

Granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering

På uppdrag av stadens förtroendevalda revisorer har EY genomfört en granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering. Syftet var att ge en övergripande nulägesanalys om huruvida kommunstyrelsen för Sundbybergs stad har tillsett att arbetet kring informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt.

I granskningen konstateras att den centrala uppföljningen av arbetet med informationssäkerhet utgör ett tydligt förbättringsområde. Brister har identifierat i hur nämnder hanterar bl.a. upphandlingar, avtal med externa leverantörer, utför informationsklassningar, upprättar driftsdokumentation för verksamhets-specifika IT-system, kontinuitetsplanerar och hanterar personuppgifter. Vidare noteras att formella rapporteringsvägar inte definierats mellan stadens koncernbolag och stadsledningskontoret samt den centrala informationssäkerhetsfunktionen. I praktiken innebär det att stadsledningskontoret saknar insyn i hur koncernbolagen arbetar med informationssäkerhet, både som helhet och för viktiga enskilda initiativ såsom informationsklassning, systemförvaltning och arbetet med dataskyddsförordningen.

Vid tiden för granskningen var informationssäkerhetsarbetet begränsat till ett fåtal stadscentrala resurser. En sådan organisationsstruktur bedöms inte vara ändamålsenlig för att bedriva ett tillfredsställande informationssäkerhetsarbete. Det saknas även tillräckliga utbildningsinsatser inom informationssäkerhetsområdet.

Incidenthanteringsprocessen utgörs av detaljerade anvisningar för hur stadens "Service Desk" ska hantera incidenter. Det saknas dock en tydlig beskrivning av tillämpbart processflöde med korrelerande roller, ansvar och rapporteringskrav för kritiska incidenter som riskerar att orsaka mer allvarliga förluster av informationstillgångar.

I syfte att ytterligare stärka stadens interna kontroll rörande informationssäkerhet presenteras i rapporten ett antal rekommendationer. Revisorerna ämnar nogsamtt följa upp kommunens strategiska arbete med informationssäkerhet framöver.

Rapporten överlämnas härmed till kommunstyrelsen. Svar till revisionen önskas senast den 30 juni 2019.

För Sundbybergs stads revisorer


Torbjörn Nylen
Ordförande


HansErik Salomonsson
Vice ordförande