Kommunrevisionen
Håbo kommun

För yttrande:
Kommunstyrelsen

För kännedom:
Kommunfullmäktiges ledamöter

Granskning av arbetet med informationssäkerhet

KPMG har av Håbo kommuns revisorer fått i uppdrag att granska kommunens arbete med informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2023. Syftet med granskningen har varit att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Den samlade bedömningen utifrån granskningens syfte är att kommunstyrelsens och nämndernas informationssäkerhetsarbete inte är systematiskt eller ändamålsenligt.

Då granskningen genomfördes pågick ett omfattande utvecklingsarbete inom hela kommunen, vilket också inriktas mot arbetet med informationssäkerhet. Det konstateras att en organisatorisk grund för arbetet lagts, och att det pågår ett arbete för att upprätta och etablera väsentliga styrdokument inom området. Däremot saknas flera operativa processer och systematik i både det operativa och långsiktiga arbetet.

Kommunledningen uttrycker en medvetenhet om betydelsen av ett ändamålsenligt informationssäkerhetsarbete där strategisk utveckling och samordning sker centralt och där nämnderna är drivande i det operativa arbetet. Uppfattningen är att nämnderna behöver stöd för att etablera former för informationssäkerhetsarbetet, varför det anses att kommunstyrelsen behöver prioritera det initialt. Med ett systematiskt informationssäkerhetsarbete ges möjlighet att identifiera ändamålsenliga it-säkerhetsåtgärder som skyddar kommunens informationstillgångar. I nuläget baseras implementerade it-säkerhetsåtgärder inte på konstaterade säkerhetsbehov, vilket enligt vår bedömning riskerar att exponera kommunen för cyberhot och intrång.

Utifrån resultatet av granskningen rekommenderas kommunstyrelsen att:

- Prioritera framtagandet av styrande dokument.
- I styrande dokument tydliggöra ansvar och roller för nyckelfunktioner inom informationssäkerhetsarbetet.
- Utvärdera nuvarande personella resurser är tillräckliga för att genomföra ett systematiskt informationssäkerhetsarbete.
- Säkerställa att en kommunövergripande riskanalys genomförs.
- Etablera en modell för informationsklassning.
- Tillse stöd och utbildning i informationsklassning och riskbedömning.
- Säkerställa att utbildning inom informationssäkerhet ges till anställda och förtroendevalda.
- Säkerställa att nuvarande övervakning, både personellt och tekniskt är tillräckligt mot bakgrund av behov samt nuvarande risker.

- Upprätta en incidenthanteringsrutin med tydliga eskaleringsvägar.
- Tillse att utbildning inom informationssäkerhet omfattar informationssäkerhetsincidenter.
- Säkerställa att uppföljning genomförs i enlighet med informationssäkerhetspolicyn.
- Säkerställa att beslutade mål följs upp regelbundet för att säkerställa att arbetet genomförs så att målen kan nås.

Vi förtroendevalda revisorer vill ha kommunstyrelsens yttrande till slutsats och rekommendationer senast den 15 juni 2024. Yttrandet ska skickas till Bertil Kinnunen, ordförande bertilkinnunen64@gmail.com och Micaela Hedin micaela.hedin@kpmg.se.

Bålsta 8 februari 2024
På uppdrag från Håbo kommuns revisorer

Bertil Kinnunen
Ordförande
Bilaga: Rapport KPMG Granskning av arbetet med informationssäkerhet

Revisorerna godkände missivet digitalt på sitt sammanträde 2024-02-08.