Sundbybergs stad

Stadens revisorer

Svar på revisorernas granskning av stadens arbete med informationssäkerhet

Stadens revisorer har i skrivelse till kommunstyrelsen granskat arbetet med informationssäkerhet och har framställt 13 rekommendationer på åtgärder för att stärka stadens kontroll över och efterlevnad av informationssäkerheten. Eftersom kommunstyrelsen inte själv äger hela ansvaret för alla de rekommendationer som lämnats har stadsmiljö- och tekniska nämnden lämnat svar till revisorerna rörande rekommendationerna 7 – 10. Båda nämnderna träffas av rekommendation 4 varför svar lämnas för respektive nämnd i den delen. Kommunstyrelsen lämnar följande kommentarer som svar på revisionens rekommendationer och övriga bedömningar:

Rekommendation 1: Avsaknad av uppföljning på arbetet med informationssäkerhet i stadens nämnder och förvaltningar.
Revisorerna bedömer att kommunstyrelsen inte har tillsett att det finns formaliserade kontroller och rutiner för stadsledningskontoret att följa upp arbetet med informationssäkerhet i Sundbybergs stads nämnder och förvaltningar. Detta inkluderar bland annat hur verksamheterna sköter upphandlingar, hanterar avtal med externa leverantörer, utför informationsklassningar, upprättar driftsdokumentation för verksamhetsspecifika IT-system, kontinuitetsplanerar och hanterar personuppgifter. Revisorerna rekommenderar att kommunstyrelsen tillser att adekvata kontroller och rutiner för uppföljning och efterlevnad mellan stadsledningskontoret och verksamheterna definieras, samt att designerade informationssäkerhetsroller tas fram och tillsätts i verksamheterna för ökad samverkan med den centrala informationssäkerhetsfunktionen.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. Stadsledningskontoret kommer under 2020 att ta fram rutiner för uppföljning av informationssäkerheten inom hela förvaltningsorganisationen. En viktig komponent i detta uppföljningsarbete kommer bli att sprida kunskapen om hur SKL:s klassificeringsverktyg KLASSA används i identifieringen och riskhanteringen av de informationsmängder som staden behandlar. KLASSA ska användas vid framställningen av förfrågningsunderlag i upphandlingar för att säkerställa att informationssäkerheten omhändertas redan i upphandlingsfasen. Särskild vikt kommer att behöva läggas vid att fastställa hur staden följer upp avtalsefterlevnaden vid hanteringen av informationsmängder åt stadens räkning och vilka sanktionsmöjligheter staden kan inskriva i avtalen vid brott mot

informationssäkerheten som leverantörerna kan göra sig skyldig till. KLASSA ska också ligga till grund för framtida kontinuitetsplanering.

Rekommendation 2: Bristfällig insyn i koncernbolagens informationssäkerhetsarbeten.
Revisorerna bedömer att kommunstyrelsen inte har tillsett att godtagbar uppsikt, i enlighet med Kommunallagen 6 kap. 1 §, i koncernbolagens informationssäkerhetsarbeten kan säkerställas då formella rapporteringskrav till stadsledningskontoret ej har fastställts. Stadsledningskontoret följer inte upp hur koncernbolagen arbetar med informationssäkerhet, varken som helhet eller för viktiga enskilda initiativ såsom informationsklassning, systemförvaltning och dataskyddsförordningsarbete. Insikt saknas även i hur koncernbolagen hanterar information som delas över det gemensamma nätverk som staden och koncernbolagen använder. Revisorerna rekommenderar att kommunstyrelsen tillser att koncernbolagens arbete med informationssäkerhet aktivt följs upp och ökar kraven på återrapportering till stadsledningskontoret, alternativt även inkorporerar bolagen i den övergripande styrmodellen för informationssäkerhet.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning och planerar att se över området under 2020. För att kunna upprätta uppföljning av informationssäkerhetsarbetet inom hela kommunkoncernen behöver ett ledningssystem för informationssäkerhet fastställas. Ledningssystemet ska utgå från informationssäkerhetspolicyn som i sin tur konkretiseras i riktlinjer och rutiner, se vidare rekommendation 4. Av ledningssystemet ska det framgå hur återrapporteringen ska bedrivas och i vilken omfattning. Med ledningssystemet på plats bedömer kommunstyrelsen att uppföljningsarbetet uppfyller den rekommendation som revisorerna lämnat.

