthålls. Systemen ska utformas så att fel, obehörig förändring eller missbruk förhindras genom exempelvis validering av in-och utdata och andra adekvata kontroller.

Risker med publicerade sårbarheter ska hanteras.

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. Krav på gallring och arkivering ska beaktas vid avveckling. Uppgifter som gallras ska förstöras på ett sådant sätt att uppgifterna inte kan återskapas eller komma i orätta händer.

5 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 av konsekvenserna av störningar, allvarliga händelser, och extraordinära händelser med hänsyn till dess inverkan på verksamheten.

5.1 Efterlevnad och uppföljning

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

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

Informationssäkerhetsarbetet ska kontinuerligt följas upp och utvärderas enligt beslutade rutiner. Detta program ska följas upp i samband med den återkommande övergripande risk-och sårbarhetsanalysen. I övrigt tar kommunstyrelsen initiativ till revidering av programmet.