EKERÖ KOMMUN

2018-03-01

Policy för informationssäkerhet och dataskydd

Dnr KS18/60-113

Bakgrund

Kommunernas verksamheter är en av de mest betydelsefulla för samhället och för individen. I det digitala samhället kan ingen verksamhet upprätthållas utan en fungerande informationshantering. Därmed är kommunens informationshantering en verksamhetskritisk resurs.

Bristfällig informationssäkerhet leder bland annat till risk för liv och hälsa och för den personliga integriteten men kan även vara en risk för en negativ ekonomisk påverkan och för att tilliten till kommunen skadas.

Förutom Ekerö kommuns interna behov finns externa krav på informationssäkerhet. Ökade krav på dataskydd, skydd för samhällsviktig verksamhet och infrastruktur samt på krisberedskap och delaktighet i det civila försvaret måste inkluderas i kommunens informationssäkerhetsarbete. Den alltmer integrerade nationella e-hälsan kräver att alla deltagande aktörer har en nivå av säkerhet som inte äventyrar helheten.

Sammantaget har kommunerna samhällets mest komplexa krav på informationssäkerhet. Därför är en fast styrning och systematik nödvändig för att Ekerö kommun ska lyckas upprätthålla en informationshantering med tillräcklig säkerhet och kvalitet. Ledningssystemet för informationssäkerhet (LIS) är verktyget för att uppnå detta.

Denna policy utgör grunden för ett systematiskt arbete med informationssäkerhet som ger en ändamålsenlig nivå av skydd och kvalitet i Ekerö kommuns informationshantering. Informationssäkerhetsarbetet ska ge stöd för den generella styrningen av kommunen, möjliggöra digitalisering och ska även tillgodose de krav på informationssäkerhet som ingår i dataskyddsförordningen.

Denna policy är även dataskyddspolicy för Ekerö kommun.

Definition

Med informationssäkerhet avses hantering av information med rätt nivå av konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Inriktning

Ekerö kommuns inriktning är att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (LIS). För att hålla rätt nivå och rätt inriktning ska kommunens informationssäkerhet utgå från riskanalyser inklusive informationsklassningar på olika nivåer i organisationen.

Informationshanteringen ska skyddas på ett kostnadseffektivt sätt där risk vägs mot nytta på ett dokumenterat och kommunicerbart sätt. Tillräckliga resurser behöver tilldelas för informationssäkerhetsarbetet.

Centrala informationssäkerhetsåtgärder som informationsklassning, styrning av åtkomst, loggning, incident- och kontinuitetshantering ska vara prioriterade i informationssäkerhetsarbetet. Det ska finnas en beslutad metod för informationsklassning som även innehåller standardiserade skyddsnivåer.

LIS regler gäller för all information som hanteras av verksamheten och alla medarbetare för att utföra kommunens uppdrag. Som medarbetare räknas även uppdragstagare. Reglerna ska tillämpas då kommunen upphandlar produkter och tjänster som kan påverka informationssäkerheten.

Särskilt gällande dataskydd

Ekerö kommuns hantering av personuppgifter ska ske endast då det finns en laglig grund för att göra detta och då på ett så begränsat sätt som möjligt. Personuppgifter som hanteras ska vara korrekta och det ska vara lätt för utomstående att få insyn i hur hanteringen sker. Insamlade uppgifter kommer endast att hanteras för det ändamål som uppgivits och lagras endast så lång tid som ändamålet motiverar.

Enda undantag från detta är behandling för arkivändamål som motiveras av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. I kommunens processer och digitala lösningar ska integritet som standard vara inbyggt i alla steg genom organisatoriska och tekniska lösningar.

Den registrerade ska kunna ta del av de uppgifter som kommunen hanterar och lagrar om personen, rätta felaktiga uppgifter och om det inte stridet mot kommunens myndighetsutövning eller andra grundläggande intressen, få uppgifter raderade.

Kommunens dataskyddsombud ska genom fortlöpande kontroller säkerställa att dataskyddet fungerar enligt ovanstående och, om så inte sker, rapportera till personuppgiftsansvariga och kommundirektören samt i vissa fall till dataskyddsmyndigheten.

