Riktlinjer för Informationssäkerhet

Bakgrund

Information är en av kommunens mest strategiska resurser och alla verksamheter är beroende av tillförlitlig information. Vi klarar idag i princip ingen verksamhet utan tillgång till våra informationsresurser och störningar i våra system kan leda till allvarliga kriser och drabba enskilda och deras hälsa. 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.

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.

Riktlinjerna för informationssäkerhet upprättas i enlighet med kommunens Trygghet- och säkerhetspolicy och är utformade från att följa lagkrav på informationssäkerhet från dataskyddsförordningen, lagen om informationssäkerhet för samhällsviktiga och digitala tjänster samt riktlinjer för hantering av personuppgifter i Marks kommun. Riktlinjerna för informationssäkerhet har också koppling till säkerhetsskydd, IT-säkerhet, krisberedskap och civilt försvar. Riktlinjerna är en del av kommunens interna regelverk som anger och tydliggör kommunens inriktningar och mål samt förhållningssätt för arbetet med informationssäkerhet under mandatperioden. Riktlinjerna ska fastställas av kommunstyrelsen under mandatperiodens första kalenderår. Revidering av dokumentet sker vid varje ny mandatperiods första kalenderår eller när behov uppstår.

Avgränsning

Riktlinjer för IT och IT-säkerhet omhändertar säkerhet i IT-system. Med detta avses data- och informationssystem, datanät, datorer och övrig datautrustning. Personuppgiftsansvar ligger under respektive nämnd i enlighet med det nämnds gemensamma reglementet i Marks kommun. Skyldigheterna som följer med personuppgiftsansvaret regleras i Riktlinjer för dataskydd.

Syfte

Det övergripande syftet är att säkerställa att Marks kommuns arbete med informationssäkerhet sker med en tydlig inriktning samt på ett välstrukturerat och informativt sätt, samt att beskriva och förtydliga olika aktörers roller och ansvar. Riktlinjerna behandlar även hur kommunen avser att uppfylla de lagkrav som ställs inom arbetet med informationssäkerhet.

Mål

Marks Kommun ska klara att skydda informationen inom kommunens verksamheter. Skyddet ska vara anpassat till skyddsvärde, risk och juridiska krav och på så sätt göra det möjligt för verksamheterna att sköta sina uppdrag och nå sina mål.

Informationssäkerhet innebär åtgärder av olika slag för att skydda information som är av betydelse för säkerhetskänslig verksamhet. Det vill säga skydda säkerhetsklassificerade uppgifter för att förebygga att uppgifterna röjs, ändras, görs otillgängliga eller förstörs samt förebygga skadlig inverkan på informationstillgångar som annars är av betydelse för säkerhetskänslig verksamhet. En stark informationssäkerhet ska bidra till verksamheternas funktionalitet, kvalitet och effektivitet samtidigt som den stärker medborgares rättigheter och personliga integritet. Informationssäkerheten ska dessutom kunna bidra till att förebygga och hantera allvarliga störningar och kriser.

Förutom kommunens egna mål utgår arbetet från internationella standarder, lagar, förordningar och föreskrifter, samt verksamhetens egna krav och ingångna avtal. Målet med informationssäkerhetsarbete är att bedriva ett långsiktigt och systematiskt informationssäkerhetsarbete genom att säkerställa våra informationstillgångars;

- **Konfidentialitet** - att information skyddas för obehörig insyn
- **Riktighet -** att information är tillförlitlig, korrekt och fullständig
- **Tillgänglighet** - att information är nåbar vid rätt tillfälle
- **Spårbarhet** - att specifika aktiviteter som rör information kan spåras

Hantering av information ska utgå från kontinuerliga riskanalyser för identifiering och värdering av risker och hot i verksamheten. Arbetet med informationssäkerhet ska vara långsiktigt och bedrivas systematiskt. Samtliga anställda ska inkluderas och medverka aktivt till att gällande säkerhetsregler och rutiner följs.
Som en del i det arbetet ingår att skapa och upprätthålla lämpligt skydd för all information som Marks kommun hanterar. Oavsett vilken form informationen har, eller hur den används, överförs eller lagras, måste den alltid ha ett godtagbart skydd.
Informationstillgångar avser all kommunens information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i.

Tillvägagångssätt
Arbetet ska bedrivas så att det blir en integrerad del av organisationens löpande verksamhet. Arbetet ska vara processorienterat och kontinuerligt utvärderas och anpassas till gällande omvärlds- och verksamhetskrav

För att uppnå kommunens övergripande mål ska informationssäkerhetsarbete bedrivas enligt ledningssystem för informationssäkerhet (LIS). Att arbeta enligt ett ledningssystem för informationssäkerhet innebär att arbeta systematiskt genom att upprätta, införa, driva, övervaka, granska, underhålla och ständigt förbättra organisationens informationssäkerhet.

Marks kommuns ledningssystem för informationssäkerhet ska bygga på den internationella SS-ISO/IEC 27000-standardserien och Myndigheten för samhällsskydd och beredskaps (MSB) tillhörande metodstöd för informationssäkerhet.

