Datum
2022-01-23

Tjänsteskrivelse

Vår referens
Anton Wikman
Utvecklingssekreterare
anton.wikman@malmo.se

Rapport från revisorskollegiet - Granskning av IT-säkerhet
STK-2021-158

Sammanfattning
Revisorskollegiet har beslutat att kommunstyrelsen ska inkomma med två yttranden med anledning av de iakttagelser och rekommendationer som framgår av stadsrevisionens rapport *Granskning av IT-säkerhet*. Syftet med granskningen var att bedöma om kommunstyrelsen och servicenämnden säkerställer att IT-säkerheten är tillräcklig för att reducera risker för obehörigt intrång. Den slutgiltiga bedömningen var att kommunstyrelsen och servicenämnden endast till viss del säkerställer en tillräcklig IT-säkerhet. Kommunstyrelsens första yttrande skickades till revisorskollegiet den 7 april 2021 och redogjorde för nio åtgärdsområden som styrelsen avsåg att vidta inom informations- och IT-säkerhet. Kommunstyrelsen beslutade att samtliga åtgärder skulle vara genomförda som senast i slutet av 2022. Det andra yttrandet – som behandlas i det här ärendet – är ett uppföljande yttrande med återrapportering av hur arbetet med de åtgärder som tidigare beslutats fortlöpt under 2021.

Sedan den tidpunkt då granskningen genomfördes och kommunstyrelsen översände sitt första yttrande har det skett förändringar i organisation och ansvarsfördelning mellan kommunstyrelsen och servicenämnden. I korthet har förändringen inneburit att det övergripande ansvaret för informationssäkerhetsfrågorna ligger kvar hos kommunstyrelsen medan all IT-styrning, inkluderat IT-säkerhetsfrågorna är överflyttade till servicenämnden.

Detta kompletterande yttrande redogör således för vilka åtgärder kommunstyrelsen vidtagit inom informationssäkerhetsområdet under perioden 2021-04-07 till 2022-01-31 samt redovisar vilka planerade och pågående åtgärder som återstår att genomföra. Samtliga kvarvarande åtgärder planeras i enlighet med kommunstyrelsens första yttrande att vara genomförda som senast i slutet av 2022.

Förslag till beslut
Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta

1. Kommunstyrelsen godkänner förslag till yttrande och skickar yttrandet till revisorskollegiet.

Beslutsunderlag
- Missiv
- Granskning av IT-säkerhet
- Kommunstyrelsens yttrande

- Beslut KS 210407 §124 med Särskilt yttrande (SD)
- Förslag till uppföljande yttrande
- G-Tjänsteskrivelse KSAU 220131 Rapport från Revisorskollegiet- Granskning av IT-säkerhet; uppföljande yttrande

Beslutsplanering
Kommunstyrelsens arbetsutskott 2021-03-29
Kommunstyrelsen 2021-04-07
Kommunstyrelsens arbetsutskott 2022-01-31
Kommunstyrelsen 2022-02-09

Beslutet skickas till
Revisorskollegiet

Ärendet
Revisorskollegiet har beslutat att kommunstyrelsen ska inkomma med två yttranden med anledning av de iakttagelser och rekommendationer som framgår av stadsrevisionens rapport *Granskning av IT-säkerhet*. Syftet med granskningen var att bedöma om kommunstyrelsen och servicenämnden säkerställer att IT-säkerheten är tillräcklig för att reducera risker för obehörigt intrång. Den slutgiltiga bedömningen var att kommunstyrelsen och servicenämnden endast till viss del säkerställer en tillräcklig IT-säkerhet.

Kommunstyrelsens första yttrande till revisorskollegiet
Kommunstyrelsens första yttrande skickades till revisorskollegiet den 7 april 2021 och redogjorde för nio åtgärdsområden som styrelsen avsåg att vidta inom informations- och IT-säkerhet. Kommunstyrelsen beslutade att samtliga åtgärder skulle vara genomförda som senast i slutet av 2022.

