Ledningens genomgång 2023
Kulturförvaltningen

Beslutad [datum]

Ledningens genomgång

Dnr: KUL 2023/1946

Kontaktperson: Jenny Ekman, informationssäkerhetssamordnare

Ledningens genomgång är ett begrepp inom ledningssystemet för informationssäkerhet enligt standarden ISO 27001 som syftar till att de som ansvarar för informationssäkerheten inom en organisation minst årligen ska informera sig om hur arbetet går.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, så kallad Ledningens genomgång, från informationssäkerhetssamordnaren.

I *Anvisningar för nämndernas arbete med verksamhetsplan 2024* uppmanas samtliga nämnder och bolagsstyrelser att ta fram en Ledningens genomgång med en planering för informationssäkerhets-arbetet under de kommande tre åren. Denna ska biläggas verksamhetsplanen.

Innehållsförteckning

1.1 Ledningssystem för informationssäkerhet

Information är en grundläggande och avgörande tillgång i en organisation, på samma sätt som medarbetare, lokaler och utrustning. Därför måste vi skydda vår information så:

- att den alltid finns när vi behöver den (tillgänglighet)
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den (konfidentialitet)

Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk så som policys och riktlinjer, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd. Det handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver. Stockholm stads arbete med informationssäkerhet utgår från ISO 27001, en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information från hot och risker. Standarden ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet, LIS.

Stockholms stads informationssäkerhetsarbete regleras i en riktlinje för informationssäkerhet som är en bilaga till stadens kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För kulturförvaltningens räkning fastställer kulturdirektören i december 2023 en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet hanteras inom kulturförvaltningen.

1.2 Vad påverkar Kulturförvaltningens informationssäkerhetsarbete?

1.2.1 Omvärld och ny lagstiftning

Rätten till tillgång (registerutdrag) har av Europiska dataskyddsstyrelsen (EDPB) valts ut som ett fokusområde för år 2024 och det är därmed ett område som kommer att prioriterats av dataskyddsmyndigheterna under det kommande året.

Kulturförvaltningen har en tillfredsställande hantering av registerutdrag och inga särskilda åtgärder planeras.

Tredjelandsöverföring av personuppgifter är ett aktuellt tema efter att EU-kommissionen godkände ett nytt avtal mellan USA och EU som ökar skyddet för personuppgifter som hanteras av USA-ägda molnleverantörer. Rättsläget i ett längre perspektiv är dock fortsatt osäkert och grundliga risk- och konsekvensbedömningar rekommenderas innan amerikanska molntjänster tas i bruk.

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

Staden genomför en satsning på normerande klassningar, där kulturförvaltningen deltar. Incidentprocessen och ett nytt verktyg för incidenthantering utreds.

1.2.3 Kompetensutveckling

Staden har även tagit fram nya e-utbildningar inom informationssäkerhet för medarbetare och chefer, som lanseras under 2024.

Under 2024-2025 pågår ett projekt för digitalt kompetenslyft på Kulturförvaltningen med finansiering av Europeiska Socialfonden (ESF). Informations- och systemägare är en särskilt prioriterad målgrupp för kompetenslyftet och informationssäkerhet är identifierat som en avgörande framgångsfaktor i förvaltningens digitala förmågor.

1.2.4 Informationsklassning och riskbedömning

Inventering och informationsklassning är grunden i det systematiska informationssäkerhetsarbetet. Under 2022 konstaterades att kulturförvaltningen släpat efter i informationsklassning och riskbedömning. Det mest prioriterade förbättringsarbetet under 2023 har varit att

- Kartlägga förvaltningens informationsmängder utifrån klassificeringsstruktur och verksamhetsprocesser
- Prioritera informationsmängderna utifrån hur känslig och verksamhetskritisk informationen är, samt hur god insikt vi har om risker i hanteringen
- Föreslå en fördelning av operativt process- och informationsägarskap
- Genomföra informationsklassning och riskanalys av prioriterade informationsmängder

Prioriterade informationsmängder är nu hanterade enligt stadens process för informationsklassning. De kommande åren behöver det systematiska arbetet med att hantera identifierade risker befästas genom att informationsklassningarna kontinuerligt revideras och handlingsplaner följs upp.

