Revidering av informationssäkerhetspolicy – Antagande
Ärende 20
KS 2017/336

2017-11-15 | Dnr: KS 2017/336

Kommunstyrelsen

Ny Informationssäkerhetspolicy från 2018

Förslag till beslut

Kommunstyrelsens förslag till kommunfullmäktige
Kommunfullmäktige antar informationssäkerhetspolicy, enligt bilaga

Ärendebeskrivning

Informationssäkerhet är den del i Kävlinge kommuns lednings- och kvalitetsprocess som avser hanteringen av verksamhetens information. Informationssäkerhetsarbetet ska ses som en del av Kävlinge kommuns interna säkerhetsarbete, och kommunfullmäktige är den verksamhet som har det övergripande ansvaret för det interna säkerhetsarbetet.

Vid Ernst & Youngs granskning 2015, vilken hade fokus på just informations- och IT-säkerhet, noterades det att Kävlinge kommuns gällande Informationssäkerhetspolicy (från 2013) behöver uppdateras. Detta har gjorts, och förslaget till ny informationssäkerhetspolicy följer den internationella standarden SS-ISO/IEC 27000, samt gällande lagstiftning (inklusive kommande dataskyddsförordningen GDPR).

Liggande förslag har även kommunicerats med Kävlinges IT-samarbetskommuner Burlöv och Staffanstorp, då likalydande informationssäkerhetspolicys i de tre kommunerna är att föredra. Informationssäkerhet skiljer sig dock från IT-säkerhet, då IT-säkerheten syftar till att skydda den IT-tekniska biten, medan informationssäkerheten skyddar all form av ren information. Således antar Kävlinge kommun en egen informationssäkerhetspolicy.

Beslutsunderlag

- Informationssäkerhetspolicy Förslag

Kommunkansliet

Mikael Persson
Kommundirektör

Mats Svedberg
Kanslichef

Kommunstyrelsen
Hanna Sandberg
• Hanna.Sandberg@kavlinge.se

Kävlinge kommun
046 - 73 90 00 • kommunen@kavlinge.se • www.kavlinge.se

Beslutet ska skickas till

För kännedom
Säkerhetsenheten
För verkställighet
Kommunfullmäktige

2018-01-10

Informationssäkerhetspolicy för Kävlinge kommun

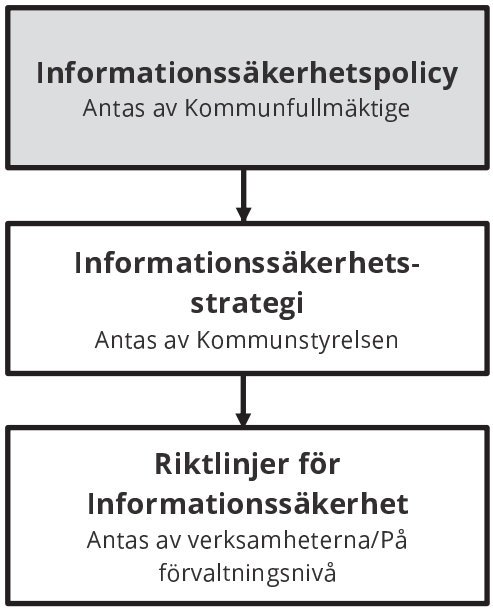
Inledning

Informationssäkerhet är den del i Kävlinge kommuns lednings- och kvalitetsprocess som avser hanteringen av verksamheternas information. Informationssäkerhetspolicyn styr tillsammans med dokumentet *Informationssäkerhetsstrategi* och verksamhetsspecifika *Riktlinjer för informationssäkerhet* kommunens informationssäkerhetsarbete.

Alla verksamheter där kommunen har ett huvudmannaansvar är bundna av denna informationssäkerhetspolicy, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna policy.

1. Policyns roll i informationssäkerhetsarbetet

Kävlinge kommuns informationssäkerhetsarbete kan beskrivas enligt följande modell:



2. Policyns syfte och avgränsning

Syftet med denna policy är att ange Kävlinge kommuns övergripande krav och inriktning med informationssäkerheten, samt att redovisa hur ansvaret och arbetet med informationssäkerhet är fördelat inom kommunen.

Avgränsning sker dels gentemot andra interna säkerhetsområden (exempelvis kommunikation och miljö), och dels gentemot icke-kommunspecifika säkerhetsområden (exempelvis IT-säkerhet).

3. Allmänt om Kävlinge kommuns informationssäkerhet

Information är en av Kävlinge kommuns viktigaste tillgångar, och hanteringen av denna är en vital del i arbetet med kommunens risk- och sårbarhetsanalyser. Informationssäkerheten omfattar alla kommunens informationstillgångar, utan undantag.

