Ledningens genomgång år 2023

Socialförvaltningen

Beslutad 2023-12-12
Reviderad [datum]

Ledningens genomgång
Bilaga till socialnämndens verksamhetsplan 2024
Dnr: SOF 2023/509
Kontaktperson: Christina Ring

1 Sammanfattning

För att nå stadens mål om en modern, hållbar och innovativ storstad ska det drivas ett systematiskt informationssäkerhets- och dataskyddsarbete 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 2024 med inriktning 2025-2026. För 2024 är det följande:

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

[1] Metoder it-området (stockholm.se)

Innehållsförteckning

1 Sammanfattning 2

2 Faktorer som påverkar verksamhetens LIS 4

2.1 Omvärldsbevakning – hot, trender och ny lagstiftning 4

2.2 Identifierat i RSA, GDPR-rapport samt VoR 5

3 Förbättringar som föreslås för verksamhetens LIS 6

3.1 2024 6

3.2 2025 8

3.3 2026 8

2 Faktorer som påverkar verksamhetens LIS

Ledningssystem för informationssäkerhet även förkortat LIS utgår från ISO standard 27001. Standarden är global och stödjer organisationer, förvaltningar och bolag att skydda känslig information från risker och hot. För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska socialnämnden 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 leder det oroliga världsläget till ökning av cyberangrepp och inom lagstiftningsområdet sker förändringar som påverkar informationssäkerhetsarbetet i snabb takt. 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 kommer under 2024 i form av förändringar i NIS-direktivet. Förslaget redovisas i februari 2024 för att sedan anpassas till svensk lag. Inom nämndens ansvarsområde omfattas idag hälso- och sjukvård av NIS. I samband med förändringen, kallad NIS 2, kan ytterligare områden komma att omfattas.

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.

2.2 Identifierat i RSA, GDPR-rapport samt VoR

I förvaltningens risk- och sårbarhetsanalys finns en risk kopplad till informationssäkerhet formulerad: *Brister i informationssäkerhet med konsekvensen att sekretessbelagda uppgifter går att komma åt för allmänheten.* Bedömningen är att konsekvenserna är som störst för verksamheter där det kan finnas en hotbild mot målgruppen Åtgärder är kontinuitetsplanering med rutiner för att skydda sårbara målgrupper.

I GDPR årsrapport för 2022[2] lyfts tre områden i skärningslinjen mellan dataskydd och informationssäkerhet. Dessa är tredjelandsöverföringar, grundläggande kompetens för förvaltningens medarbetare avseende dataskydd och informationssäkerhet samt samarbetet avseende frågorna dataskydd och informationssäkerhet.

Identifierade risker

Risk	Konsekvens	Sannolikhet/ konsekvens (1-4)	Risk-värde	Åtgärd
Behörighetshantering	Bristande hantering av behörigheter innebär risk för icke behörig åtkomst till känslig information	4/3	16	Rutin för att säkerställa korrekt hantering samt uppföljning av borttag av åtkomst för icke behörig personal
Risk för bristande regelefterlevnad mot kraven i GDPR med anledning av det osäkra rättsläget för tredjelandsöverföringar.	Inlåsning i avtal som inte uppfyller krav på säkerhetsåtgärder för personuppgifter.	3/4	12	Information och utbildning till nyckelroller. Säkerställ att frågan hanteras i processer för nyutveckling och anskaffning.
Felaktig hantering av verksamhetens information på grund av otillräckliga kunskaper och inaktuella rutiner.	Information kan röjas till obehöriga eller inte vara tillgänglig eller korrekt när den behövs i verksamheten. Bristande lagefterlevnad.	3/3	9	Genomför planerade utbildningar. Följ upp utbildningsinsatser. Säkerställ att Lokal anvisning är känd och följs
Incidenter hanteras inte enligt riktlinjer och krav	Information kan röjas till obehöriga Bristande lagefterlevnad.	3/4	12	Implementering av lokal rutin för incidenthantering. Öka kompetens hos chefer och medarbetare.

[2] Bilaga 8 - GDPR årsrapport 2022 (insynsverige.se)

Informationsklassning genomförs inte	Känslig information skyddas inte på rätt sätt och riskerar spridas till icke behöriga personer	2/4	8	Inventera informationstillgångar som verksamheten ansvarar för. Ta fram rutin för underhåll över tid Säkerställ att Lokal anvisning är känd och följs. Utbildningsinsatser för chefer och informationsansvariga.
Brister inom informationssäkerhet i upphandlingsförfarande	Rätt krav ställs inte vid anskaffning och utveckling av varor och tjänster vilket innebär brister i skydd av information	2/4	8	Etablera en arbetsgrupp för informationssäkerhet för kunskapsöverföring, informationsdelning och redundans.

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, det lokala ledningssystemet, uppnås. Exempelvis avseende incidenthantering analyseras frågan om incidenter som uppstår i verksamheten rapporteras. Om rapportering inte sker ska en analys av varför genomföras samt förslag på förbättringar för att öka anmälningsfrekvensen tas fram.

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

3.1 2024

Styrning och uppföljning

- Under året inleder 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.
- Uppföljning av *Ledningens genomgång* årligen.
- Roller, ansvar och mandat framgår i Lokal anvisning för informationssäkerhetsarbetet, under året kommer denna implementeras i organisationen.

Genomföra inventering och informationsklassning samt upprätta registerförteckning

- Inventering av nämndens information med prioritering av informationsmängder som innehåller integritetskänsliga och känsliga personuppgifter alternativt omfattas av NIS
- Upprätta 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
- Obligatoriska arbetssätt inom de prioriterade områdena behörighetshantering, implementering av lokal anvisning, incidenthantering, informationsklassning och informationssäkerhet vid upphandlingsförfarande.
- Stödmaterial på intranätet

Utbildningar för chefer

- Genomföra befintlig och kommande obligatorisk stadsövergripande e-utbildning som lanseras under 2024. Åtta avsnitt under våren om 5-10 minuter som genomförs enskilt.

Utbildningar för medarbetare

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

Struktur för samarbete inom informationssäkerhet och dataskydd

- Etablera en arbetsgrupp med representation av nyckelkompetenser för att säkerställa det operativa arbetet inom dataskydd och informationssäkerhet

Uppdatera lokal anvisning

- Se över och uppdatera lokal anvisning för att säkerställa ändamålsenlig styrning av informationssäkerhetsarbetet, genomförs årligen.
- Under året tydliggörs årshjul och uppföljningen i samarbete med stadsledningskontoret.

2025

Genomföra inventering och informationsklassning, uppdatering av registerförteckning

- Uppdatera inventering av nämndens information
- Uppföljning av upprättad registerförteckning och säkerställa 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

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

3.2 2026

Genomföra inventering och informationsklassning, uppdatering av registerförteckning

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

Uppdatera Lokal anvisning

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

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