Vimmerby kommun

Informationssäkerhetspolicy

Vimmerby kommun

Ärendenummer 2022/453
Dokumentansvarig Kommunstyrelsen
Beslutad av Kommunstyrelsen
Datum för beslut 20
Börjar gälla 2023-09-19

Innehåll

Om Informationssäkerhetspolicy

Informationssäkerhetspolicyn är ett dokument som redovisar Vimmerby kommuns övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat.

Denna policy gäller för informationssäkerhet inom Vimmerby kommun och bör kompletteras med riktlinjer och övriga styrdokument i respektive verksamhet.

Om informationssäkerhet

Information finns i alla kommunens verksamheter och handlar om allt vi gör och allt vi säger, exempelvis om vår personal, våra tjänster, vår ekonomi och det omgivande samhället med invånare, företag, föreningar med flera. Information är därför i sig en av kommunens viktigaste tillgångar.

För att nå hög kvalitet i vårt arbete måste information hanteras på rätt sätt. Det innebär att information finns tillgänglig när den behövs, att den är korrekt och att obehöriga inte får åtkomst till den. Avbrott i tillgången till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån tre aspekter:

- Konfidentialitet: att information inte tillgängliggörs eller avslöjas till obehörig.
- Riktighet: att information är korrekt, aktuell och fullständig.
- Tillgänglighet: att information är åtkomlig och användbar av behörig.

Information har i olika grad krav på sig gällande de tre aspekterna. Kraven på hantering av information styrs av lagar och förordningar, eller av organisationens egna målsättningar. Dessutom har självklart medborgare, företag och andra aktörer i vår omvärld behov och förväntningar som ställer krav på vår informationssäkerhet.

Informationssäkerhet begränsas inte till säkerhet i IT-system, utan omfattar information i alla dess former och oavsett hur information lagras, bearbetas och kommuniceras. Information kan t. ex. vara i form av text, ljud, bilder och film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Mål med informationssäkerhet

Målet för Kommunalförbundet Itsams och Vimmerby kommuns informationssäkerhetsarbete är att hantera och skydda informationen på sådant sätt att rättsliga och verksamhetsmässiga krav uppnås, samt att medborgares förtroende upprätthålls. Detta skapar en robust, säker och tillförlitlig informationshantering i hela organisationen.

Skyddet ska vara anpassat till informationens skyddsvärde, risk och lagkrav och ska därigenom möjliggöra för kommunens verksamheter att uppnå sina mål. En god informationssäkerhet inom kommunen främjar verksamheternas funktionalitet, kvalitet och effektivitet. Dessutom främjas invånares rättigheter och personliga integritet, kommunens förmåga att förebygga och hantera allvarliga störningar och kriser, samt förtroendet för kommunens informationshantering och IT-system.

Principer och arbetssätt

Kommunalförbundet Itsam och Vimmerby kommun ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet ska gentemot kommunens verksamheter vara normerande, stödjande och kontrollerande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande kommunens informationstillgångar, samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Vimmerby kommun ska:

- vara systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS). Systematiken innebär kontinuerliga uppföljningar med reviderade handlingsplaner enligt metodiken planera, genomföra, följa upp och åtgärda.

- löpande ses över och förbättras, eftersom kommunen och dess omvärld, inklusive hotbild, är under ständig förändring.

- utifrån återkommande risk- och sårbarhetsanalyser och inträffade incidenter, vidta nödvändiga åtgärder för att säkerställa att vår information har rätt skydd. Skyddsåtgärder ska vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en otillräcklig säkerhet kan medföra.

- inbegripa säkerhetskrav inför upphandling, utveckling, användning och avveckling av informationstillgångar. Uppföljning av ställda krav ska ske kontinuerligt.

- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa. Våra kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av incidenter.

- utgå ifrån att alla informationstillgångar är identifierade och dokumenterade. Hantering av personuppgifter ska följa särskilda riktlinjer. All information ska sparas, alternativt gallras, enligt gällande lagstiftning och finnas dokumenterat.

