ÖSTERÅKERS KOMMUN
Revisorerna

Kommunstyrelsen (för yttrande)
Kommunfullmäktige (för kännedom)

Granskning av IT -och informationssäkerhet

Vi har låtit genomföra en granskning av om Kommunstyrelsen säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen.

Efter genomförd granskning bedömer vi att Kommunstyrelsen inte helt säkerställt och vidtagit en tillräcklig styrning, uppföljning och kontroll av informations- och cybersäkerhet i kommunen. Granskningen visar bl a att:

- Österåkers kommun har en dedikerad och kunnig teknikgrupp som målinriktat arbetar med samt ansvarar för frågor gällande IT- och informationssäkerhetsområdet i flera dimensioner.
- Det finns beredskapsfunktioner, dels i form av KiB och TiB, men även specifikt för IT- och informationssäkerhet.
- Kommunen har goda, dock informella, rutiner för backup-hantering.
- Kommunen saknar i nuläget till stor del styrande dokumentation, bl.a. återställningsplaner och informationssäkerhetspolicy. Vissa områden har styrande dokumentation, varav mycket inte längre är aktuellt, medan andra områden endast täcks av en digital applikation.
- Det finns inga dokumenterade rutiner för hur utvärderingar och förbättringar förväntas genomföras. Detta sker via informella samtal mellan berörda parter.
- Österåkers kommuns arbete präglas till stor del av manuella och ad hoc-mässiga rutiner, bl.a. vid incidenthantering.

Utifrån genomförd granskning lämnar vi följande rekommendationer till Kommunstyrelsen:

- Dokumentera huvudsakliga informationssäkerhetsprocesser.
- Ta fram en formaliserad Disaster Recovery Plan.
- Formalisera sårbarhetshanteringen med definierade processer för att upptäcka sårbarheter.
- Säkerställ att alla kommunalt anställda regelbundet genomgår utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet.
- Komplettera processkartan för incidenthantering med en tydlig incidenthanteringsplan.
- Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.
- Säkerställ att återföring av lärdomar efter samtliga informationssäkerhetsincidenter görs.

- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.

Rekommendationerna är utvecklade i granskningsrapporten.

Vi översänder revisionsrapporten till Kommunstyrelsen med begäran om yttrande rörande åtgärder utifrån granskningens resultat och rekommendationer. Yttrandet emotses senast den 30 september 2021.

För Österåkers kommuns revisorer, 2021-06-16

Bengt Olin
Ordförande i kommunrevisionen