Rekommendation 3: Avsaknad av övergripande organisationsstruktur för informationssäkerhet.
Revisorerna bedömer att kommunstyrelsen inte har tillsett att det finns en övergripande struktur för hur Sundbybergs stad skall organisera sig i arbetet med informationssäkerhet, inklusive beskrivningar av roller, relaterade ansvarsområden och kompetensnivåer som är nödvändiga att finnas på stadsledningskontoret och i verksamheterna för att driva arbetet med informationssäkerhet. Revisorerna rekommenderar att kommunstyrelsen tillser att en informationssäkerhetsspecifik organisationsstruktur definieras och beslutas.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning och planerar att se över detta under 2019. Stadsledningskontoret har tagit fram ett förslag på organisering av arbetet med informationssäkerhet. I förslaget beskrivs de roller som stadsledningskontoret bedömer behövs för att kunna tillgodose den bedömning som revisorerna gjort, antalet funktioner som bedöms behövas för att kunna möta de utmaningar och risker som revisorerna identifierat, samt innehållet i de uppdrag som respektive roll förväntas utöva. Förslaget ska förankras i

stadsledningskontorets ledningsgrupp. Arbetet ligger i linje med rekommendation 5 nedan.

Rekommendation 4: Otydlig ansvarsfördelning mellan säkerhetsavdelningen och IT-enheten i arbetet med informationssäkerhet.
Revisorerna bedömer att kommunstyrelsen inte har tillsett att ansvarsfördelningen mellan säkerhetsavdelningens informationssäkerhetsfunktion och IT-enheten tydligt har definierats i arbetet med informationssäkerhet. Formella kravställningar mellan funktionerna har inte utförts och det saknas tydligt ägarskap för vem som skall tillse vad utförs inom ramen för informationssäkerhet. Forumen för samverkan mellan informationssäkerhetsfunktionen och IT-enheten efterlevs inte. Revisorerna rekommenderar att kommunstyrelsen tillser att roller och ansvar mellan stadsledningskontorets informationssäkerhetsfunktion och IT-enhet tydliggörs, samt att regelbundna forum för samverkan kring informationssäkerhetsrelaterade utmaningar och uppföljning av planerade initiativ inrättas.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning att det saknas en tydlig, men också dokumenterad, ansvarsfördelning mellan trygghets- och säkerhetsavdelningen och IT-enheten i arbetet med informationssäkerhet. Trygghets- och säkerhetsavdelningen har under 2018 – 2019 i ett projekt med enheten för digitalisering och service samt IT-enheten inom bolagskoncernen utarbetat ett förslag till riktlinjer för informationssäkerhet som kräver beslut. Dessa riktlinjer kommer ska beredas i stadsdirektörens ledningsgrupp under 2019. Riktlinjerna är indelade i fyra delar, varav den första delen (den som riktar sig mot användarna) är färdigskriven och acceptanstestad i projektgruppen. Trygghets- och säkerhetsavdelningen kommer också under 2019 tillsammans med enheten för digitalisering och service att återuppta arbetet i ett tidigare inrättat forum. Utifrån de övriga delarna i riktlinjerna för informationssäkerhet kommer forumet att utveckla processerna för informationssäkerhet, gränsdragningsfrågorna och ansvarsfördelningen. Trygghets- och säkerhetsavdelningen ska vara tydligt definierad kravställare i informationssäkerhetsfrågorna och enheten för digitalisering och service ska agera professionell rådgivare i desamma.

Rekommendation 5: Informationssäkerhetsarbetet är begränsat till ett fåtal resurser.
Revisorerna finner att Sundbybergs stads centrala informationssäkerhetsarbete är begränsat till de båda nyckelrollerna säkerhetschef och informationssäkerhetssamordnare/dataskyddsombud. Tillgängliga och definierade stödresurser på stadsledningskontoret och i verksamheterna är begränsade. Det saknas även uppföljning av hur många och vilka av stadens IT-system som står utan tillsatta systemägare och systemförvaltare i enlighet med systemförvaltningsmodellen. Revisorerna rekommenderar att kommunstyrelsen tillser att nivån av medvetande och involvering i stadens informationssäkerhetsarbete sprids inom både stadsledningskontoret och i verksamheterna, exempelvis genom formaliserade utbildningsinitiativ, samt att fler

designerade informationssäkerhetsroller tas fram och tillsätts centralt och i verksamheterna.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. Som tidigare nämnts har stadsledningskontoret tagit fram ett organisatoriskt förslag som möter rekommendationen om fler designerade informationssäkerhetsroller. På verksamhetsnivå kommer det under hösten 2019 att inledas en samverkan med designerade informationssäkerhetsombud under ledning av trygghets- och säkerhetsavdelningen i syfte att skapa medvetande och involvering i stadens informationssäkerhetsarbete. Dessa ombud ska bistå sina verksamheter med verksamhetsnära stöd i informationssäkerhetsarbetet, framförallt vad gäller användningen av KLASSA på lokal nivå. De kommer också att bistå dataskyddsombudet i personuppgiftsärenden tillsammans med stadens systemförvaltare.