För kommunens informationssäkerhetsarbete ska följande gälla:

- Arbetet ska bygga på en helhetssyn och omfatta processer, människor och teknik.
- Att personal har tillräckliga kunskaper om informationssäkerhet i förhållande till sina arbetsuppgifter
- Det är säkerställt att det finns en förmåga att upprätthålla en säker informationshantering som är effektiv och bidrar till ökat skydd och stöd för medarbetare, tredje man och samarbetspartners.
- Vara förebyggande och proaktiv och kännetecknas av en god förmåga och organisation för att kunna hantera incidenter, allvarliga störningar och kriser.
- Ta tillvara möjligheterna i aktiv samverkan med det omgivande samhället, inbegripande myndigheter, företag och nätverk som kan vara ett stöd.
- Informationssäkerhetsarbetet ska ta sin utgångspunkt i standarden ISO/IEC 27000, dataskyddsförordningen och övrigt gällande lagar och förordningar.
- Riktlinjer konkretiseras med beslut om, tillämpningsrutiner och övriga systemnära beslut.
- Varje nämnd är personuppgiftsansvarig och samtliga informationstillgångar ska vara förtecknade inom respektive nämnd.
- Det sker kontinuerlig uppföljning av system och rutiner.

Risk och sårbarhetsanalyser
Risk- och sårbarhetsanalyser ska göras för att förebygga oönskade händelser som kan inträffa och få negativ påverkan på informationssäkerheten. Risk- och sårbarhetsanalyser ska genomföras kontinuerligt samt vid större förändringar, till exempel vid större systemuppdateringar, nyutveckling, nya användargrupper, extern

åtkomst eller som en följd av en inträffad incident. Verksamheter som omfattas av lagen om samhällsviktiga och digitala tjänster har särskilda krav att genomföra risk- och sårbarhetsanalyser och dessa analyser ska uppdateras årligen. Samtliga förvaltningar och bolag ska medverka i arbetet med informationssäkerhetsanalyser och upprättandet av tillhörande handlingsplaner för informationssäkerhetsarbetet.

Risk och sårbarhetsanalysen ligger till grund för hur arbetet med informationssäkerhet ska bedrivas. Handlingsplaner för informationssäkerhet innehåller konkreta mål och åtgärder bland annat baserade på analysen.

Rutiner, metoder, vägledningar och andra stöddokument tas fram centralt för att stödja arbetet med informationssäkerhet på olika nivåer och för att underlätta tillämpningen och efterlevnaden av trygghet- och säkerhetspolicyn och dessa riktlinjer för informationssäkerhet.

Hantering av informationstillgångar
Samtliga informationstillgångar i kommunen ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är informationsägare och systemägare.

Informationsklassificering
Samtliga informationstillgångar ska klassificeras enligt kommungemensam modell för informationsklassificering och är en grundläggande komponent i informationssäkerhetsarbetet. Genom att klassificera information utifrån krav på dess konfidentialitet, riktighet, tillgänglighet och spårbarhet skapar vi förståelse för och kan styra vilket skydd som krävs för olika informationsmängder. Det är informationen som är den primära tillgången och som ska klassificeras. Resurser som används för att hantera informationen, till exempel programvaror, system, tjänster och fysiska tillgångar ska utformas och anpassas till de krav som klassificeringen i förlängningen ställer på dessa. För den information som hanteras i verksamhetssystem och digitala verktyg ska Marks kommuns systemförvaltarmodell efterlevas. Informationsägare och systemägare ska säkerställa att informationssäkerhetskrav fastställs och följs upp. Särskilt fokus ska ligga på information med höga skyddskrav.

Kommunens ambition är att till så stor som möjligt nyttja standardiserade sätt att klassificera information på. SKR:s modell KLASSA ska användas för att klassificera information som behandlas både digitalt och analogt. Det innebär att informationen, ur ett säkerhetsperspektiv, klassas i skala 0–4 utifrån konfidentialitet, tillgänglighet, riktighet och spårbarhet.

Nivå 0 innebär att inga krav finns på informationen ur det specifika avseendet. Nivå 4 innebär att kravnivån på informationen, utifrån det specifika avseendet, är av betydelse för Sveriges säkerhet eller att bristande säkerhet kan leda till terrorbrott. Information som omfattas av sekretess bör klassas som minst nivå 2 utifrån konfidentialitet. Rörande all information med konfidentialitetsnivå 1 eller högre så

begränsas åtkomsten till uppgifterna till de som är i direkt behov av informationen för sin yrkesutövning.

Klassningen av informationsbehandlingar ska vara samordnade med digitaliseringsenhetens klassning av IT-system som syftar till att identifiera vilka resurserna som krävs för driften av systemet.