Kommunstyrelsens uppföljande yttrande till revisorskollegiet
Sedan den tidpunkt då granskningen genomfördes och kommunstyrelsen översände sitt första yttrande har det skett förändringar i organisation och ansvarsfördelning mellan kommunstyrelsen och servicenämnden. I korthet har förändringen inneburit att det övergripande ansvaret för informationssäkerhetsfrågorna ligger kvar hos kommunstyrelsen medan all IT-styrning, inkluderat IT-säkerhetsfrågorna, är överflyttade till servicenämnden. Revisorskollegiet har därför ombett kommunstyrelsen och servicenämnden att i detta kompletterande yttrande begränsa sina svar till det som ligger inom ramen för nuvarande uppdrag, oavsett om de riktades till någon annan i granskningen.

Utifrån ovanstående bakgrund är stadskontorets bedömning att samtliga av de ursprungliga nio åtgärdsområdena fortfarande faller under styrelsens ansvar i den omfattning de beslutade åtgärderna berör informationssäkerhetsområdet. Detta kompletterande yttrande redogör således för vilka åtgärder kommunstyrelsen vidtagit inom informationssäkerhetsområdet under perioden 2021-04-07 till 2022-01-31 samt vilka planerade och pågående åtgärder som återstår att genomföra. Samtliga kvarvarande åtgärder planeras i enlighet med kommunstyrelsens första yttrande att vara genomförda som senast i slutet av 2022.

Stadskontoret framhåller att eftersom majoriteten av åtgärderna innebär förändringar i styrdokument, processer, rutiner och vägledningar så går det ännu inte att dra några slutsatser rörande

vilka effekter åtgärderna hittills haft i verksamheten.

Sammanställning av stadskontorets åtgärder som redogjorts för i yttrandet

Åtgärd	Planerad	Pågående	Avslutad	Kommentar
Ny riktlinje för informationssäkerhet i Malmö stad.		X		Ärende STK-2021-1717
Kartläggning av resursbehov på stadskontoret avseende informationssäkerhet och dataskydd.		X		Ärende STK-2022-55
Ny metod för uppföljning och aktivitetsplanering		X		Ärende STK-2021-795
Översyn av befintlig trygghets- och säkerhetspolicy.	X			Revidering av befintlig policy ska påbörjas under 2022.
Nulägesuppföljning avseende Malmö stads informationssäkerhetsarbete 2021.			X	Ärende STK-2021-795
Utveckling av befintligt metodstöd för informationsklassificering.			X	Sker löpande vid behov.
Uppgradering av IT-systemet iFacts			X	Fortsatt anpassning och utveckling sker löpande.
Uppdatering av befintlig riskanalysmetod avseende informationssäkerhetsrisker samt utveckling av riskanalysmodul i iFacts.		X		
Integrering av IT- och digitaliseringsavdelningens kravbibliotek i iFacts och anpassning med befintlig klassningsprocess i Malmö stad.		X		
Vägledning avseende klassificering och kravställning i upphandlingsprocessen.			X	
Vägledning vid klassning och kravställning vid personuppgiftsbehandling i tredje land.			X	
Kontinuerlig omvärldsbevakning inom utbildningsområdet avseende informationssäkerhet.			X	Sker löpande vid behov.
Framtagning av underliggande anvisningar till nya riktlinjen.	X			
Behovskartläggning avseende stadsövergripande utbildningsplattform.	X			
Översyn och uppdatering av befintlig process för inrapportering och uppföljning av informationssäkerhetsincidenter.	X			
Definiera begreppen systemägare och systemförvaltare				Uppdraget har övergått till serviceförvaltningen.
Utveckla incidentprocessen för IT-säkerhet				Uppdraget har övergått till serviceförvaltningen.

Ansvariga
Micael Nord Näringslivsdirektör
Magdalena Bondeson Sektionschef
Andreas Norbrant Stadsdirektör