Informationssäkerhetspolicy

Dokumenttyp: Policy
Antagen av Knivsta kommunfullmäktige 2021-11-24, § 138
Giltighetstid: Tills vidare
Dokumentansvarig: Kanslichef Åsa Franzén

Innehåll

Denna policy ingår i Knivsta kommuns ledningssystem för informationssäkerhet (LIS). Dokumentet är en del av kommunens strategiska informationssäkerhetsarbete och bygger på SS-ISO/IEC 27000 standarden.

En **policy** inom LIS talar om kommunens **mål och inriktning** med informationssäkerhetsarbetet och antas av fullmäktige.

En **riktlinje** inom LIS beskriver hur kommunens informationssäkerhetsarbete förhåller sig till lagstiftning, anger **övergripande ansvarsområden** och antas av styrelse eller nämnd.

1. INLEDNING

Knivsta kommun hanterar stora mängder information inom alla verksamheter. För att Knivsta kommun ska kunna utföra sitt uppdrag behöver kommunen arbeta systematiskt med informationssäkerhet.

1.1 Syfte

Den här policyn är antagen av fullmäktige och anger övergripande mål och inriktning på informationssäkerhetsarbetet samt hur ansvaret i dessa frågor är fördelat. Policyn konkretiseras i

- *riktlinjer* som antas av styrelse eller nämnd i form av
    - *Kommunriktlinjer* som antas av Kommunstyrelsen och gäller generellt i kommunens verksamheter antas av Kommunstyrelsen och gäller generellt i kommunens verksamheter samt:
    - *Nämdriktlinjer* som antas av respektive nämnd och gäller inom respektive nämnds verksamhetsområde

1.2 Omfattning

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

Informationssäkerheten omfattar all typ av information oavsett hur den lagras, bearbetas eller kommuniceras. Information kan t.ex. vara i form av text, ljud, bilder och film, och kommuniceras med stöd av IT, papper eller genom tal.

1.3 Definitioner

Information handlar om allt vi gör t.ex. uppgifter om personal, tjänster, ekonomi, enskilda medborgare, företag och föreningar m.m. Informationen måste hanteras på rätt sätt. Informationssäkerhet handlar om att ha rutiner för hur information ska användas, bevaras och skyddas utifrån fyra aspekter:

- *Konfidentialitet:* att information inte tillgängliggörs eller avslöjas för obehöriga individer, enheter eller processer.
- *Riktighet:* att information är exakt, aktuell och fullständig,
- *Tillgänglighet:* att information är åtkomlig och användbar för behöriga,
- *Spårbarhet:* att det går att härleda aktiviteter eller händelser till ett identifierat objekt t.ex. handling, användare, dator, skrivare eller system.

Vilka krav på skydd av de olika aspekterna som information har skiljer sig åt. I vissa fall finns det rättsliga krav, i andra är det kommunens målsättningar som styr eller medborgares behov och förväntningar.

2. MÅL MED INFORMATIONSSÄKERHET

Informationssäkerheten ska bidra till att Knivsta kommun kan fullgöra sina uppdrag och följa aktuella lagar och förordningar. Knivsta kommun ska uppnå och upprätthålla en informationssäkerhet som:

- innebär en robust, säker och tillförlitlig informationshantering
- bidrar till att samtliga informationstillgångar är identifierade och förtecknade
- möjliggör ett aktivt medverkande i det digitala samhället
- bidrar till att uppsatta mål nås för kvalitet, effektivitet och personlig integritet
- motsvarar invånares och externa parters behov och förväntningar
- uttrycks i aktuella styrdokument: riktlinjer, anvisningar och instruktioner
- efterlever krav i lagar, förordningar, föreskrifter och avtal.

2.1 Principer och arbetssätt

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

Arbetet med informationssäkerhet inom Knivsta 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 27XXX med målet att skapa ett ledningssystem för informationssäkerhet (LIS)
- löpande ses över och förbättras
- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa
- 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. SKR (Sveriges kommuner och regioner), MSB (Myndigheten för samhällsskydd och beredskap) och SIS (Swedish Standards Institute).

2.2 Verksamhetsdriven informationssäkerhet

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 It-centrum och externa systemleverantörer.

För detta ändamål ska informationsklassning tillämpas, vilket innebär att information klassas med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Därigenom kan en anpassad och effektiv informationssäkerhet skapas.

Knivsta 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.

3. ANSVAR

3.1 Medarbetare

Medarbetare har ett ansvar att följa kommunens informationssäkerhetspolicy samt övriga styrdokument. Medarbetare ska också uppmärksamma brister och incidenter rörande informationssäkerheten och meddela sådana till närmsta chef.

3.2 Fullmäktige och nämnder

Fullmäktige har övergripande ansvar för att verksamheten sköts (genom revisionen och liknande uppföljningsuppdrag) och resurssätts (ekonomiskt, genom budgeten) i enlighet med lagar och fullmäktiges beslut, inklusive denna policy. Nämnderna och styrelser har det yttersta ansvaret för informationssäkerheten i de verksamheter som bedrivs inom respektive verksamhetsområden och bolag.

3.3 Verksamhetsansvarig

Verksamhetsansvarig oavsett nivå ansvarar för informationssäkerheten inom sin verksamhet. Verksamhetsansvarig ska se till att medarbetare har ett säkerhetsmedvetande och tillräcklig kunskap för att uppfylla målen med informationssäkerhetsarbetet.

3.4 Informationssäkerhetsansvarig

Ansvarar för övergripande strategiskt arbete och samordning av kommunens informationssäkerhetsarbete.

4. UPPFÖLJNING

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.