

Policy för informationssäkerhet och dataskydd

Beslutat av: Kommunfullmäktige

[Beslutat datum]

Diariennr: KS 2025/209-19

Innehåll

1. Inledning och syfte.....	3
2. Omfattning	3
3. Information- och personuppgiftshantering	3
4. Riskhantering och incidenthantering	4
5. Utbildning och medvetenhet	4
6. Efterlevnad och uppföljning	4

1. Inledning och syfte

Täby kommuns policy för informationssäkerhet och dataskydd fastställer principer och ställningstaganden för hur kommunen systematiskt ska skydda och hantera information, inklusive personuppgifter. Syftet är att säkerställa en trygg, lagenlig och effektiv informationshantering som värnar om både organisationen och individers rättigheter.

Målet med informationssäkerhet och dataskyddsarbetet är att:

- Säkerställa att rätt information är tillgänglig för rätt person vid rätt tidpunkt.
- Upprätthålla informationens riktighet, tillförlitlighet och spårbarhet.
- Skydda information från obehörig åtkomst, ändring och förlust.
- Efterleva lagkrav, såsom dataskyddsförordningen (GDPR) och offentlighets- och sekretesslagen, cybersäkerhetslagen.
- Stärka förtroendet för kommunens verksamheter genom en säker och transparent informationshantering.

Täby kommun ska bedriva ett systematiskt informationssäkerhets- och dataskyddsarbete som bygger på riskanalyser, tydliga ansvarsförhållanden och kontinuerlig uppföljning för att möta både nuvarande och framtida utmaningar inom informationssäkerhet och dataskydd.

2. Omfattning

Policyn omfattar all information som hanteras inom Täby kommuns verksamheter, oavsett form eller lagringsplats – och gäller för samtliga medarbetare och förtroendevalda. Kommunens ska tillse att externa parter som får tillgång till kommunens information genom avtal blir bundna av motsvarande krav på hantering.

3. Information- och personuppgiftshantering

Information är en av Täby kommuns mest värdefulla tillgångar och kommunen har ett ansvar att skydda denna på ett säkert och lagstadgat sätt.

Allt informationssäkerhets- och dataskyddsarbete ska utgå från principerna om tillgänglighet, riktighet och konfidentialitet för att säkerställa verksamhetens funktion

och allmänhetens förtroende. Arbetet ska vidare bedrivas som en kontinuerlig och aktiv process där information hanteras utifrån dess känslighet och gällande lagkrav.

För att säkerställa en hög säkerhetsnivå ska vedertagen praxis och ändamålsenliga metoder tillämpas. Arbetet ska vara kostnadseffektivt och proportionerligt i förhållande till de risker som identifieras.

Informationssäkerhet och dataskydd ska vara en integrerad del av kommunens verksamhetsstyrning och är en förutsättning för att uppnå kommunens övergripande mål. Arbetet ska ledas och samordnas på ett sätt som säkerställer att ansvarsfördelningen är tydlig och att arbetssätten blir en naturlig del av beslut och processer i hela organisationen som leder till kontinuerlig förbättring.

4. Riskhantering och incidenthantering

Riskbedömningar ska genomföras regelbundet för att identifiera och minimera hot mot informationssäkerheten. Informationssäkerhets- och personuppgiftsincidenter ska rapporteras utan dröjsmål enligt kommunens incidenthanteringsrutiner. För att säkerställa verksamhetens motståndskraft vid incidenter ska det finnas kontinuitets- och återhämtningsplaner.

5. Utbildning och medvetenhet

Alla medarbetare ska regelbundet erbjudas utbildningar inom informationssäkerhet och dataskydd för att stärka medvetenheten och säkerställa policyns efterlevnad. Policyn med tillhörande anvisningar ska finnas lätt tillgängliga för samtliga anställda och informationssäkerhet och dataskydd ska vara en naturlig del av kommunens löpande kompetensutveckling.

6. Efterlevnad och uppföljning

Efterlevnad av policyn och tillhörande anvisningar ska följas upp med internkontroll och egen revision. Om brister identifieras ska åtgärdsplaner upprättas för att korrigera och förbättra informationssäkerhets- och dataskyddsarbetet.

Leverantörer och tredjeparter ska genomgå återkommande säkerhetsrevisioner för att säkerställa att de uppfyller kommunens krav.

Policyn ska ses över minst en gång per mandatperiod och revideras vid väsentliga förändringar i lagstiftning, verksamhet eller riskbild.