Ledningens genomgång år 2026

Socialförvaltningen

Beslutad 2025-12-09

Ledningens genomgång

Dnr: SOF 2025/798

Kontaktperson: Morgan Lindengren

Sammanfattning

För att nå stadens mål om en modern, hållbar och innovativ storstad ska ett systematiskt informationssäkerhets- och dataskyddsarbete drivas inom nämnder och styrelser.

Förvaltningschef leder och styr arbetet med informationssäkerhet inom den egna verksamheten. Enligt stadens tillämpningsanvisningar till riktlinje för informationssäkerhet[1]
anges att *Ledningens genomgång* ska genomföras årligen, i enlighet med den internationella standarden SS-ISO/IEC 27001.

Nämnden ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna kontrollarbetet. Identifierade aktiviteter redovisas både i följande rapport samt i nämndens verksamhetsplan under mål 3.5. Förbättringar som föreslås för verksamhetens Ledningssystem för informationssäkerhet (LIS) presenteras i kapitel 3, i en prioriterad ordningsföljd identifierad i arbetet med framtagandet av första versionen av *Ledningens genomgång* 2026 med inriktning 2027–2028. För 2026 är det följande:

- Uppdatera *Lokal anvisning för informationssäkerhet*
- Utveckla arbetet med att registrera personuppgiftsbehandlingar enligt GDPR
- Utreda förvaltningens hantering av skyddade personuppgifter

[1] Stadens tillämpningsanvisningar till riktlinje för informationssäkerhet

Innehållsförteckning

1. Vad är Ledningens genomgång?

Ledningens genomgång innebär en genomlysning av informationssäkerhetsarbetet inom verksamheten och ska resultera i beslut om förbättringar inför nästkommande verksamhetsår. Rapporteringen ska även innefatta dataskydd utifrån vad som framkommer i GDPR-årsrapport, som årligen sammanställs av dataskyddsombudets för nämndens/styrelsens räkning.

1.2 Faktorer som påverkar verksamhetens LIS

Ledningssystem för informationssäkerhet (LIS) utgår från ISO standard 27001. Standarden är global och stödjer organisationer, förvaltningar och bolag att skydda känslig information från risker och hot. Socialnämnden ska ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att nämnden ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering.

1.2.1 Omvärldsbevakning – hot, trender och ny lagstiftning

Informationssäkerhetsområdet påverkas av flera faktorer i omvärlden. Exempelvis innebär det oroliga världsläget till en ökning av cyberangrepp och inom lagstiftningsområdet sker snabba förändringar som påverkar informationssäkerhetsarbetet. Därmed krävs ett aktivt arbete med att säkerställa korrekt skydd för nämndens informationsmängder och att samtliga medarbetare har en grundläggande kompetens inom informationssäkerhet.

Ökade krav på informationssäkerhet inom samhällsviktig verksamhet kom under 2024 i form av förändringar i EU-direktivet *The Directive on security of Network & Information Systems*, förkortat NIS-direktivet. Förslaget, som kallas NIS2, redovisades i februari 2024. Den svenska anpassningen av förslaget, formulerat som en ny lag – cybersäkerhetslagen – väntades träda i kraft 1 januari 2025. Arbetet med att införliva lagen har dock skjutits upp och väntas nu istället träda i kraft den 15 januari 2026.

1.2.2 Vad händer inom staden – budget, inriktningar, lokala förändringar eller satsningar

Under året har tjänsten Säkra meddelanden lanserats vid förvaltningen. Säkra meddelanden är Stockholms stads val av tjänst för kommunikation av extra skyddsvärd eller känslig information, och fastän tjänsten tidigare funnits tillgänglig för alla stadens medarbetare, har den vid förvaltningen endast använts i liten utsträckning. Genom pilotprojekt, framtagandet av en rutin och flertalet utbildningar har användandet av tjänsten nu förankrats bland förvaltningens verksamheter. Ett utvärderingsarbete planeras genomföras under hösten.

1.2.3 Vad har verksamheten identifierat i RSA-arbetet

I RSA identifieras främst risken för brist i rutiner och bristande efterlevnad av rutiner i anslutning till den oönskade händelsen som är att personal har felaktig behörighet och får del av känslig information via gruppdiskar, mappar och samarbetsytor. Åtgärd föreslås i VoR.

1.2.4 Resultatet från egen uppföljning (VoR och IKP)

Arbetssätt	Oönskad händelse	Sannolikhet	Konsekvens	Riskvärde	Åtgärd
Behörighetshantering	Personal har felaktig behörighet och får del av känslig information - Agresso och Lisa självservice	3. Möjlig	2. Lindrig	6	-
	Personal har felaktig behörighet och får del av känslig information - gruppdiskar, mappar, samarbetsytor	4. Sannolikt	3. Kännbar	12	Säkerställ kunskap om och att rutin för behörighetshantering är känd och följs
	Personal har felaktig behörighet och får del av känslig information - Platina	2. Mindre sannolikt	4. Allvarlig	8	-
	Personal har felaktig behörighet och får del av känslig information - Platina	2. Mindre sannolikt	4. Allvarlig	8	-

