Katrineholm

Informationssäkerhets-policy för Katrineholms kommun

Dokumentinformation

Beslutshistorik
Antagen av kommunfullmäktige 2010-06-21 § 106

Senast ändrad av kommunfullmäktige
2013-12-16 § 203

2021-06-14 § 95

Giltighet
Gäller från och med 2021-06-14

Gäller till och med 2023-12-31

Förvaltarskap[1]
Inom kommunstyrelsens ansvarsområde

Kategori
- Anvisningsdokument

Uppföljning
Hur:

När:

[1] Förvaltarskapet innebär ansvar för att:
- dokumentet efterlevs
- är tillgängligt
- följa eventuellt ändrade förutsättningar för dokumentet
- dokumentet följs upp och revideras
- dokumentet är aktuellt och uppdaterat

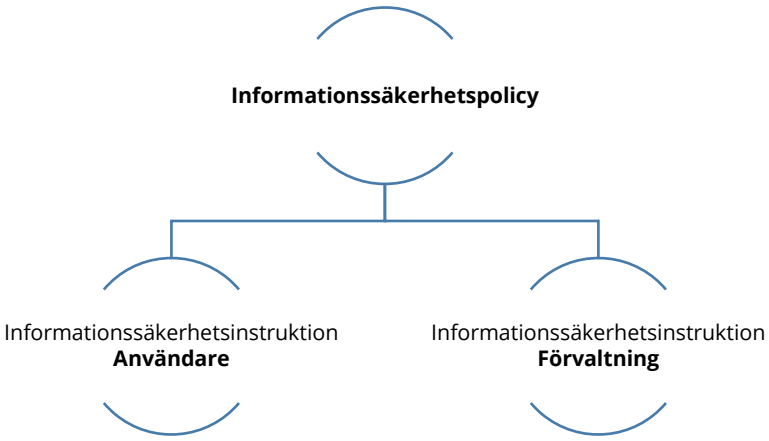
Innehåll

Informationssäkerhetspolicy för Katrineholms kommun

Informationssäkerhet är den del i organisationens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Informationssäkerhetspolicyn och särskilda informationssäkerhetsinstruktioner styr kommunens informationssäkerhetsarbete.

Policyns roll i informationssäkerhetsarbetet

Styrande dokument för informationssäkerhetsarbetet är Katrineholms kommuns informationssäkerhetspolicy och informationssäkerhetsinstruktionerna för användare och förvaltning.



Informationssäkerhetsinstruktion - Användare redovisar:

- hur en användare ska verka för att upprätthålla en god säkerhet.

Målgruppen för instruktionen är samtliga medarbetare vid kommunen samt andra parter som får tillgång till kommunens informationstillgångar.

Informationssäkerhetsinstruktion Förvaltning redovisar:

- det ansvar som ingår i de olika rollerna,
- hur informationssäkerhetsarbetet ska bedrivas,
- de riktlinjer som gäller för områden av särskild betydelse, samt
- regler för systemutveckling, systemunderhåll och incidenthantering.

Målgruppen för instruktionen är kommunens ledning, förvaltningsledning, systemägare och eventuell samordningsansvarig.

Allmänt om informationssäkerhet

Information är en av Katrineholms kommuns viktigaste tillgångar och hanteringen av den är en viktig del i arbetet med kommunens risk- och sårbarhetsanalys.

Utgångspunkter i Katrineholms kommuns arbete med informationssäkerhet är:

- lagar, förordningar och föreskrifter,

- krav uppsatta av Katrineholms kommun,
- avtal,
- att ge bättre förutsättningar för ledning, styrning, uppföljning, utvärdering och resursfördelning.

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar kommunens informationstillgångar utan undantag. Med informationssäkerhet avses:

- att informationen endast delges behöriga personer (**konfidentialitet**), samt att informationen levereras vid rätt tidpunkt och till skäliga kostnader,
- att informationen är riktig, komplett och aktuell (**riktighet**),
- att information som efterfrågas och som kommunen har ett ansvar att tillhandahålla finns och inte medvetet eller omedvetet förstörs utan stöd i lag eller gallringsbeslut (**tillgänglighet**), och
- att eftersökande, förändring eller borttagning av information går att spåra (**spårbarhet**).

Informationssäkerheten är en integrerad del av Katrineholms kommuns verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det omfattar samtliga anställda, förtroendevalda, myndiga elever inom skola/vuxenutbildning och uppdragstagare som arbetar med kommunens information. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för Katrineholms kommuns informationstillgångar. Rapporteringen ska ske till närmsta chef samt Informationssäkerhetsansvarig.

Alla delar inom kommunen är bundna av denna informationssäkerhetspolicy. Lokala avvikelser från denna policy inom organisationen är tillåtet, dock reglerar denna policy en miniminivå för hur informationssäkerhetsarbetet ska bedrivas. Eventuella lokala avvikelser får inte obefogat begränsa tillgången till information.

