Ledningens genomgång år 2026 med inriktning 2027-2028

Äldrenämnden

Bilaga 6 till VP 2026

Ledningens genomgång

Dnr: ALD 2025/92

Kontaktperson: Henrik Adestedt

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. Det skärpta omvärldsläget och den snabba tekniska utvecklingen gör att verksamheter ständigt ställs inför stora utmaningar att hänga med. Därför är ett systematiskt arbete en grundförutsättning för god kontroll.

Övergripande prioriterade områden för 2026 med inriktning 2027-2028 är följande;

- Införande av Cybersäkerhetslagen.
- Uppdatera rutin för incidenthantering och kontinuitet samt rapportering till tillsynsmyndighet.
- Kompetenshöjande insatser samt analys av resultatet.
- Kartläggning av behörighetshantering och mappstruktur på gemensamma mappar.
- Etablera systemstöd kopplat till informationssäkerhet

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 samlad analys som genomförts utifrån risk- och sårbarhetsanalys (RSA) och väsentlighet och riskanalys (VOR), aktuella incidenter, lagförändringar, lokala rutiner och löpande arbete under 2025 föreslås ett antal åtgärder för det fortsatta arbetet för 2026 med inriktning mot 2027-2028.

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

Informationssäkerhetsarbetet behöver följa aktuell samhällsutveckling och anpassas i relation till teknikutveckling, förändrad lagstiftning och aktuell hotbild.

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 kritiska delar av samhället har arbetet med införandet utav NIS2- och CER-direktivet i svensk rätt kommit vidare för att införa nya regler för cybersäkerhet. Den 14 oktober lämnas lagrådsremissen till Regeringen och Cybersäkerhetslagen beräknas träda i kraft 15 januari 2026. Bedömningen är att äldreförvaltningen träffas av kraven i båda direktiven.

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. Det innebär att det idag finns mekanismer på plats som gör det möjligt att anlita leverantörer som uppfyller EU:s krav för överföring av personuppgifter till USA. Den personuppgiftsansvariga måste emellertid även fortsättningsvis säkerställa att lämpliga ”överföringsmekanismer” finns på plats oavsett om det är till USA eller andra länder utanför EU/EES

området. I samband med beslut om amerikanska leverantörer behöver också en exitplan beaktas om mekanismerna skulle förändras.

I och med Brexit upprättades ett adekvantsbeslut som gör att överföring av uppgifter till engelska bolag fortsatt var kvar på samma skyddsnivå. Detta beslut faller 27 december 2025 och inget nytt beslut är fattat från EU, ännu.

Sammantaget pekar utvecklingen i omvärlden och aktuella händelser under året på att ett välfungerande systematiskt och riskbaserat informationssäkerhetsarbete är fortsatt viktigt. Dessutom ökar kraven på verksamheterna för att upprätthålla en adekvat skyddsnivå.

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 DSOs-årsrapport.

Resultatet från analyser i angränsande 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. Alla risker förutsätter en ökad kompetens för att möjliggöra ett arbete i syfte att minska riskerna. Föreslagna åtgärder i dataskyddsombudets årsrapport från 2025 sammanfaller tillsammans med övriga måldokument inom staden.

1.2.4 Resultat från Väsentlighets- och riskanalys (VoR)

Under arbetet med Väsentlighets- och riskanalys för 2026 identifierades flera risker för det systematiska informationssäkerhetsarbetet. Det handlar om behörighetshanteringen som behöver kartläggas för att identifiera behov av förändrade arbetssätt. Aktuella incidenter i kombination med kommande lagar kommer innebära behov av justeringar i incidenthanteringen samt upprätta rutiner för rapportering till tillsynsmyndighet. Det är också ett tydligt mål att klassningsarbetets vikt behöver stärkas och att informationssäkerheten vid upphandlingar säkerställs.

1.2.5 Resultat från riskanalys av Äldreförvaltningens verksamhetsövergripande informationssäkerhetsarbetet

Genom en analys av styrkor och svagheter i Äldreförvaltningen systematiska informationssäkerhetsarbetet identifierades följande risker:

• Risk att arbete med informationssäkerhet försvåras på grund av utvecklingstakten inom området. Det leder till utmaning inom kompetens hos förvaltningens medarbetare.
• Risk för bristande regelefterlevnad mot skärpta krav i NIS2/CER och kommande Cybersäkerhetslagen.
• Risk att känslig information inte skyddas vid kommunikation på grund av bristande användning av tillgängliga tjänster.
• Risk för onödig spridning av uppgifter på grund av brister i behörighetsstyrning.
• Risk att incidenter, där roll och ansvarsfördelningen är otydlig, leder till felaktig hantering, till exempel personuppgiftsansvar och personuppgiftsbiträden.
• Risk för avsaknad av eller eftersläpning i lokal styrning på grund av att operativt arbete prioriteras.
• Risk för att åtgärder och aktiviteter inte genomförs på grund av låg prioritet mot kärnuppdrag.

1.3 Åtgärder som föreslås för Äldreförvaltningens LIS

1.3.1 2026

Efterlevnad av Cybersäkerhetslagen

- Kompetenshöjande insatser för hela förvaltningen.

- Säkerställa leverantörskedjor vid upphandling och gällande avtal.
- Uppdatera rutiner och resurser för behörigheter, incidenthantering och rapportering till tillsynsmyndighet

Uppdatera rutin för incidenthantering och kontinuitet

- Fortsatt arbete med säkerställande av roller och ansvar inom avtalsområden gällande dataskydd. Upprättande av instruktioner och avtal vid behov.
- Uppdatera rutiner och resurser för behörigheter, incidenthantering och rapportering till tillsynsmyndighet

Kompetenshöjande insatser på hela förvaltningen inom informationssäkerhet

- Uppdatera den nya obligatoriska e-utbildningen inom informationssäkerhet för alla medarbetare på Äldreförvaltningen.
- Genomföra utbildningar inom informationssäkerhet, riskmedvetenhet och ansvar för alla enheter på Äldreförvaltningen.
- Analysera kompetensbehovet och föreslå ytterligare insatser.

Behörighetshantering

- Kartläggning av behörighetshanteringen inom Äldreförvaltningen.
- Påbörja arbetet med roller och ansvar för mappstruktur på gemensamma lagringsytor.

Etablera systemstöd kopplat till informationssäkerhet

- Påbörja införandet utav tjänsten Säkra meddelanden på verksamheter inom Äldreförvaltningen.
- Äldreförvaltningen är en pilotverksamhet i införandet av Säker Digital Kommunikation (SDK) i Stockholms Stad och förbereder verksamheten för ett första införande under året 2026.
- Äldreförvaltningen kommer också utreda möjligheten för verksamheterna att börja använda Digital post för digitala utskick mot exempelvis privatpersoner.
- Införandet av elektroniska underskrifter och validering för förvaltningen analyseras och föreslås.

1.3.2 2027 - 2028

Efterlevnad av Cybersäkerhetslagen

- I och med att lagen ännu inte finns är det svårt att exakt veta vad som kommer ställas för krav. Därför behövs efterlevnaden av lagen utredas och analyseras.

Följa upp kompetenshöjande insatser på Äldreförvaltningen

- Kartlägga och analysera behovet av fortsatta insatser.

Behörighetshantering

- Genomföra föreslagna åtgärder inom behörighetshanteringen
- fortsatt arbetet med roller och ansvar för mappstruktur på gemensamma lagringsytor.

Etablera systemstöd kopplat till informationssäkerhet

- Fortsatt arbete med införande av tjänster på Äldreförvaltningen.

Översyn av leverantörsrelationer

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

Uppdatera Lokal anvisning

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