Ledningens genomgång år 2024 med inriktning 2025-2026

Äldreförvaltningen

Ledningens genomgång
Bilaga 5

Dnr: ALD 2023/204

Kontaktperson: Annamaria Sundbye Feldt / Sanna Bjälevik Chronan

1 Sammanfattning

Informationssäkerhet i Stockholm stad omfattar att följa riktlinjer, gällande lagstiftning och att identifiera sårbarheter och risker. Ledningens genomgång är ett underlag som följer upp äldreförvaltningens arbete med informationssäkerhet. Underlaget ska uppdateras årligen och godkännas av förvaltningsledningen. Det årliga arbetet omfattar att identifiera områden som har behov av utveckling och förbättringar. Syftet är att stärka det löpande arbetet och i samverkan med andra närliggande områden och leverantörer ha god kontroll samt öka kvaliteten inom informationssäkerhet.

Övergripande prioriterade områden för 2024 med inriktning 2025-2026 är följande;

- Informationsklassning
- Utbildning – från ledningsgruppen till chefer och medarbetare
- Leverantörsstyrning
- It-säkerhet
- Incidenthantering
- Uppdaterade tillämpningsanvisningar

Utgångspunkten för det årliga arbetet är budgetmål, politiska prioriteringar, omvärldsläget samt granskning av förvaltningens styrkor och svagheter. Stockholms stads informationssäkerhetsarbete regleras i en tillämpningsanvisning som är en bilaga till stadens Kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Med ett systematiskt arbete och årligen uppdaterat underlag säkrar äldreförvaltningen att informationssäkerhet är ett prioriterat och omhändertaget område.

Utifrån en riskanalys som genomfördes i oktober 2023 föreslås ett antal åtgärder för det fortsatta arbetet för 2024 med inriktning mot 2025-2026.

Innehållsförteckning

1.1 Inledning

Ett systematiskt och riskbaserat informationssäkerhetsarbete utgår från ett ledningssystem för informationssäkerhet, förkortat LIS. Arbetet med LIS i Stockholms stad utgår från den global standarden ISO 27000-serien. Arbetet syftar till att skydda information från att förvanskas, förstöras eller delas med obehöriga som ett led i att säkerställa att verksamheten når sina mål och grundläggande demokratiska principer upprätthålls. Ledningssystemet fungerar som ett ramverk för att säkerställa ändamålsenliga åtgärder som omsätter verksamhetens krav på informationssäkerhet i styrning, processer och aktiviteter.

1.2 Bakgrund

Stockholm stad gör en gemensam kraftsamling inom området informationssäkerhet som en följd av identifierade förbättringsområden som revidering av policys och riktlinjer utifrån lagstiftning, aktuell samhällsutveckling samt i relation till ökning av digitala produkter, tjänster och system.

1.2.1 Omvärldsbevakning – hot, trender och ny lagstiftning

Informationssäkerhetsarbetet påverkas av flera faktorer i omvärlden. Exempel på aspekter som är särskilt viktiga att förstå och förhålla sig till i utformningen av verksamhetens systematiska informationssäkerhetsarbete är säkerhetsläget, återuppbyggnad av totalförsvaret, aktuell lagstiftning och teknikutvecklingen.

För att möta samhällsutvecklingen och ökade krav på informationssäkerhet i samhällsviktig verksamhet genomförs förändringen i NIS-direktivet. Direktivet är under utredning för att kunna genomföras med anpassningar i svensk rätt. Förslag på svensk tillämpning redovisas i februari 2024.

Inom dataskyddsområdet har ett nytt EU-beslut om skydd av personuppgifter som hanteras av USA-ägda leverantörer skapat juridiska förutsättningar för att föra över personuppgifter till amerikanska molnleverantörer som anslutit sig till villkoren i avtalet. I ett längre perspektiv är rättsläget fortsatt osäkert. Det är till exempel oklart om avtalet mellan USA och EU klarar en prövning i EU-domstolen.

Sammantaget pekar utvecklingen i omvärlden på att ett välfungerande systematiskt och riskbaserat informationssäkerhetsarbete är fortsatt viktigt.

1.2.2 Process och beslut

Ledningens genomgång är ett årligen återkommande underlag. Inhämtning av identifierade åtgärder och framtagande av ledningens genomgång genomförs av medarbetare med ansvar för informationssäkerhet inom äldreförvaltningen. I arbetet ska samverkan ske med förvaltningens dataskyddsombud (DSO) samt andra relevanta nyckelpersoner. Identifiering av åtgärder samt uppföljning av föregående års underlag genomförs under perioden augusti-september. Framskrivning sker under oktober där budgetpresentationen ska beaktas i relation till underlaget. Ledningens genomgång lämnas vidare till skribenter för arbetet med att framställa den årliga verksamhetsplanen för äldreförvaltningen. Ledningens genomgång överlämnas som bilaga till verksamhetsplanen och beslutas av förvaltningsledningen under november. Äldreförvaltningens verksamhetsplan med bilagor godkänns av äldrenämnden.