Den som använder Katrineholms kommuns informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för disciplinära åtgärder.

Mål

För Katrineholms kommuns informationssäkerhetsarbete ska gälla att:

- all personal har kunskap om gällande informationssäkerhetsregler,
- att informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, andra användare, samverkande partners och tredje man,
- ingångna avtal är kända och följs,
- krishanteringsförmågan upprätthålls,
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation,
- hotbilden för varje enskilt informationssystem som är av vikt för Katrineholms kommuns verksamhet analyseras fortlöpande,
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs, såsom förlust, skada, sabotage, förvanskning av information och otillbörlig åtkomst,
- årliga mål för arbetet beslutas i och framgår av verksamhetsplaneringen,

- Katrineholms kommun når sina övergripande visioner, strategier och mål.

Principer och arbetssätt

Katrineholms 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 Katrineholms kommuns informationstillgångar samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Katrineholms kommun ska:

- bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik,
- vara systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000 och dokumenteras i ett ledningssystem för informationssäkerhet,
- löpande ses över och förbättras, eftersom Katrineholms kommun och dess omvärld, inklusive hotbild, är under ständig förändring,
- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa,
- bygga på Katrineholms kommuns värderingar och ta hänsyn till verksamheters behov, externa krav samt rådande hotbild,
- 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 och underliggande riktlinjer för informationssäkerhet,
- ske i aktiv samverkan med det omgivande samhället såsom myndigheter, företag och nätverk, särskilt sådana som är normgivande inom informationssäkerhet som till exempel SKR (Sveriges kommuner och regioner), MSB (Myndigheten för samhällsskydd och beredskap), SIS (Svenska institutet för standarder) och IMY (Integritetsskyddsmyndigheten).

Verksamhetsdriven informationssäkerhet genom informationssäkerhetsklassning

Verksamheter har ansvar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras informationsmängder är, och därmed informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheter 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.

Katrineholms 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, tillgänglighet** och **spårbarhet.**

Roller och ansvar

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

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvaret och tillhörande åligganden för respektive roller beskrivs utförligare i Informationssäkerhetsinstruktion Förvaltning och Informationssäkerhetsinstruktion Användare.

Kommunstyrelsen har ägandeskapet för informationssäkerhetspolicyn och det övergripande ansvaret för informationssäkerheten. Kommunstyrelsen ansvarar även för att vid behov besluta om förändringar.

Nämnderna har det yttersta ansvaret inom respektive verksamhetsområde. Det innebär ansvar för att styrdokumentet beaktas i beslutsprocessen samt för att efterfråga och ta del av uppföljning.

Arkivmyndigheten/Arkivmyndigheterna leder arbetet med framtagande av dokumenthanteringsplaner, instruktioner för arkivering av digital/manuell information

Informationssäkerhetssansvarig har det operativa ansvaret för samordning av informationssäkerhetsarbetet i Katrineholms kommun. Det innebär ansvar för att dokumentet efterlevs, att det finns tillgängligt, att följa eventuellt ändrade förutsättningar för dokumentet, att dokumentet följs upp och revideras samt att dokumentet är aktuellt och uppdaterat. Informationssäkerhetsinstruktioner beslutas av Informationssäkerhetsansvarig. Referensgruppen i revisionsarbetet består av kommunjurist, säkerhetsansvarig, säkerhetsskyddsansvarig.

IT-säkerhetsansvarig samordnar arbetet med säkerheten i Katrineholms kommuns IT-miljö. IT-säkerhetsansvarig har tillsynsansvar för att IT-miljön är tillförlitlig och motsvarar interna och externa krav.

Dataskyddsombud kontrollera att dataskyddsförordningen (GDPR) följs inom Katrineholms kommun genom att utföra kontroller samt genomföra informations- och utbildningsinsatser.

Systemägaren är den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer. Varje facknämnd utser systemägare för informationssystem inom nämndens ansvarsområde. Denna policy upphäver inte det normala linjeansvaret. Det är alltid nämnden/styrelsen som har det övergripande ansvaret för informationen i ett IT-system. Systemägaren ansvarar för att basnivån för informationssäkerheten uppnås.

Systemförvaltarna utses av respektive systemägare och ansvarar för den dagliga användningen av informationssystemen.

Medarbetare, förtroendevald och myndig elev i skola/vuxenutbildning har ett ansvar att följa Informationssäkerhetspolicyn, Säkerhetsinstruktion Förvaltning och Säkerhetsinstruktion Användare.

Revidering och uppföljning

Revidering:

- Informationssäkerhetspolicyn ska ses över vid revidering av kommunplanen eller årligen.
- Informationssäkerhetsinstruktionerna revideras vid behov eller vid förändringar i informationssäkerhetspolicyn som påverkar informationssäkerhetsinstruktionerna.

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att:

- beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- regler följs, och
- att policy, säkerhetsinstruktioner och riskanalyser vid behov revideras.