Kommunrevisionen
Täby kommun

Kommunstyrelsen

För kännedom:
Kommunfullmäktige

Granskning av kommunens informations- och IT-säkerhetsarbete

KPMG har av Täby kommuns förtroendevalda revisorer fått i uppdrag att genomföra en översiktlig granskning för att upprätthålla en god informations och IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Det övergripande syftet med granskningen har varit att granska om kommunstyrelse och nämnder bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Den sammanfattande bedömningen utifrån granskningens syfte är att kommunstyrelse och nämnder i allt väsentligt bedriver ett systematiskt informationssäkerhetsarbete och att det sker på ett ändamålsenligt sätt.

Vi gör vår bedömning baserat på att det finns styrande och stödjande dokument som tydliggör krav på hur arbetet ska bedrivas samt tydliggör ansvar för aktiviteter och åtgärder som behöver vidtas för att informationssäkerhetsarbetet ska vara systematiskt.

Vi konstaterar att det finns ett engagemang för frågorna, en organisation och ansvarsfördelning som ger förutsättningar för ett systematiskt arbete. Vi bedömer att riskbedömningar och kartläggningar har bidragit till en kännedom om sårbarheter och behov av förbättringsåtgärder och att dessa har prioriterats för att stärka kommunens informations- och IT-säkerhet. Åtgärder har följts upp och i delar rapporterats till kommundirektör och kommunstyrelsen.

Även om vår bedömning är att arbetet i allt väsentligt sker på ett systematiskt sätt har vi identifierat ett antal förbättringsområden för att informations- och IT-säkerhetsarbetet ska stärkas ytterligare. Då granskningen baseras på uppgifter på en övergripande nivå är vissa av rekommendationerna till nämnderna av mer generell karaktär.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen utifrån deras övergripande ansvar att:

- Aktualisera informationssäkerhetspolicyn och utvärdera behov av riktlinjer för arbetet i enlighet med lämnat uppdrag till kommundirektören.

- Överväga om informationssäkerhetsutbildningar ska vara obligatoriska, samt besluta med vilken regelbundenhet de ska genomföras samt etablera rutiner för att även inkludera nyanställda och nytillträdda förtroendevalda.

- Utvärdera behov av att stärka kommunens förmåga att upptäcka säkerhetshändelser genom bl.a. övervakning och loggar, både avseende tekniska implementationer och att det finns en incidentorganisation och beredskap med tillräckliga förutsättningar att skyndsamt agera på hot och risker.

- Etablera ledningens genomgång i enlighet med anvisningar så att en samlad uppföljning av informationssäkerhetsarbetet finns dokumenterad och rapporteras till kommunstyrelsen.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och samtliga nämnder att:

- Säkerställa att informationsklassning och riskbedömning har gjorts för de informationstillgångar som hanteras inom respektive verksamhet.
- Utifrån informationsklassning och riskbedömning säkerställa att de skyddsbehov som identifieras följs upp med relevanta säkerhetsåtgärder.
- Säkerställa att utbildningsinsatser regelbundet genomförs för att bibehålla och utveckla en säkerhetskultur och medvetenhet om informationssäkerhetsrisker.

Revisionen önskar att kommunstyrelsen ger ett yttrande över granskningens slutsatser senast den 30 mars 2024.

Täby 16 november 2023

På uppdrag från Täby kommuns revisorer

Lars Nordin	Malin Forsberg Helgesson
Ordförande	Vice ordförande

Bilaga: Rapport KPMG granskning av kommunens information- och IT-säkerhetsarbete

Revisorerna har godkänt missivet på revisionssammanträde 2023-11-16.