Handläggare
Maria Wedenlid
Telefon: 08-508 11 837

Till
Servicenämnden
2018-12-18

Stadens informationssäkerhetsarbete - projektrapport från Stadsrevisionen

Svar på remiss från kommunstyrelsen

Förvaltningens förslag till beslut

Remissen besvaras med förvaltningens tjänsteutlåtande

Anna-Karin Sandén
t.f. förvaltningschef

Annika Press
Administrativ chef

Sammanfattning

Kommunstyrelsen har begärt yttrande från bland andra servicenämnden angående Stadens informationssäkerhetsarbete - projektrapport från Stadsrevisionen.

Förvaltningen är positiv till granskningen och har fått underlaget för faktagranskning innan ärendet har remitterats inom staden.

Förvaltningen delar revisorernas bedömning att det funnits oklarheter kring ansvarsfördelning och implementering gällande riktlinjerna.

Serviceförvaltningen
Stab

Palmfeltsvägen 5
Box 7005
12107 Stockholm
Telefon 08-508 11 837
maria.wedenlid@stockholm.se
stockholm.se

Bakgrund

Kommunstyrelsen har begärt yttrande från servicenämnden angående Stadens informationssäkerhetsarbete - projektrapport från Stadsrevisionen. Yttrandet ska vara stadsledningskontoret tillhanda senast den 25 januari 2018.

Ärendet

Den kommunala revisionen är fullmäktiges kontrollinstrument för att granska den verksamhet som bedrivs i nämnder och bolag. Stadsrevisionen i Stockholm stad granskar nämnders och styrelsers ansvarstagande för att genomföra verksamheten enligt fullmäktiges uppdrag.

Revisionskontoret har genomfört en granskning för att bedöma om kommunstyrelsens, fastighetsnämndens, servicenämndens och Farsta stadsdelsnämnds styrning, ledning och uppföljning av informationssäkerhetsarbetet är tillräckligt.

Revisorernas bedömning är att staden på en övergripande nivå har relevanta styrdokument i vilka också ansvarsfördelningen för informationssäkerhetsarbetet beskrivs. Granskningen visar emellertid att de förvaltningar som omfattats av granskningen inte tycker att ansvaret i alla delar är tydligt samt att de efterfrågar stöd i hur arbetet ska organiseras och bedrivas.

Revisorerna anser att nämndernas arbete med att säkerställa efterlevnaden av gällande styrdokument behöver utvecklas. Riktlinjerna för informationssäkerhet behöver på ett tydligare och aktivare sätt kommuniceras och implementeras i verksamheterna.

Nämnderna bör också säkerställa att de har fungerande rutiner för att IT-relaterade händelser rapporteras i incidentrapporteringssystemet IA.

Revisorernas sammanfattande bedömning är att stadens arbete avseende styrning, ledning och uppföljning av informationssäkerhetsarbetet behöver utvecklas.

Avslutningsvis lämnar rapporten en del rekommendationer till kommunstyrelsen och två rekommendationer till de granskade nämnderna. De som rör nämnderna är följande:

- Kommunicera och implementera stadens riktlinjer för informationssäkerhet i organisationen.
- Kontrollera efterlevnaden av stadens riktlinjer för informationssäkerhet.

Ärendets beredning

Ärendet har beretts inom staben i samråd med övriga avdelningar.

Förvaltningens synpunkter och förslag

Förvaltningen är positiv till granskningen och har fått underlaget för faktagranskning innan ärendet har remitterats inom staden.

Förvaltningen delar revisorernas bedömning att det funnits oklarheter kring ansvarsfördelning och implementering gällande riktlinjerna.

I rapporten nämns att det inom de nämnder som har granskats saknas tillräcklig kompetens om hur informationssäkerhetsarbetet ska bedrivas. Förvaltningen anser att det även saknats tydliga direktiv på hur arbetet ska bedrivas och med det försvåras nämndens förutsättningar att säkerställa att man har rätt kompetens för uppgiften. Informationssäkerhetslandskapet har förändrats i dagens digitala samhälle. Därför bör kommunstyrelsens direktiv och riktlinjer för arbetet även omfatta hur man ökar medvetenheten hos stadens alla medarbetare.

Tydliga direktiv om incidentrapportering i IA och uppföljning är, som rapporten säger, önskvärt. Förvaltningen vill därutöver påpeka att direktiven om incidentrapportering bör beakta och förtydliga vad datainspektionen säger gällande anmälan av personuppgiftsincidenter. Tidsfristen på 72 timmar enligt GDPR bör förtydligas samt hur relationen mellan de olika typerna av incidentrapportering ser ut. Även om en händelse inte leder till anmälan till datainspektionen så kan den behöva dokumenteras i IA.

Bilagor

1. Stadens informationssäkerhetsarbete, nr 8. Projektrapport från Stadsrevisionen dnr 3.1.3.-79/2018