1.2.3 Resultat från risk- och sårbarhetsanalys (RSA) och GDPR-årsrapport.

Resultatet från analyser i närliggande områden är viktiga ingångsvärden för att identifiera vilka åtgärder som är relevanta i det fortsatta informationssäkerhetsarbetet. I verksamhetens Risk- och sårbarhetsanalys (RSA) är hot mot informationssäkerhet identifierad som en risk för att säkerställa robusthet och kontinuitet i förvaltningens samhällsviktiga verksamhet. I uppföljningen av dataskyddsarbetet framgår vikten av informationsklassningar och en systematisk kring att säkerställa ett anpassat dataskydd över tid.

1.2.4 Resultat från Väsentlighets- och riskanalys (VoR)

Under arbetet med Väsentlighets- och riskanalys för 2024 identifierades två risker för det systematiska informationssäkerhetsarbetet. Det handlar om risk för bristande informationssäkerhet så att information att inte är tillgänglig när den behövs, alternativt inte går att lita på att den är korrekt eller hanteras felaktigt så att obehöriga kan ta del av den. Därutöver beskrivs risken för bristande kontinuitet i det systematiska informationssäkerhetsarbetet med risken att incidenter inte upptäcks och hanteras i tid som möjlig konsekvens.

1.3 Åtgärder som föreslås för äldreförvaltningens LIS

Åtgärder presenteras i en prioriterad ordningsföljd som är identifierade i arbetet med framtagande av första versionen av Ledningens genomgång 2024 med inriktning 2025-2026. Prioriteringarna kan omfördelas under 2024 beroende på framkomna behov och fynd under arbetet med informationssäkerhet. Ändringar i prioriteringar godkänns av förvaltningsledningen.

1.3.1 2024

Genomföra inventering och informationsklassning, upprätta registerförteckning

1. Upprätta en registerförteckning för informationshantering, klassningar och årliga processer.
2. Inventera verksamhetsprocesser och system som innebär informationshantering.
3. Etablera ett årshjul som möjliggör planering över tid. Fokus för 2024 års klassningsarbete är verksamhetsprocesser som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter.

Utbildning till chefer

4. Genomföra obligatorisk e-utbildning som lanseras under 2024. Åtta avsnitt under våren om 5-10 minuter som genomförs enskilt.

Utbildning till medarbetare

5. Genomföra obligatorisk e-utbildning som lanseras under 2024. Åtta avsnitt om 5-10 minuter som genomförs i grupp.

Delta i normerande klassningar

6. Delta i normerande klassningar i samarbete med objektförvaltningen för de system som berörs av NIS-direktivet utifrån hälso- och sjukvård. Förutsätter att verksamhetsrepresentanter deltar.

Uppdatera Lokal anvisning

7. Se över och uppdatera lokal anvisning för att säkerställa ändamålsenlig styrning av informationssäkerhetsarbetet.

1.3.2 2025

Genomföra inventering och informationsklassning, uppdatering av registerförteckning

1. Uppdatera inventering av verksamhetsprocesser och system som innebär informationshantering
2. Uppdatera informationsklassning
3. Uppföljning av upprättad registerförteckning.

Fokus för 2025 års arbete är verksamhetsprocesser som träffas av NIS-direktivet.

4. **Följa upp utbildningsinsatser för chefer och medarbetare**

Uppdatera rutin för incidenthantering

5. Säkerställ anpassning till nytt arbetssätt och verktygsstöd när det lanseras.

Översyn av leverantörsrelationer

6. Inventera och bedöm avtal med externa parter som är involverade i att hantera verksamhetens information.

Uppdatera Lokal anvisning

7. Se över och uppdatera lokal anvisning för att säkerställa ändamålsenlig styrning av informationssäkerhetsarbetet.

1.3.3 2026

Inventering och informationsklassning samt uppdatera registerförteckning

1. Uppdatera inventering av verksamhetsprocesser och system som innebär informationshantering samt uppdatera informationsklassning. Fokus för 2025 års arbete är verksamhetsprocesser som identifierats som verksamhetskritiska i RSA-arbetet.

Uppdatera Lokal anvisning

2. Se över och uppdatera lokal anvisning för att säkerställa ändamålsenlig styrning av informationssäkerhetsarbetet.