Kommunstyrelsen

Redovisning av revisionsrapport om informationssäkerhet

Ärende

Med föreliggande ärende beskrivs slutsatserna från revisionsuppdrag om att genomföra en granskning av kommunens informationssäkerhet. Granskningens syfte har varit att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll. Ärendet beskriver även planen för utvecklingen av informationssäkerhetsarbetet i kommunen.

Kommunledningskontorets förslag till beslut

Kommunstyrelsens beslut

Kommunstyrelsen noterar informationen och lägger redovisningen till handlingarna.

Bakgrund

Informationssäkerhet handlar om att förhindra att information läcker ut, förvanskas eller förstörs. Det handlar också om att göra information lättillgänglig när den behövs och för rätt person. Begreppet omfattar information tryckt på papper, lagrad elektroniskt, som överförs per mejl eller post, visas på film eller yttras i en konversation. Den tekniska utvecklingen, och de risker som föreligger på Informationssäkerhets- och IT området förutsätter att arbetet med informationssäkerhet sker kontinuerligt och systematiskt.

Slutsatser från revisionsrapporten

PwC sammanfattande bedömning grundade sig i de revisionsfrågor som ingick i granskningen. Den samlade bedömningen är att Danderyds kommuns kommunstyrelse vid revisionstillfället inte helt säkerställer ett ändamålsenligt informationssäkerhetsarbete och att detta sker med tillräcklig intern kontroll. Detta då kommunstyrelsen inte genomför någon systematisk kravställning och uppföljning av att kommunens verksamheter fullgör sina uppgifter inom informationssäkerhetsområdet. Enligt erhållna intervjusvar sker viss muntlig rapportering om kommunens

informationssäkerhetsarbete av informationssäkerhetssamordnare till kommunstyrelsen, arbetet är däremot inte dokumenterat.

Då kommunstyrelsen är informationsägare och därmed även riskägare är det kommunstyrelsen som måste delegera och säkerställa att riskanalyser genomförs systematiskt och att risker åtgärdas. Idag finns det inte en tillräcklig kontroll och uppföljning av att risker identifieras, varken för kommungemensamma eller verksamhetsspecifika system.

PwC har noterat att IT-enheten inom Danderyds kommun har flera pågående, positiva arbetsinsatser för att förbättra arbetet med IT- och informationssäkerhet. IT-enheten har, trots sin begränsade storlek, ett stort ansvar över många av verksamhetens frågor, ställningstaganden och uppgifter för kommunens leveransförmåga kopplat till den digitala infrastrukturen.

För att optimera informationssäkerhetsarbetet inom kommunen rekommenderar kommunledningskontoret att verksamheten ansvarar för prioriteringar av informationssäkerhetsfrågor. Ansvarsfördelning som beställare och utförare mellan verksamhet och IT-enheten behöver förtydligas för att skapa effektivitet i processer kopplat till IT- och informationssäkerhet och hanteras fördelaktigt genom att införliva, förtydliga och förankra befintlig systemförvaltningsmodell samt inkludera informationssäkerhetsrelaterade aktiviteter till roller som systemägare, systemförvaltare etc.

Kommunledningskontorets slutsatser och plan för fortsatt arbete

Vidtagna åtgärder vid kommunledningskontoret sedan hösten 2022

Sedan oktober 2022 har kommunen bland annat infört en ”SOC-tjänst”, det vill säga en tjänst som analyserar och övervakar cyberhot. Kommunen har även infört en systemförvaltningsmodell och påbörjat ett aktivt dataskyddsarbete för hanteringen av personuppgifter och genomfört ett riskanalysarbete av socialförvaltningens system Treserva samt genomfört grundläggande utbildning i informationssäkerhet för samtliga medarbetare som innehar ett danderydskonto.

Kommunledningskontorets planerade arbete

Kommunledningskontoret avsikt är att fortsätta bedriva informationssäkerhetsarbetet genom att dels utveckla regelverken inom

området dels genom att omhänderta rekommendationer från genomlysningarna av kommunens informationssäkerhetsarbete.

Arbetet kommer under de följande åren att bedrivas löpande under det reguljära informationssäkerhetsarbetet genom inventering, analys av informationstillgångar och informationsprocesser, samt genomförande av riskanalyser för informationssäkerhet. Arbetet ska säkerställa att kommunen och dess förvaltningar har målsättningar och organisation för informationssäkerhet samt att informationsvärdering och informationsklassning genomförs. Kompetensutveckling ska kontinuerligt ske för centrala informationsägare och informationssäkerhetsarbetet ska följas upp och utvärderas. Målsättningen är att samtliga verksamheter bedriver ett aktivt informationssäkerhetsarbete med ledningssystem för Informationssäkerhet och ISO 27 000 som ledstång, har kunskap och tar ansvar som informationsägare och ställer rimliga och korrekta krav på konfidentialitet, riktighet och tillgänglighet.

Konsekvenser för barn och unga

Ett systematiskt informationssäkerhetsarbete innebär inga negativa konsekvenser för barn.

Ekonomiska konsekvenser

Att bedriva ett grundläggande systematiskt informationssäkerhetsarbete innebär inte några större behov av investeringar. Analysarbetet som bedrivs kan dock komma att påverka kraven på it-system och kan innebära behov av investeringar som i dessa fall får redovisas separat.

Johan Lindberg
Kommundirektör

Patrik Hansson
Administrativ chef

Handlingar i ärendet

1. Tjänsteutlåtande, Redovisning av revisionsrapport om informationssäkerhet
2. PwC-rapport, Granskning av informationssäkerhet

Expedieras
Revisorerna