Informationssäkerhetsincidenter
Marks kommun ska klara av att upptäcka, hantera och rapportera incidenter som innebär ett hot eller en störning mot informationssäkerheten. Incidenterna ska hanteras i ett kommungemensamt ärendehanteringssystem. I de fall där incidenter ska rapporteras till särskild myndighet ska rapporteringen göras av verksamheten med stöd av utvecklingsledare för informationssäkerhet.

Kontinuitetsplaner
Inom varje förvaltning ska det finnas en ständigt aktuell kontinuitetsplanering där organisering och åtgärdsplan vid störningar i verksamheten finns dokumenterat. Respektive förvaltningschef avgör vilka IT-stöd som omfattas av kontinuitetsplanering.

Anskaffning, utveckling och underhåll av IT-tjänster
Upphandlande verksamhet ansvarar för att vid anskaffning, utveckling och avveckling av IT-tjänster, som till exempel datasystem och molntjänster, säkerställa rätt nivå av informationssäkerhet. När nya system ska anskaffas eller nya funktionaliteter i system ska utvecklas så måste krav som rör informationssäkerhet inkluderas. Kraven ska utgå ifrån den klassningen av informationsbehandling som har gjorts. Om ett system för en helt ny informationsbehandling ska anskaffas bör en klassning göras innan systemet kravställs. Systemägaren för systemet har ansvar att rätt säkerhetskrav formuleras som överensstämmer med kraven från verksamheten. Ta även hänsyn till riktlinjer för hantering av personuppgifter i Marks kommun för krav på personuppgiftsansvarig avseende tillräcklig säkerhetsnivå för den registrerades personuppgifter

För att uppnå rätt nivå av informationssäkerhet för IT-tjänster krävs:

- Informationsklassificering med tillhörande riskanalys genomförs och resultatet ligger till grund för informationssäkerhetskraven vid upphandling.
- Servicenivåavtal (SLA) med leverantören.
- Krav på rapportering av leverantörens arbete med informationssäkerhet.
- Krav på insyn i leverantörens testning.
- Krav på uppföljning och övervakning av leverantörens efterlevnad med Marks kommuns informationssäkerhetskrav.

Organisation och Ansvar

Kommunstyrelsen fastställer riktlinjer för informationssäkerhet. Säkerställer att nämnder och bolag avsätter tillräckliga resurser för förvaltningarnas och bolagens informationssäkerhet. Säkerställer att kommunens styrning och ledning gällande informationssäkerhet är effektiv och ändamålsenlig genom styrning och stöd.

Övriga nämnder och bolagsstyrelser Ansvarar för att riktlinjer för tillämpas och följs upp.

Kommundirektör säkerställer att kommunens IT-miljö, exempelvis tjänster, processer, systeminfrastruktur är tillräcklig och uppfyller verksamheters krav, legala krav och beslutad policy, riktlinjer och rutiner. Vidare säkerställer kommundirektören att det övergripande och strategiska arbetet för att leda och utveckla informationssäkerhetsarbetet, är samordnat.

Förvaltnings- och bolagsansvariga samt övriga chefer i verksamheterna att riktlinjerna är kända inom den egna verksamheten.

Personuppgiftsansvariga (PuA) är samtliga nämnder i kommunen. Skyldigheterna som följer med personuppgiftsansvaret regleras i riktlinjer för personuppgifter. Ansvaret för informationssäkerhet följer verksamhetsansvaret med särskilt ansvar på chefsnivå.

Informationsägare ansvar för informationsmängd och ska avgöra hur informationen ska klassas och utifrån denna ställa krav på hur information kan och får hanteras och användas.

Systemägare har det övergripande ansvaret för att datasystemet förvaltas på bästa sätt för verksamheten. Systemägaren fattar de avgörande besluten om datasystemets anskaffning, utveckling eller avveckling. Systemägaren ansvarar för att systemsäkerhetsplan finns och revideras vid behov. Systemägaren ansvarar för att det finns en informationsägare

Systemförvaltare ansvarar att säkerhetskraven verkställs i den tekniska miljön.

Varje anställd ska ha den kunskap som krävs för att förstå sitt ansvar för informationssäkerhet. Det ska också säkerställas att kunskaper om hot och problem som rör informationssäkerhet tillgodoses samt att man är rustad för att följa kommunens regelverk för informationssäkerhet under sitt arbete. Anställda ansvarar för att gällande regler för informationssäkerheten följs samt att upptäckta brister rapporteras enligt fastställda rutiner.

Uppföljning/Efterlevnad

Kontinuerlig uppföljning av informationssäkerhetsarbete ska ske i enlighet med ledningssystemet för informationssäkerhet. Revision av hela eller stora delar av kommunens informationssäkerhet ska göras regelbundet. Särskilt fokus ska ligga på uppföljning av hantering av informationsmängder med höga skyddskrav.

Årligen ska efterlevnad gällande Riktlinjer för informationssäkerhet följas upp genom internkontroll.

Sårbarheter och brister som upptäcks vid granskningar ska framgå av en åtgärdsplan. Akuta sårbarheter och brister ska åtgärdas omedelbart.