2021-01-20

Lunds kommuns revisorer

För yttrande till:
Kommunstyrelsen

För kännedom till:
Kommunfullmäktige

Granskning av informationssäkerhet

Såväl nationellt som internationellt har diskussionen om informationssäkerhet i IT-samhället accentuerats under senare år. Det handlar då både om medvetna attacker mot informationssystem och datahantering och om oförutsedda brister i systemen. Kommunerna lagrar en betydande mängd data och många uppgifter, ofta sekretessbelagda, som rör enskilda individer.

Lunds kommuns förtroendevalda revisorer har därför valt att granska kommunstyrelsens arbete med informationssäkerhet. Vår sammanfattande bedömning är att kommunstyrelsen delvis har en ändamålsenlig intern kontroll avseende IT- och informationssäkerhet.

Granskningen visar att det finns grundläggande riktlinjer, rutiner och policys men det saknas en tydlig koppling mellan målen för informationssäkerhet och andra strategiska målsättningar för kommunen. Avsaknaden av en tydlig strategi på lång och kort sikt, kan påverka effektiviteten i arbetet med informationssäkerhet.

Vidare har brister noterats i utbildningsinsatser, behörighet- och åtkomsthantering samt säkerställandet av tillräcklig insyn i leverantörers arbete med informationssäkerhet.

Det saknas även ett tydligt ansvar för uppföljning och samordning. Detta medför brister i uppsikten över nämndernas arbete med informationssäkerhet. Risken med otydligt ansvar och bristande uppföljning är att kommunens policys och riktlinjer inte efterlevs, och att skyddsåtgärder genomförs på en ojämn nivå runtom i kommunens verksamheter.

Vi bedömer i stort att kommunstyrelsen har säkerställt en ändamålsenlig incidenthanteringsprocess som är utformad i enlighet med praxis. Dock bedömer vi att prioritering av incidenter inte beaktar informationsklassning och riskanalys i tillräcklig utsträckning.

Baserat på granskningens slutsatser har kommunrevisionens huvudsakliga rekommendationer formulerats inom tre områden:

- Strategi, styrning och organisation
- IT-drift, förändringar samt behörigheter
- Incident-, risk och informationshantering

I granskningsrapporten presenteras detaljerade rekommendationer, nedan framgår revisionens huvudsakliga rekommendationer till kommunstyrelsen.

Strategi, styrning och organisation

- Etablera en långsiktig strategi och tydliga mål för kommunens arbete med informationssäkerhet
- Tydliggöra processer och ansvar för koordinering och uppföljning av kommunens arbete kring informationssäkerhet

- Införa kontinuerliga och anpassade utbildningsinsatser
- Kartlägga samhällsviktiga tjänster och hantera dessa utifrån informationssäkerhet

IT-drift, förändringar samt behörigheter

- Uppdatera processen för IT-förändringar med utgångspunkt i ett enat systemstöd
- Uppdatera processen för borttagande av behörigheter i kommunens informationssystem

Incident-, risk och informationshantering

- Säkerställa att informationssäkerhet är en tydlig del av kommunens risk- och sårbarhetsanalys
- Tydliggöra rutiner för hantering av incidenter relaterade till informationssäkerhet
- Tydliggöra riktlinjer för uppföljning och övervakning av externa leverantörer
- Formalisera rutiner för säkerhetskopieringar och återläsningstester

Revisorerna önskar svar på vilka åtgärder som kommer att vidtas med anledning av vad som framkommit i granskningen och de rekommendationer som lämnas.
Svar önskas senast den 26 februari 2021.

På uppdrag av Lunds kommuns revisorer

_____

Lars Trägen
Ordförande kommunrevisionen
Lunds kommun