TJÖRNS kommun

Informationssäkerhetspolicy

Typ av styrdokument	Policy
Beslutsinstans	Kommunfullmäktige
Beslutsdatum och paragraf	2022-10-20, § 168
Diarienummer	2021/141-003
Datum för senaste revidering	2022-10-20
Giltighetstid	2022-2027
Dokumentansvarig funktion	Informationssäkerhetssamordnare
Målgrupp för dokumentet	Nämnder och bolag inom Tjörns kommun

TJÖRNS kommun

Revideringar

Beslut	Diarienummer	Revidering avser

Informationssäkerhetspolicy

Inledning

Om informationssäkerhetspolicyn

Denna policy innehåller Tjörns kommuns viljeinriktning och övergripande mål för informationssäkerhetsarbetet. Dokumentet gäller för Tjörns kommuns nämnder och bolag med dess verksamheter och gäller tills vidare men bör revideras efter 3-5 år efter antagande.

Allmänt om informationssäkerhet

Information är en av kommunens viktigaste tillgångar. Tillgången till information och vår informationshantering är avgörande för alla som arbetar inom kommunen och för vår myndighetsutövning.

Behovet av informationssäkerhet ökar i takt med att kommuninvånarna förväntar sig effektiv kommunikation, dels via självbetjäning med hjälp av olika e-tjänster, dels i sin direktkontakt med kommunen. I allt större utsträckning sker också i förvaltningarna användning och utveckling av systemstöd för att leverera tjänster på ett effektivt sätt. Invånarna ska kunna förvänta sig att kommunen hanterar information som rör dem, exempelvis personuppgifter och information om de olika tjänster de använder, på ett säkert sätt. I samband med kriser krävs också effektiv och säker kommunikation med berörda verksamheter och invånare.

Konsekvensen av bristande informationssäkerhet kan medföra störningar i samhällsviktiga verksamheter, att information går förlorad, förvanskas eller rent av stjäls. Det kan även medföra ekonomiska förluster och att förtroendet för Tjörns kommun påverkas negativt.

Begreppsförklaring

Informationssäkerhet är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder som vidtas för att skydda informationstillgångar.

Informationen måste skyddas så
- att den alltid finns när vi behöver den (**tillgänglighet**),
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (**riktighet**), och
- att endast behöriga personer får ta del av den (**konfidentialitet**).

Övergripande mål

Målsättningen med informationssäkerhetsarbetet är att:

- Ett systematiskt informationssäkerhetsarbete är en naturlig del i kommunens verksamheter och är integrerad i organisationens befintliga sätt att leda och styra.
- Medvetandegöra och öka den allmänna kunskapen om informationssäkerhet inom organisationen.
- Informationssäkerhet beaktas i digitaliseringsarbetet; i synnerhet vid användande och utveckling av ny och innovativ teknik.
- Informationssäkerhetsperspektivet beaktas i alla fundamentala beslut för informationstillgångar (anskaffning, utveckling, avskaffande).

Vägledande principer och krav

Kommunen ska bedriva ett systematiskt informationssäkerhetsarbete med stöd av standardserien ISO/IEC 27000 för informationssäkerhet samt anpassa arbetet för att säkerställa efterlevnad av övrigt tillämpliga författningar.[1] Ledningen ska säkerställa att informationssäkerhetsarbetet tilldelas nödvändiga resurser samt att interna regler upprättas, efterlevs, utvärderas och anpassas.

Av särskild vikt är att följande krav uppfylls.

- Skyddsbehovet av information ska klassificeras med avseende på konfidentialitet, riktighet och tillgänglighet så att ändamålsenliga och proportionella säkerhetsåtgärder kan införas.
- Regelbundna riskbedömningar ska genomföras för informationssystemen och ansvarig verksamhet ska aktivt medverka i uppföljningen av riskhanteringen.
- Samtliga informationssystem ska vara identifierade, förtecknade och ha en tydlig organisation med ansvar för förvaltning och utveckling i enlighet med beslutad förvaltningsmodell.
- Kritiska informationssystem ska ha en uppdaterad och känd kontinuitetsplanering som skyndsamt ersätter befintliga arbetssätt vid avbrott och störningar.

[1] I ISO/IEC 27000-standardserien ingår aktiv omvärldsbevakning med analys av rättsliga krav. Vanligt förekommande krav som påverkar kommunal verksamhet är bland annat tryckfrihetsförordningen, offentlighets- och sekretesslagen, EU:s dataskyddsförordning (GDPR), NIS-regleringen, säkerhetsskyddslagen, arkivlagen, patientdatalagen och brottsbalken.

- Samtliga medarbetare ska få möjlighet att tillgodogöra sig en grundläggande förståelse för informationssäkerhet och tillämpning av den i den egna vardagen och verksamheten.

Övriga styrdokument inom området

Denna policy kompletteras med detaljerade och organisationsövergripande riktlinjer för informationssäkerhet. Dessa riktlinjer bör innehålla regler för bland annat förvaltningsmodell av informationstillgångar, informationssäkerhetsarbetets organisation och ansvar, principer för säkerhetsåtgärder, informationsklassningsmodell, tillåten och otillåten informationshantering.

Kommundirektören får i den mån som finnes lämpligt utfärda andra typer av detaljerade styrdokument såsom handlingsplaner med kortsiktiga mål, handböcker och instruktioner i syfte att stärka arbetet.