David Bogaeus
Informationssäkerhetssamordnare

Yttrande över revisionsrapport – Granskning av informationssäkerhet

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta

att yttra sig över granskningsrapporten i enlighet med kommunkontorets tjänsteskrivelse.

Sammanfattning

EY har på uppdrag av Lunds kommuns förtroendevalda revisorer genomfört en granskning av kommunstyrelsens arbete med informationssäkerhet. Granskningens syfte har varit att bedöma om kommunstyrelsens interna kontroll kopplat till IT- och informationssäkerhet är ändamålsenlig. Granskningen har fokuserat på styrning, organisation och incidenthantering.

Underlag för beslutet

- Kommunkontorets tjänsteskrivelse 2020-02-12 Revisionsrapport – Granskning av informationssäkerhet
- Kommunrevisionens granskningsrapport – Granskning av informationssäkerhet
- Kommunrevisionens missiv till granskningsrapport – Granskning av informationssäkerhet

Ärendet

EY har på uppdrag av Lunds kommuns förtroendevalda revisorer genomfört en granskning av kommunstyrelsens arbete med informationssäkerhet. Granskningens syfte har varit att bedöma om kommunstyrelsens interna kontroll kopplat till IT- och informationssäkerhet är ändamålsenlig. Granskningen har fokuserat på styrning, organisation och incidenthantering.

Granskningen visar att det finns etablerat ett grundläggande ramverk med policy, riktlinjer, mallar och andra dokument som underlättar och tydliggör styrningen av informationssäkerhetsarbetet. Det har dock identifierats brister. Det finns en avsaknad av tydliga kort- och långsiktiga målsättningar för informationssäkerhet. Därutöver saknas en långtgående vision och viljeriktning som är tydligt kopplad till verksamheternas, och kommunens, övergripande strategier.

Revisionen pekar ytterligare på att Lunds kommun har en etablerad struktur med roller och ansvar för informationssäkerhet, men har fortsatt en bit att kvar i att etablera detta i verksamheterna. Det saknas rutiner och riktlinjer som tydliggör och säkerställer genomförande, utvärdering och utveckling av informationssäkerhetsarbetet. Det saknas också en tydlig utbildningsplan för informationssäkerhet.

Vidare framgår av granskning att Lunds kommun har ett grundläggande arbete med operationella rutiner för informationssäkerhetsarbete. Dessa rutiner är i stor utsträckning i linje med riktlinjer och god praxis, men brister har identifierats i bland annat processen för borttagande av behörigheter. Samt att det finns ett behov av att integrera informationssäkerhet som en del av incidenthanteringsprocessen.

Utifrån granskningsresultat rekommenderar Lunds kommuns revisorer kommunstyrelsen att:

- Tydliggöra processer och ansvar för koordinering och uppföljning av kommunens informationssäkerhetsabete
- Införa kontinuerliga och anpassade utbildningsinsatser
- Kartlägga samhällsviktiga tjänster och hantera dessa utifrån informationssäkerhet
- Etablera en långsiktig strategi och tydliga mål för kommunens informationssäkerhetsarbete
- Uppdatera processen för IT-förändringar med utgångspunkt i ett enat systemstöd
- Uppdatera processen för borttagande av behörigheter i kommunens informationssystem
- Säkerställa att informationssäkerhet är en tydlig del av kommunens risk- och sårbarhetsanalys
- Tydliggöra rutiner för hantering av informationssäkerhetsrelaterade incidenter
- Tydliggöra riktlinjer för uppföljning och övervakning av externa leverantörer
- Formalisera rutiner för säkerhetskopieringar och återläsningstester

Föredragning

Kommunkontoret delar revisionens bedömning av förbättringspunkter, men betonar att arbetet med att åtgärda de punkter som rapporten lyfter fram redan är åtgärdat eller under utveckling.

Lunds kommun har en struktur med ett grundläggande arbete med operationella rutiner för informationssäkerhetsarbetet, samt en etablerad struktur med roller och ansvar för informationssäkerhet. Detta är arbete som redan pågår och påvisar den vilja och fokus kommunkontoret har att arbeta med informationssäkerhet.

Målsättningen med informationssäkerhetsarbetet kan beskrivas i tre faser. Fas ett innebär inrättande av resurser t ex informationssäkerhetssamordnare. Fas två innebär en översyn av policy och riktlinjer som reglerar organisationens arbete med informationssäkerhet. Fas tre innefattar arbete med att analysera den nuvarande lägesbilden och hur den svarar upp mot önskad målbild. För att på så vis kunna identifiera handfasta åtgärder och skapa en tydlig vision framåt inom informationssäkerhetsarbetet. Arbetet i del ett är avklarat och där arbetet med fas två har påbörjats.

På kommunkontoret finns två tjänster, en informationssäkerhetssamordnare samt en IT-säkerhetsspecialist, för att tydliggöra processer och arbeta mot att etablera en långsiktig strategi med tydliga mål för kommunens informationssäkerhetsarbete.

Under 2020 genomförde Lunds kommun en upphandling av dataskyddsombud. Från och med den 1 september 2020 levereras därmed rollen som dataskyddsombud som en extern tjänst, istället för att som tidigare utgjort en intern heltidstjänst. Denna förändring är framförallt gjord för att kommunen ska kunna frigöra resurser internt, avseende stöd och rådgivning. Genom förändringen kan kommunen nu avropa dataskyddsombudets stöd i de frågor där det bedöms behövas, medan den interna resursen kan fokusera på att arbeta förebyggande och proaktivt med dataskyddsfrågor. Dataskydd är som bekant en del av informationssäkerhetsarbetet och i och med denna förändring, i kombination med tillsättningen av en informationssäkerhetssamordnare, har ett arbete påbörjats för ett samarbete i dessa frågor utifrån dessa två perspektiv.

Genom dessa två tjänstetillsättningar och upphandlingen av externt dataskyddsombud anser kommunkontoret att man på ett bra sätt svarat upp mot den kritik som rapporten lyfter om ett behov av att kunna ta ett helhetsgrepp på informationssäkerhetsarbetet.

Kommunkontorets ansats har från början varit att komma längre i arbetet. Den pågående pandemin har dock gjort att arbetet har försenats och resurser har istället varit tvungna att fokuseras mot att tackla den komplexa situationen som uppkommit som en följd av krisen. Trots detta fortsätter arbetet kontinuerligt även om tidtabellen har blivit förskjuten något.

Revisionens rekommendationer kommer, tillsammans med granskningsrapporterna från kommunens dataskyddsombud att ligga till grund för kommunens planering av kommande arbete inom såväl dataskydd och personuppgiftshantering som inom information- och IT-säkerhet.

Beredning
Ärendet har beretts av kommunkontoret.

Barnets bästa
En barnkonsekvensanalys har inte bedömts relevant i ärendet.

Ekonomiska konsekvenser
Förslaget medför inga ekonomiska konsekvenser.

Christoffer Nilsson
Kommundirektör

Vesna Casitovski
Kanslichef

Beslutet skickas till
För verkställighet eller motsvarande åtgärd:
Kommunrevisionen

För kännedom:
Kommunkontoret, enheten för trygghet och säkerhet