Ledningens genomgång år 2025

Socialförvaltningen

Beslutad 2024-12-10

Ledningens genomgång
Bilaga till socialnämndens verksamhetsplan 2025

Dnr. SOF 2024/667

Kontaktpersoner:
Christina Ring, områdeschef Enheten för digitalt verksamhetsstöd (EDV), christina.ring@stockholm.se
Morgan Lindengren, informationssäkerhetssamordnare (ISAM), morgan.lindengren@stockholm.se

1 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.

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.

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* 2025 med inriktning 2026-2027. För 2025 är det följande:

- Genomföra inventering och informationsklassning samt upprätta registerförteckning
- Implementering av obligatoriska arbetssätt i Integrerat ledningssystem (ILS)
- Utbildningar för chefer och medarbetare
- Struktur för samarbete inom informationssäkerhet och dataskydd
- Uppdatera lokal anvisning

[1] Tillämpningsanvisningar till riktlinje för informationssäkerhet

Innehållsförteckning

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.

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 har under 2024 kommit 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 och därefter har ett arbete påbörjats med att anpassa förslaget till svensk lag. Ett resultat av detta är cybersäkerhetslagen, en ny lag som väntas träda i kraft 1 januari 2025.

Inom nämndens ansvarsområde omfattas idag hälso- och sjukvård av NIS. I samband med förändringen kan ytterligare områden komma att omfattas.

2.2 Identifierat i RSA, DSO-årsrapport samt VoR

Risker i Risk- och sårbarhetsanalys (RSA)

I förvaltningens RSA finns en risk kopplad till informationssäkerhet formulerad: *Brister i informationssäkerhet med konsekvensen att sekretessbelagda uppgifter går att komma åt för allmänheten.* Befintlig åtgärd är, enligt RSA, utbildning i informationssäkerhet för chefer och medarbetare, vilket syftar till att höja verksamhetens förmåga att hantera information på ett säkert och korrekt sätt.

Förbättringsområden i dataskyddsombudets (DSO) årsrapport

I DSO-årsrapport för 2023 lyfts framförallt två områden där förvaltningen brister i sitt dataskyddsarbete. Dessa är:

- **Registerförteckningen.** Förvaltningen ska ta fram och underhålla ett register över personuppgiftsbehandlingar med hjälp av verktyget Draftit Privacy Records. Denna förteckning bedöms i dagsläget som ofullständig av DSO. Detta åtgärdas genom att prioritera arbetet med att registrera personuppgiftsbehandlingar, exempelvis via workshops och utbildningar i hur Draftit Privacy Records kan nyttjas.

- **Konsekvensbedömning.** DSO bedömer att förvaltningens befintliga konsekvensbedömningar av personuppgiftsbehandlingar behöver ha en tydligare koppling till de behandlingar de berör. Också detta åtgärdas genom att prioritera arbetsuppgifter knutna till registrering av personuppgiftsbehandlingar.

Under 2024 har ett arbete inletts för att åtgärda dessa brister. Arbetet väntas fortgå under 2025, dock med reservation för att DSO-årsrapport för 2024 kan komma att lyfta andra fokusområden.

Risker i Väsentlighets- och riskanalys (VoR) 2025 under mål 3.5, process *Systematiskt informationssäkerhetsarbete*

Arbetssätt	Oönskad händelse	Sannolikhet	Konsekvens	Riskvärde	Åtgärd
Behörighetshantering	Personal har felaktig behörighet och får del av känslig information – Agresso och Lisa självservice	2. Mindre sannolikt	3. Kännbar	6	Behövs ej vid riskvärde under 9
	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	Säkerställ kunskap om och att rutin för behörighetshantering är känd och följs
	Personal har felaktig behörighet och får del av känslig information – Sociala system	2. Mindre sannolikt	4. Allvarlig	8	Säkerställ kunskap om och att rutin för behörighetshantering är känd och följs
Implementering av lokal anvisning	Den lokala anvisningen för informationssäkerhet är inte känd eller följs inte	3. Möjlig	3. Kännbar	9	Säkerställa att den lokala anvisningen för informationssäkerhet är känd och tillämpas inom hela förvaltningen
	Bristande kunskap om och följsamhet mot stadens riktlinje för informationssäkerhet, vilket kan leda till brister i informationshantering/incidenter	3. Möjlig	3. Kännbar	9	Kontroll av att medarbetare årligen genomför stadens e-utbildningar inom informationssäkerhet och dataskydd
Incidenthantering	Incidenter hanteras inte enligt riktlinjer och lagkrav	3. Möjlig	4. Allvarlig	12	Kontroll av att lokal rutin för incident-hantering finns 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