Krav på Ekerö kommuns ledningssystem för informationssäkerhet (LIS)

Ekerö kommuns LIS ska styra informationshanteringen så att informationen hanteras med den säkerhet som ledningen bedömt lämplig utifrån verksamhetens behov och externa krav. Styrningen omfattar att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering.

LIS dokumenteras i denna policy samt i riktlinjer och instruktioner ordnade i en hierarkisk struktur. Dokumentationen ska ses som en helhet och det ska finnas en spårbarhet mellan olika ingående dokument.

LIS viktigaste del är dock inte dokumentationen utan medarbetarnas kunskap, medvetenhet och motivation. Forum för dialog och utveckling i informations-säkerhetsfrågor samt målgruppsanpassat material är därför centrala funktioner i LIS. Det ska inrättas ett särskilt forum för samordning och hantering av informationssäkerhetsfrågor med representation från verksamheten och specialistfunktioner. Forumet sammankallas regelbundet och leds av informationssäkerhetsstrateg.

LIS omfattar inte de krav som följer av säkerhetsskyddslagen.

Ansvar och roller

Ansvaret för informationssäkerhet delas upp i ett ledningsansvar och ett verksamhetsansvar.

Kommunen ska ha tillgång till tillräcklig kompetens inom informations-säkerhetsområdet för att kunna hantera den komplexa kravbilden. Kompetensen ska finnas både i form av spetskompetens och i form av en bred förståelse av betydelsen av informationssäkerhet hos medarbetarna.

Det ska finnas en informationssäkerhetskultur som uppmuntrar engagemang hos alla medarbetare och, förutom att följa gemensamma regler, motiverar dem till att delta i att ständigt förbättra informationssäkerheten.

Ledningsansvar: kommundirektör och informationssäkerhetsstrateg

Kommunstyrelsen har det yttersta ansvaret för informationssäkerhetsarbetet inom Ekerö kommun. Kommundirektören har ansvaret för att säkerställa att rätt kompetens finns i kommunens verksamhet för att genomföra de intentioner som formuleras i denna policy. I detta ansvar ingår att säkerställa att det finns styrdokument för LIS och resurser för att genomföra det som dessa styrdokument föreskriver. Kommundirektören ska även tillse att dataskyddsombud finns utsett för

kommunen som kan fungera i denna egenskap för kommunens personuppgiftsansvariga.

Kommundirektören ska ha en uppdaterad lägesbild över identifierade risker avseende informationshantering och besluta om hur dessa risker ska hanteras. Arbetet med lägesbilden ska när så är lämpligt samordnas med kommunens övriga riskhantering.

Informationssäkerhetsstrategen ska, i enlighet med kommundirektörens beslut, strategiskt och operativt utöva ledningsansvaret. Informationssäkerhetsstrategen ska som stöd för kommunens verksamhetsplanering årligen ta fram ett förslag på plan med budget för informationssäkerhetsarbetet.

Verksamhetsansvar: chefer och medarbetare

Ansvaret för informationssäkerhet är ett verksamhetsansvar och styrningen av informationssäkerhet ska utgå från nyttan i verksamhetsprocesserna. Ansvaret ska vara känt och accepterat.

Att utveckla och upprätthålla informationssäkerhet enligt LIS är en del i kommunens generella chefsansvar. Förvaltningschef/kontorschef har det övergripande ansvaret för informationssäkerheten inom respektive förvaltning/kontor. Detta innebär ansvar för tillämpningen av ledningssystemets regelverk i den egna förvaltningen/kontoret. Detta ansvar innebär bland annat att se till att personalen hanterar information enligt gällande styrdokument samt anpassning av LIS-regler för den egna verksamheten.

På IT-avdelningen ska en IT-säkerhetsansvarig finnas som har ansvaret för att utveckla och förvalta de IT-säkerhetsåtgärder som är följden av de krav som ställs i LIS.

IT-avdelningen har ett särskilt ansvar att omsätta LIS funktionella krav på säkerhet till tekniska lösningar. IT-driftchefen ska därför årligen ta fram ett förslag på plan med budget för it-säkerhetsåtgärder som följer informationssäkerhetsstrategens plan för informationssäkerhetsarbetet.

Uppföljning

Uppföljning av kommunens arbete med informationssäkerhet och dataskydd ska ske på ett regelbundet och strukturerat sätt.