Rekommendation 6: Begränsade utbildningar och kompetenshöjande initiativ rörande informationssäkerhet.
Revisorerna bedömer att kommunstyrelsen inte har tillsett att stadsövergripande, obligatoriska och regelbundet återkommande utbildningar inom informationssäkerhet genomförs för Sundbybergs stads användare. Ingen uppföljning av tidigare genomförda, enskilda utbildningsinsatser har gjorts och efterlevnad av den användaranvisning för nyttjande av stadens IT-miljö som signeras av nyanställda följs inte upp av informationssäkerhetsfunktionen. Revisorerna rekommenderar att kommunstyrelsen tillser att en utbildningsplan för informationssäkerhet formaliseras. Denna bör innefatta genomförande av obligatoriska och regelbundna utbildningar inom informationssäkerhet med uppföljning av deltagande. Kommunstyrelsen rekommenderas även tillse att kommunikation och signering av användaranvisningen för nyttjande av stadens IT-miljö säkerställs.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. Under 2019/2020 kommer trygghets- och säkerhetsavdelningen att ta fram webbaserade kortutbildningar som stadens samtliga medarbetare ska erbjudas. I detta arbete ingår också att undersöka vilka möjligheter Sundbybergs stad har att knyta tillträdet till stadens IT-system för nyanställda till fullföljandet av obligatoriska webbutbildningar inom området informationssäkerhet.

Rekommendation 11: Passiv lagring av informationssäkerhetspolicy och relaterade anvisningar.
Revisionen konstaterar att Sundbybergs stads informationssäkerhetspolicy och relaterade användaranvisningar lagras passivt på intranätet och förutsätter att användare avsiktligt letar upp informationen. Revisionen rekommenderar att kommunstyrelsen tillser att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till stadens användare med en bestämd frekvens.

Kommentar: Kommunstyrelsen delar revisorernas bedömning att det inte är tillräckligt med enbart passiv information vad gäller informationssäkerheten. Det är dock inte sannolikt att periodiskt återkommande utskick når igenom informationsbruset och leder till förhöjd kunskap eller medvetenhet om informationssäkerheten. Stadsledningskontoret ser därför över olika möjligheter att förbättra informationen kring olika policys, riktlinjer och rutiner av liknande dignitet som informationssäkerhetspolicyn. Det kan handla om riktade informationsinsatser till ansvariga, information vid rekrytering och vid olika förändringar i rutiner och motsvarande. Det finns också stora möjligheter att anhängiggöra informationen i samband med närbesläktad informationsspridning. Det kan också finnas möjligheter att bifoga information (informationsrutor, länkar, etcetera) i de digitala verktyg och system som används för dokument- och informationshantering.

Rekommendation 12: Brist på uppföljning av kontinuitetsplaner för skyddsvärda verksamhetssystem.
Revisionen bedömer att kommunstyrelsen inte har tillsett att central uppföljning från stadsledningskontoret görs för verksamhetssystem med information som har klassats som skyddsvärd för säkerställande att kvalitativ kontinuitetsplanering har genomförts i enlighet med definierad kontinuitetsplaneringsmall. Revisionen rekommenderar att kommunstyrelsen tillser att kontinuitetsplaner utformas för samtliga verksamhetssystem som i genomförd informationsklassning har bedömts som skyddsvärda, samt att samtliga kontinuitetsplaner samlas ihop på stadsledningskontorsnivå för central kvalitetssäkring och koordinering av regelbunden testning av kontinuitetsplanerna.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. Trygghets- och säkerhetsavdelningen har under försommaren 2019 under ledning av enheten för digitalisering och service inlett ett arbete med att identifiera stadens kritiska verksamhetssystem. När modellen för att identifiera dessa är fastställd ska samtliga identifierade system grundligt informationsklassificeras och därefter ska det för varje system upprättas kontinuitetsplaner som löpande ska följas upp och testas.

Rekommendation 13: Avsaknad av fullständig registerförteckning för personuppgifter.
Revisionen bedömer att kommunstyrelsen inte har tillsett att en fullständig och formellt definierad registerförteckning har upprättats över hur personuppgifter behandlas av staden. Revisionen rekommenderar att kommunstyrelsen tillser att en fullständig registerförteckning upprättas.

Kommentar: Kommunstyrelsen instämmer i revisorernas bedömning. Under 2020 kommer registerförteckningen att omarbetas i samarbete med informationssäkerhetsombuden och systemförvaltarna i verksamheterna. Därefter ska förteckningen löpande uppdateras, dock som minst en gång årligen.

På kommunstyrelsens vägnar

Peter Schilling (S)
kommunstyrelsens ordförande