Med *informationstillgångar* avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Informationstillgångar kan exempelvis lagras i datorer, skickas via Internet, skrivas ner på papper, bestå av foton eller ritningar eller framföras muntligen.

Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till informationssäkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för kommunens informationstillgångar. Rapportering sker enklast till närmaste chef, alternativt till säkerhetchefen vid allvarligare incidenter.

Utgångspunkter för kommunens arbete med informationssäkerhet är gällanande lagar, förordningar och föreskrifter, samt egna kommunala krav och avtal.

3.1 Ledord: Tillgänglighet, Riktighet, Spårbarhet och Konfidentialitet

I linje med Myndigheten för Samhällsskydd och Beredskaps rekommendationer, liksom den etablerade svenska och internationella standarden inom området *SS-ISO/IEC 27000*, formas Kävlinge kommuns informationssäkerhetsarbete utifrån de fyra ledorden *tillgänglighet, riktighet, spårbarhet* och *konfidentialitet.*

• **Tillgänglighet**: Att informationen är tillgänglig i förväntad utsträckning och inom önskad tid

• **Riktighet**: Att information skyddas mot oönskad och obehörig förändring eller förstörelse

• **Spårbarhet**: Att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare (vem, vad, när)

• **Konfidentialitet**: Att information inte tillgängliggörs eller avslöjas till obehörig

4. Organisation, roller och ansvar

Kommunfullmäktige har det övergripande ansvaret för kommunens interna säkerhetsarbete, vilket också innefattar informationssäkerhetsarbetet. Kommunstyrelsen har i sin tur det övergripande utredningsansvaret vid policymissbruk. Verksamhetscheferna har det direkta ansvaret för informationssäkerhetsarbetet inom sin respektive verksamhet.

Varje verksamhet innehar det yttersta säkerhetsansvaret för sin verksamhets informationstillgångar och informationssäkerhetsabete. Vid grövre policymissbruk kan ärendet lyftas till kommunstyrelsen, som i sin tur kan lyfta ärendet till kommunfullmäktige vid mycket allvarliga incidenter.

6. Generella krav

Nedan presenteras de krav som Kävlinge kommuns ledning har på kommunen och dess verksamheter gällande informationssäkerhetsarbetet.

6.1 Informationstillgångar ska alltid skyddas

Informationstillgångar ska skyddas i skälig omfattning, så att individer, samverkande partners, ekonomiska tillgångar, investeringar, säkerhetsobjekt och säkerhetsinstallationer inte skadas. Händelser i informationssystem som kan leda till negativa konsekvenser ska förebyggas. Information ska aldrig spridas eller användas utöver det som är syftet med informationshanteringen.

6.2 Förteckning av kommunens informationssystem

Samtliga informationssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare, vad som är syftet med systemet samt vilka känsliga uppgifter systemet hanterar. Vissa informationssystem är en förutsättning för att kunna bedriva kommunens verksamhet. För dessa ska en riskanalys upprättas med stöd av kommunens verktyg för analys av informationssäkerhet (se punkt 6.4 om informationsklassning).

6.3 Informationssäkerhetsutbildning

All personal ska regelbundet få den utbildning som behövs för att informationssäkerheten ska upprätthållas. Nya medarbetare ska ha kännedom om *Informationssäkerhetsstrategin*, samt sin verksamhets riktlinjer för informationssäkerhet.

6.4 Informationsklassning

Information som hanteras i kommunen ska klassificeras med avseende på konfidentialitet, riktighet, spårbarhet och tillgänglighet enligt kommunens gällande klassningsmodell, samt enligt gällande lagstiftning och föreskrifter.

6.5 Kontinuitetsplanering

Kontinuitetsplaneringen är av central betydelse för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. En kontinuitetsplan ska finnas för driften av IT-verksamheten baserad på de olika informationssystemens samlade krav.

7. Konsekvenser vid policymissbruk

Det är främst verksamhetscheferna som ansvarar för eventuella konsekvenser vid policymissbruk, men även kommunstyrelsen kan besluta om konsekvenser. Konsekvenserna ska stå i proportion till missbrukets/felhanteringens omfattning, och enbart syfta till att reparera vållad skada. Det är dock alla anställdas skyldighet att uppmärksamma missbruk/felhantering av informationssäkerheten. Vid större incidenter ska kommunstyrelsen besluta om utredning, och vem som är lämplig att bedriva utredningen.

8. Revidering och uppföljning

Informationssäkerhetspolicyn, *Informationssäkerhetsstrategi* och verksamheternas *Riktlinjer för informationssäkerhet* ska löpande följas upp och vid behov revideras. Ansvarig för revidering av policy och strategi är säkerhetschefen. Ansvarig för revidering av de verksamhetsspecifika riktlinjerna är verksamhetscheferna (alternativt delegerad informationssäkerhetsansvarig för verksamheten).