KOMMUNSTYRELSEN

Kommunrevisionen
Täby kommun

Yttrande avseende revisorernas granskning av kommunens informations- och säkerhetsarbete

Sammanfattning

Revisorerna har granskat om kommunen bedriver ett systematiskt informationssäkerhetsarbete på ett ändamålsenligt sätt.

Revisorernas bedömning efter granskning är att kommunstyrelsen och nämnder i allt väsentligt bedriver ett systematiskt informationssäkerhetsarbete och att det sker på ett ändamålsenligt sätt.

I de fall där revisorerna har identifierat förbättringsområden finns pågående och planerade åtgärder.

Synpunkter

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

Granskningen avser kommunstyrelsen, barn- och grundskolenämnden, gymnasie- och näringslivsnämnden, kultur- och fritidsnämnden, stadsbyggnadsnämnden, socialnämnden, äldrenämnden, överförmyndarnämnden, lantmäterinämnden, valnämnden, Södra Roslagens miljö- och hälsoskyddsnämnd.

Revisorernas bedömning efter granskningen är att kommunstyrelsen och nämnder i allt väsentligt bedriver ett systematiskt informationssäkerhetsarbete och att det sker på ett ändamålsenligt sätt.

Revisorerna har identifierat ett antal förbättringsområden för att informations- och IT-säkerhetsarbetet ska stärkas ytterligare.

Revisorerna rekommenderar kommunstyrelsen att:

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

2. 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.

3. 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.

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

Revisorerna rekommenderar kommunstyrelsen och samtliga nämnder att:

1. Säkerställa att informationsklassning och riskbedömning har gjorts för de informationstillgångar som hanteras inom respektive verksamhet.

2. Utifrån informationsklassning och riskbedömning säkerställa att de skyddsbehov som identifieras följs upp med relevanta säkerhetsåtgärder.

3. Säkerställa att utbildningsinsatser regelbundet genomförs för att bibehålla och utveckla en säkerhetskultur och medvetenhet om informationssäkerhetsrisker.

Kommunstyrelsens kommentarer på revisorernas rekommendationer.

Sammanfattade kommentar

De synpunkter och åtgärder som lyfts fram är relevanta och motsvarar också i huvudsak inriktning samt pågående och planerade åtgärder som redogjorts för under granskningen.

För kommunstyrelsen

1. Kommunstyrelsen bedömer att en revidering av policyn i enlighet med plan för uppdatering av styrdokument i kommunen är relevant, men ser att instruktioner till medarbetare fortsatt utarbetats med benämningen *anvisningar* istället för riktlinjer, för att harmonisera med kommunens nomenklatur för styrdokument och i enlighet med verkställighet enligt delegationsordningen.
2. Informationssäkerhetsutbildningar sker löpande genom riktade utskick till såväl medarbetare, chefer och förtroendevalda. Informationssäkerhetsutbildningar är av hög prioritet och deltagande/slutförande av utbildningar följs noggrant upp. Genom att utbildningarna läggs in som ett tydligt moment i introduktionen vid nyanställning och genom återkommande utskick och uppföljning under året för befintliga medarbetare bedömer kommunstyrelsen att effekten uppnås.
3. Ett utredningsarbete pågår i syfte att hitta säkra och kostnadseffektiva alternativ för övervakning och loggning av kommunens kritiska IT-miljöer. Ett arbete pågår även för att upprätta en incidentorganisation med förutsättningar och beredskap att skyndsamt agera på hot och risker.
4. Genomförs enligt upprättade anvisningar, inom ramen för ordinarie linjearbete.

För kommunstyrelsen och samtliga nämnder

1. Genomförs enligt upprättade anvisningar, inom ramen för ordinarie linjearbete.
2. Genomförs enligt upprättade anvisningar, inom ramen för ordinarie linjearbete.
3. Informationssäkerhetsutbildningar sker löpande genom riktade utskick till såväl medarbetare, chefer och förtroendevalda.

Informationssäkerhetsutbildningar är av hög prioritet och deltagande/slutförande av utbildningar följs noggrant upp.