Arbetssätt	Oönskad händelse	Sannolikhet	Konsekvens	Riskvärde	Åtgärd
Implementering av lokal anvisning	Den lokala anvisningen för informationssäkerhet är inte känd eller följs inte	3. Möjlig	3. Kännbar	9	Säkerställ att den lokala anvisningen för informationssäkerhet är känd och tillämpas inom hela förvaltningen. **Beskrivning** - Information vid introduktion av nyanställda - Information årligen vid APT
Incidenthantering	Incidenter hanteras inte enligt riktlinjer och lagkrav	3. Möjlig	4. Allvarlig	12	Kontroll av att lokal rutin för incidenthantering finns tillgäng och följs
Informationsklassning	Känslig information skyddas inte på rätt sätt och riskerar att spridas till icke behöriga personer	2. Mindre sannolikt	4. Allvarlig	8	Dataskyddsombudets årsrapport inkluderar kontroll av informationsklassning Säkerställa att chefer inom förvaltningen har tillräcklig kunskap om informationsklassning och tillämpar den inom sina verksamheter **Beskrivning** - Chefer inom förvaltningen identifierar behov av informationsklassning och tar stöd av EDV (sic; nytt enhetsnamn Område digitalisering och it, ODI)
Informationssäkerhet inom upphandlingsförfarande	Rätt krav gällande informationssäkerhet ställs inte vid anskaffning och utveckling av varor och tjänster, vilket gör att informationen inte får rätt skydd	2. Mindre sannolikt	4. Allvarlig	8	Kontroll av att upphandlingsstrategi avseende informatonssäkerhet har beaktats i alla upphandlingar

1.2.5 Resultatet från revisioner

Inga aktuella resultat från revisioner finns att redovisa.

1.2.6 Risker som identifierats i GDPR-årsrapport

I GDPR-årsrapport för 2024 lyfts framförallt ett område där förvaltningen brister i sitt dataskyddsarbete. Detta är:

- **Konsekvensbedömning.** Förvaltningens dataskyddsombud (DSO) bedömer att förvaltningens befintliga konsekvensbedömningar av personuppgiftsbehandlingar behöver ha en tydligare koppling till de behandlingar de berör.

Under hösten 2025 inleds en kartläggning över de av förvaltningens personuppgiftsbehandlingar som bedöms medföra en så pass hög risk för de registrerades fri- och rättigheter att konsekvensbedömning blir aktuellt. Kartläggningen utgår inledningsvis från de personuppgiftsbehandlingar som registrerats under 2025. Arbetet väntas fortgå under 2026, dock med reservation för att GDPR-årsrapport för 2025 kan komma att lyfta andra fokusområden.

1.2.7 Information om avvikelser (incidenter och andra händelser)

Miljödata-incidenten. Den 25 augusti informerades Stockholms stad av systemleverantören Miljödata om att deras it-miljöer utsatts för ett cyberangrepp. Staden hade vid tidpunkten inget driftsatt system hos Miljödata men en testmiljö för systemet Stella som testats som nytt system för arbetsmiljöincidenter. Staden anmälde incidenten till Integritetsskyddsmyndigheten (IMY) och till polisen, som inledde en förundersökning om dataintrång.

Den 2 september kom besked från Miljödata om att hotaktören kommit åt information i samband med attacken. Den röjda informationen uppgavs innefatta personuppgifter för samtliga månadsanställda och timanställda vid stadens förvaltningar, inklusive personer med skyddade uppgifter.

Förvaltningen anmälde personuppgiftsincidenten till IMY den 27 augusti och kompletterade anmälan den 16 september. I samband med incidenten aktiverades förvaltningens krisledning för att, i löpande samråd med Stadsledningskontoret, vidta nödvändiga

åtgärder med att, bland annat, informera registrerade och hantera de risker som incidenten innebar. Krisledningen avvecklades den 1 oktober.

Övriga incidenter. De övriga personuppgifts- eller informationssäkerhetsincidenter som inträffat vid förvaltningen har varit av mindre allvarlig grad och hanterats lokalt.

1.3 Förbättringar som föreslås för verksamhetens

Uppdatera *Lokal anvisning för informationssäkerhet*

Förvaltningens styrdokument *Lokal anvisning för informationssäkerhet* revideras årligen och uppdateras vid behov, exempelvis vid förändringar i verksamhetens systematiska informationssäkerhetsarbete eller dataskyddsorganisation.

Utveckla arbetet med registrering av personuppgiftsbehandlingar enligt GDPR

Under hösten 2024/våren 2025 inleddes vid förvaltningen ett omfattande arbete med att registrera personuppgiftsbehandlingar i verktyget Draftit. Det fastställda arbetssättet – att registrera enligt processer i förvaltningens klassificeringsstruktur – har visat sig mer gångbart för vissa verksamheter och utmanande för andra, beroende på verksamhetens karaktär. Ett förslag för 2026 är därför att utvärdera, utveckla och vid behov förändra arbetssättet i syfte att underlätta arbetet för berörda medarbetare. Syftet med detta är både att öka antalet genomförda registreringar och fördjupa medarbetarnas kunskap om hur lagkraven i GDPR knyter an till de egna verksamheterna.

Utreda förvaltningens hantering av skyddade personuppgifter

I samråd med förvaltningens DSO konstateras ett behov av tydligare riktlinjer och rutiner för hanteringen av skyddade personuppgifter. Ett arbete med detta har inletts, och för 2026 föreslås att arbetet fortgår för att säkerställa en korrekt och rättssäker hantering av uppgifterna i fråga.