- vara väl kommunicerat till verksamheten; all personal ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och för att kunna leva upp till denna policy.

Verksamhetsdriven informationssäkerhet genom informationsklassning

Verksamheterna har ansvar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras information är, och därmed kunskap om informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheterna, utifrån informationens skyddsvärde, ställer krav på de aktörer som hanterar informationen, exempelvis användare, systemansvariga samt drifts- och systemleverantörer.

För detta ändamål ska informationsklassning tillämpas, där information klassas med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Därigenom kan en anpassad och effektiv informationssäkerhet skapas.

Kommunalförbundet Itsam och Vimmerby kommun ska tillämpa en enhetlig modell för informationsklassning som anger olika nivåer av skyddskrav, vari information ska klassas baserat på interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Roller och ansvar

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Det gäller från kommunledning till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Kommunens informationssamordnare eller motsvarig och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhetsansvaret.

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvar och tillhörande uppgifter för respektive roller beskrivs utförligare i riktlinjer inom informationssäkerhetsområdet.

Ansvarig nämnd/ styrelse i Vimmerby kommun med bolag fastställer denna policy. Vid behov ska Kommunalförbundet Itsams direktion initiera revidering av policyn men minst en gång per mandatperiod.

Kommunstyrelsen ansvarar för samordning och uppföljning av informationssäkerhetsarbetet i kommunen.

Varje nämnd och bolagsstyrelse ansvarar för informationssäkerheten inom sitt verksamhetsområde och ska därför, inom ramen för sitt lokala ledningssystem och i enlighet med policy och riktlinjer, anta verksamhetsnära styrdokument för informationssäkerhet. Varje nämnd och bolagsstyrelse ansvarar för att planera och följa upp informationssäkerheten i verksamheten, och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla en robust, säker och tillförlitlig informationshantering.

Kommundirektör och Vd har kommunstyrelsens eller bolagsstyrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt i enlighet med denna policy och tillhörande riktlinjer. Kommundirektören ansvarar för att övergripande riktlinjer utarbetas och hålls aktuella i enlighet med policy. Vd ansvarar för att lokala riktlinjer vid behov utarbetas och hålls aktuella.

Verksamhetsansvariga, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Varje verksamhetsansvarig ansvarar för att egna medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en nödvändig informationssäkerhet i verksamheten kan uppnås.

Medarbetare och förtroendevalda har ett ansvar att följa kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Man har som medarbetare och förtroendevald också ansvar att vara uppmärksam på brister och fel gällande informationshantering, utrustning och informationsinnehåll, och rapportera sådana enligt fastställda rutiner.

Informationsägare är informationsansvarig för all data i, eller exporterat från, informationstillgången. I ansvaret ingår även att tillgången efterlever vid var tid gällande lagstiftning, samt informationssäkerhetspolicy och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om tillgångens informationssäkerhetsnivå genom att klassning sker enligt beslutad modell.

Systemägare har det övergripande ansvaret för ett it-system/lösning. Ansvaret inbegriper att riskanalyser genomförs och att krav på skydd säkerställs. Systemägare utser systemförvaltare.

Systemförvaltaren är den eller de personer i berörda verksamheter som aktivt förvaltar it-systemet på systemägarens uppdrag.

Kommunalförbundet Itsam ansvarar för att säkerheten i kommunens IT-miljö är tillförlitlig och motsvarar interna (verksamhetens) och externa (legala) krav. IT-miljön ska även uppfylla de krav som denna informationssäkerhetspolicy ställer.

Driftansvarig för informationstillgång innehar den tekniska kompetensen och ansvarar tillsammans med systemägare och systemförvaltare för att den dagliga driften upprätthålls enligt avtal. Kan vara Kommunalförbundet Itsam eller extern leverantör.

Informationssäkerhetsrådet är styrgruppen för informationssäkerhet för medlemskommunerna i Kommunalförbundet Itsam. Ska driva det övergripande och strategiska arbetet med att utveckla och samordna informationssäkerhetsarbetet i medlemskommunerna.