Datum
2022-12-07

Antal sidor
8

Torsby kommuns informationssäkerhetspolicy

En del av Torsby kommuns ledningssystem för informationssäkerhet (LIS)

Antagen av kommunfullmäktige 2023-02-27 § 13

Kicki Lech
säkerhetssamordnare
Strategiavdelningen
073-275 57 76 mobil
christina.lech@torsby.se

Innehållsförteckning

Reviderad, datum och §	**Revideringen avser**

Inledning

Information är en av kommunens viktigaste tillgångar och en väsentlig förutsättning för att kunna bedriva verksamheten. Kommunens informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt. Den här policyn utgör kommunens viljeriktning för att hantera information på ett systematiskt och informationssäkert sätt.

Informationssäkerhetspolicyn är en del av Torsby kommuns ledningssystem för informationssäkerhet (LIS). Ledningssystemet baseras på SS-ISO/IEC 27000 och Myndigheten för samhällsskydd och beredskaps (MSB) metodstöd för systematiskt informationssäkerhetsarbete.

Informationssäkerheten ska vara en integrerad del av den kommunala verksamheten. Alla som hanterar information har ett ansvar att upprätthålla informationssäkerheten. Chefer på alla nivåer har ett ansvar att aktivt verka för en positiv attityd till informationssäkerhetsarbetet.

Den här informationssäkerhetspolicyn ersätter dokumentet *Informationssäkerhet i Torsby kommun* som antogs av kommunfullmäktige 2008-09-15. Den kompletteras med dokument såsom rutiner och hanteringsanvisningar allt eftersom de tas fram eller revideras.

Informationssäkerhet

Information finns i alla kommunens verksamheter och handlar om allt det kommunen gör, exempelvis om personal, tjänster och det omgivande samhället med medborgare, företag, föreningar och så vidare. Information är därför en av kommunens viktigaste tillgångar.

För att nå en hög kvalitet i arbetet måste information hanteras på rätt sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån följande tre aspekter:

- konfidentialitet – vilket innebär att informationen endast ska vara tillgänglig för behöriga användare,
- riktighet – vilket innebär att informationen ska vara korrekt, aktuell och fullständig och
- tillgänglighet – vilket innebär att informationen ska vara åtkomlig och användbar när verksamheten behöver den.

Information har olika krav på sig gällande de tre nämnda aspekterna. Kraven kommer från lagstiftning såsom offentlighets- och sekretesslagen, dataskyddsförordningen, lag om informationssäkerhet i samhällsviktiga och digitala tjänster, säkerhetsskyddslagen, socialtjänstlagen, patientdatalagen och hälso- och sjukvårdslagen med flera.

Kraven kommer även från Torsby kommuns risk- och sårbarhetsanalys samt kommunens egna målsättningar. Dessutom har medborgare, företag och andra aktörer i vår omvärld, behov och förväntningar som ställer krav på kommunens informationssäkerhet.

Informationssäkerhetsarbetet stöds, tillsynas och följs upp från flera myndigheters håll, bland annat av Myndigheten för samhällsskydd och beredskap (MSB), Sveriges kommuner och regioner (SKR), Integritetsskyddsmyndigheten (IMY), Säkerhetspolisen (SÄPO) och Livsmedelsverket.

Informationssäkerhet omfattar information i alla dess former, analog som digital, och oavsett hur informationen lagras, bearbetas och kommuniceras.

Mål med informationssäkerhet

Torsby kommun ska bedriva ett aktivt informationssäkerhetsarbete med syfte att säkerställa att kommunens information, oavsett om den är analog eller digital, hanteras på ett säkert sätt utifrån aspekterna konfidentialitet, riktighet och tillgänglighet.

Torsby 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 mål inom andra områden, exempelvis kvalitet och effektivitet nås,
- motsvarar medborgares och externa verksamheters behov och förväntningar och
- efterlever krav i lagar, förordningar, föreskrifter och avtal.

Målsättningen med informationssäkerhetsarbetet är att säkerställa Torsby kommuns verksamhet mot avbrott, förebygga oönskade händelser och minimera konsekvenserna om de trots allt skulle inträffa.

Ansvar i informationssäkerhetsarbetet

Kommunfullmäktige, kommunstyrelsen och nämnderna

Kommunfullmäktige uttrycker sin viljeriktning rörande informationssäkerhetsarbetet i denna policy. Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhetsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp ramarna för arbetet med informationssäkerhet. Nämnderna ansvarar för informationsäkerheten inom ramen för sina verksamheter. Nämnderna har det yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den får hanteras och av vem den får hanteras.

Ledningen och verksamhetsansvar

Informationssäkerhetsansvaret följer ordinarie verksamhetsansvar. Det innebär att den som har ansvar för en verksamhet (exempelvis en organisatorisk del, en process eller ett projekt) även har ansvar för informationssäkerheten i den verksamheten.

Ledningen inom tjänstemannaorganisationen ska vara förebilder inom informationssäkerhetsarbetet, hålla sig informerade om hur arbetet fortgår, fatta beslut och tilldela resurser som motsvarar målsättningar och ambitioner.

Medarbetare och förtroendevalda

Alla medarbetare och förtroendevalda i Torsby kommun ansvarar för att hantera information på ett säkert sätt. Det innebär att följa de styrdokument som finns samt att rapportera incidenter som uppstår.

Principer och arbetssätt

Torsby kommun ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet ska vara normerande, stödjande och kontrollerande. Viktiga förmågor i arbetet är att kunna identifiera hot, sårbarheter och risker rörande kommunens informationstillgångar. Det är även viktigt att utforma och införa säkerhetsåtgärder för att reducera de identifierade riskerna till en acceptabel nivå.

Arbetet med informationssäkerhet inom Torby kommun ska:

- drivas av verksamheterna själva med stöd av informationssäkerhetsstrateg och IT-avdelningen. Arbetet ska vara en integrerad del av verksamheterna,
- 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,
- innebära att all information, oavsett om den är analog eller digital, ska klassas utifrån antagen klassningsmodell,
- löpande ses över och förbättras utifrån att kommunens omvärld och hotbild ständigt förändras,
- 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 och externa krav och
- vara kommunicerat till verksamheten; chefer, medarbetare och förtroendevalda ska få information och utbildning för att nå och upprätthålla en grundnivå i säkerhetsmedvetande och för att kunna leva upp till gällande styrdokument.

Uppföljning och efterlevnad

Varje verksamhet ansvarar för att följa upp sitt eget informationssäkerhetsarbete och på begäran lämna vidare information till informationssäkerhetsstrateg.

Efterlevnaden av informationssäkerhetsarbetet ska följas upp till exempel via interkontroll, revisioner och i ledningens förbättringsarbete.

Ledningens genomgång

Informationssäkerhetsstrateg ansvarar för att minst en gång årligen följa upp och redovisa informationssäkerhetsarbetet genom så kallad ledningens genomgång. På ledningens genomgång deltar kommundirektör och ledningsgrupp utifrån kommundirektörs önskemål.

Incidentrapportering

Chefer, medarbetare och förtroendevalda i Torsby kommun ska följa upp informationssäkerhetsarbetet genom att rapportera avvikelser och incidenter samt åtgärda informationssäkerhetsbrister. I förekommande fall ska incidenter rapporteras till berörda myndigheter.