Informationssäkerhet inom upphandlings-förfarande	Rätt krav gällande informationssäkerhet ställs inte vid anskaffning och utveckling av varor och tjänster, vilket gör att information inte får rätt skydd	2. Mindre sannolikt	4. Allvarlig	8	Kontroll av upphandlingsstrategi avseende informationssäkerhet har beaktats i alla upphandlingar

3 Förbättringar som föreslås för verksamhetens LIS

I *Ledningens genomgång* ska en genomlysning av förvaltningens egen LIS genomföras. Syftet är inte att kontrollera om exempelvis en viss rutin finns på plats, utan att säkerställa att syftet med rutinen uppnås. Exempelvis avseende incidenthantering analyseras frågan om incidenter som uppstår i verksamheten rapporteras. Om rapportering inte sker ska en analys av varför genomföras och förslag på förbättringar för att öka anmälningsfrekvensen ska tas fram.

Förbättringsåtgärder presenteras i en prioriterad ordningsföljd identifierad i arbetet med framtagandet av *Ledningens genomgång* 2025 med inriktning 2026-2027. Inventering och informationsklassning är grunden i informationssäkerhetsarbetet och för 2024 har arbete kopplat till registerförteckning och informationsklassning särskilt prioriterats för hela staden. Prioriteringarna kan omfördelas under 2025 om ändrade förutsättningar uppstår i informationssäkerhetsarbetet, vilka beslutas av förvaltningsledningen.

3.1 2025

Styrning och uppföljning

- Under året fortsätter nämnden arbetet med att implementera styrningen av informationssäkerhetsarbetet i stadens integrerade system för ledning och styrning (ILS). Som ett led i detta ingår utbildning och stödmaterial till chefer inom organisationen.
- Årlig uppföljning av *Ledningens genomgång*.

Genomföra inventering och informationsklassning samt utveckla registerförteckning

- Inventering av nämndens information med prioritering av informationsmängder som innehåller integritetskänsliga och känsliga personuppgifter alternativt omfattas av NIS. Hit hör även förberedelser inför NIS2 med hänsyn till de förändringar som potentiellt kommer att påverka detta arbetsområde.
- Fortsätta arbetet med upprättandet av registerförteckning och säkerställa korrekt hantering enligt gällande regelverk i dataskyddsförordningen.
- Säkerställa planering och genomförande av informationssäkerhetsklassning med tillhörande aktiviteter enligt stadens process.

Implementering av obligatoriska arbetssätt i ILS

- Genom ILS ges aktuella verksamheter tillgång till de obligatoriska arbetssätten avseende informationssäkerhet.
- I ILS anges också de obligatoriska arbetssätten för systematiskt informationssäkerhetsarbete inom de prioriterade områdena behörighetshantering, implementering av lokal anvisning, incidenthantering, informationsklassning och informationssäkerhet vid upphandlingsförfarande.

Utbildningar för chefer och medarbetare

- Genomföra obligatoriska utbildningar i informationssäkerhet och dataskydd. Genomförs årligen.

Struktur för samarbete inom informationssäkerhet och dataskydd

- Fortsätta samarbetet inom den under 2024 etablerade arbetsgruppen av representanter för nyckelkompetenser inom informationssäkerhet. Detta i syfte att utveckla och följa upp det operativa arbetet med informationssäkerhet och dataskydd.

Uppdatera lokal anvisning för informationssäkerhet

- Se över och uppdatera lokal anvisning för att säkerställa ändamålsenlig styrning av informationssäkerhetsarbetet. Genomförs årligen.
- Tydliggöra årshjul för informationssäkerhetsarbete och uppföljning i samarbete med stadsledningskontoret.

3.2 2026

Genomföra inventering och informationsklassning, uppdatering av registerförteckning

- Uppdatera inventering av nämndens information
- Uppföljning av upprättad registerförteckning och säkerställ korrekt hantering
- Uppföljning av genomförda informationssäkerhetsklassningar och säkerställ genomförda aktiviteter
- Genomför omklassning

Följ upp utbildningsinsatser för chefer och medarbetare

Följ upp de obligatoriska arbetssätten i ILS

Uppdatera Lokal anvisning för informationssäkerhet

- Se över och uppdatera *Lokal anvisning* för att säkerställa ändamålsenlig styrning av informationssäkerhetsarbetet

3.3 2027

Genomföra inventering och informationsklassning, uppdatering av registerförteckning

Uppdatera Lokal anvisning

Förvaltningsledningen beslutar att godkänna förslagen i Ledningens genomgång i sin helhet.