Informationssäkerhets-policy

För en tillförlitlig informationshantering i en digitaliserad värld

Örebro kommun **2017-03-14** **Ks 412/2016**
orebro.se

ÖREBRO

PROGRAM
Uttrycker värdegrund och önskvärd utveckling av verksamheten.

POLICY
Uttrycker ett värdegrundsbaserat förhållningssätt och principer för vägledning.

STRATEGI
Konkretiserar ett program eller en policy och utgör en grund för Prioritering.

HANDLINGSPLAN
Beskriver konkreta mål och åtgärder.

RIKTLINJER
Säkerställer ett riktigt agerande och en god kvalitet vid handläggning och utförande.

Beslutad av Kommunstyrelsen, den 14 mars 2017, § 5

Dokumentansvarig på politisk nivå: Kommunstyrelsen
Dokumentansvarig på tjänstemannanivå: Informationssäkerhetsansvarig
Informationsklass: Öppen

Innehåll

Om denna informationssäkerhetspolicy

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Örebro kommun, och kompletterar kommunens övriga styrdokument inom bland annat IT, kvalitet, kommunikation och övrig säkerhet. Alla kommunens verksamheter omfattas av policyn, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Informationssäkerhetspolicyn gäller inte för kommunens bolag, undantaget när de använder sig av kommunens gemensamma informationstillgångar, eller då det finns särskilda behov av samordning.

Informationssäkerhetspolicyn är ett övergripande dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat. Styrdokumentet riktlinjer för informationssäkerhet är mer detaljerat och konkretiserar denna informationssäkerhetspolicy.

Denna policy är fastställd av kommunstyrelsen och gäller fr.o.m. 2017-03-14.

Om informationssäkerhet

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

För att nå en hög kvalitet i vårt arbete måste information hanteras på rätt sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt 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 kan härledas från rättsliga krav eller från Örebro kommuns 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

Informationssäkerhet har inget egenvärde, utan ska bidra till att Örebro kommun når sina övergripande visioner, strategier och mål. Örebro kommun ska uppnå och upprätthålla en informationssäkerhet som

- innebär en robust, säker och tillförlitlig informationshantering,
- möjliggör ett aktivt medverkande i det digitala samhället,
- bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personliga integritet,
- motsvarar medborgares och externa verksamheters behov och förväntningar,
- uttrycks i aktuella styrdokument som policy och riktlinjer,
- efterlever krav i lagar, förordningar, föreskrifter och avtal.

Principer och arbetssätt

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

Arbetet med informationssäkerhet inom Örebro 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 med målet att skapa ett ledningssystem för informationssäkerhet (LIS),
- löpande ses över och förbättras, eftersom Örebro 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 Örebro 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 t.ex. SKL (Sveriges kommuner och landsting), MSB (Myndigheten för samhällsskydd och beredskap) och SIS (Swedish Standards Institute).

Verksamhetsdriven informationssäkerhet genom informationsklassning

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 kommunens digitaliseringsavdelning och externa 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.

Örebro 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. 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. Kommunens informationssäkerhetsansvarige 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. Ansvaret och tillhörande åligganden för respektive roller beskrivs utförligare i riktlinjer för informationssäkerhet.

Medarbetare har ett ansvar att följa Örebro kommuns informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Man har som medarbetare också ansvar att vara uppmärksam på brister och incidenter rörande informationssäkerheten och meddela sådana till kommunsupporten och närmsta chef.

Ledningar i form av kommunfullmäktige, kommunstyrelse, program- och driftsnämnder har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom sina respektive verksamhetsområden.

Verksamhetsansvariga, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Det åligger varje verksamhetsansvarig att tillse att sina medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås.

Objektägare ansvarar för att förvaltningsobjekt efterlever informationssäkerhetspolicy och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om objektets informationssäkerhetsnivå(-er) genom att klassning sker i enlighet med Örebro kommuns modell för informationsklassning. Objektägare ska utse förvaltningsledare.

Förvaltningsledare ansvarar för att objekts informationssäkerhetsrelaterade mål och åtgärder nås respektive genomförs.

Digitaliseringsavdelningen ansvarar för att säkerheten i Örebro kommuns IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt denna informationssäkerhetspolicy och underliggande riktlinjer för informationssäkerhet.

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

Informationssäkerhetsansvarig har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Informationssäkerhetsansvarig ska arbeta i samråd med säkerhetschefen och övriga ledamöter i kommunens informationssäkerhetsråd.

Stadsarkivet har tillsynsansvar för att informationen hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen, samt kommunens interna styrdokument rörande informationens långsiktiga hantering och bevarande.

Personuppgiftsansvariga är kommunstyrelsen och övriga nämnder i kommuner. Dessa är ansvariga för hanteringen av personuppgifter och ska utse personuppgiftsombud som kontrollerar att personuppgifter hanteras på ett korrekt sätt i verksamheten.

Uppföljning och rapportering

Efterlevnaden av informationssäkerhetspolicyn och riktlinjer för informationssäkerhet ska följas upp regelbundet.

Informationssäkerhetsansvarig ska årligen rapportera läge och status gällande informationssäkerhet till kommundirektören och kommunstyrelsen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.