Att informationen har kartlagts och klassats lägger grunden för nästa steg, att kontinuerligt utvärdera det riskminimerande arbetet. Det är lämpligt att i samband med detta genomföra sk tröskelanalyser och konsekvensbedömningar enligt GDPR där det är nödvändigt.

1.2.5 Risker som identifierats i GDPR-årsrapport

Även i GDPR-årsrapporten lyfter dataskyddsombudet brister i tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifter. Under 2023 har arbetssätten för dataskydd och annan informationssäkerhet integrerats och gemensamma arbetssätt implementerats. Bland annat finns en gemensam process för registerförteckning, informationsklassning och riskbedömning/konsekvensanalys, i enlighet med dataskyddsombudets rekommendation. Genom informationsklassningarna har införda skyddsåtgärder dokumenterats och risker för de registrerades integritet och rättigheter minimerats.

Dataskyddsombudet lyfter i årsrapporten även behovet av utbildning inom dataskyddsarbete av nyckelroller. Under 2023 utbildades informationssäkerhetssamordnare och dataskyddshandläggare i processerna för processen att sammanställa information för registerförteckning, informationsklassning, riskanalys/tröskelanalys och eventuell konsekvensbedömning.

Dataskyddsombudet föreslår även utbildning av nyckelroller som informationsägare och projektledare, vilket adresseras inom ramen för projektet Digitalt kompetenslyft.

1.2.6 Vad har verksamheten identifierat i RSA-arbetet

I kulturförvaltningens risk- och sårbarhetsanalys lyfts risker för att systemstöd inte är tillgängligt på grund av exempelvis elavbrott, samt risken för phishing och cyberattacker. Det är viktigt att skapa en säkerhetskultur och öka medvetenheten i organisationen med planerade utbildningsinsatser. För att motverka risker och säkerhetsbrister i lokala verksamhetssystem behöver det systematiska arbetet med informationsklassning och riskhantering fortsätta.

1.2.7 Resultatet från egen uppföljning (VoR och IKP)

I förvaltningens tertialrapport 2 2023 rapporterades inga väsentliga avvikelser. Under året har kontroller genomförts i förvaltningens verksamhetssystem för att säkerställa att rätt person har rätt behörighet. Vidare har kontroller genomförts inom områden såsom registerförteckning, informationsklassning och hantering av registerförteckning.

I 2024 års väsentlighets- och riskanalys har förvaltningen identifierat att stöd till informationsägare gällande förteckning av informationstillgångar och personuppgiftsbehandlingar som en oönskad händelse som behöver föras in till förvaltningens internkontrollplan 2024.

1.2.8 Resultatet från revisioner

I revisionens årsrapport för 2022 kvarstår rekommendationen att kulturförvaltningen ska utveckla styrning och uppföljning av arbetet med att efterleva dataskyddsförordningen. Vidare rekommenderas att informationsklassificera informationstillgångar samt regelbundet och systematiskt inventera personuppgiftshandlingar.

Ett systematiskt dataskyddsarbete behöver implementeras och ansvar och ägandeskap behöver förtydligas i de olika delmomenten i dataskyddsförordningen. Arbetet med informationsklassning är eftersatt och ett kontinuerligt arbetssätt behöver införas. I verksamhetsberättelsen 2023 redovisas vidtagna åtgärder under 2023.

1.2.9 Information om avvikelser och incidenter

Kulturförvaltningen har en etablerad process för hantering av avvikelser och incidenter. Under året har ett flertal mindre incidenter rapporterats och hanterats. Ingen incident har behövt rapporteras till Integritetsskyddsmyndigheten IMY.

1.3 Prioriterade åtgärder

Under den kommande treårsperioden planeras en rad förbättringsaktiviteter med syftet att implementera att riskbaserat och systematiskt informationssäkerhetsarbete i enlighet med Stockholm stads riktlinje för informationssäkerhet. En av de vägledande principerna är att säkerhetsnivå och inriktning för arbetet bygger på riskanalyser och informationsklassningar.

1.3.1 Uppdatera lokal anvisning

En första version av lokal anvisning för informationssäkerhet har arbetats fram under 2023. Årliga revisioner föreslås för att kontinuerligt vidareutveckla arbetssätt och rutiner.

2024

- Vidareutveckling av lokal anvisning, exempelvis förtydligande av organisationen och rutinen för tröskelanalys och vid behov konsekvensbedömning

2025-2026

- Fortsatt vidareutveckling av lokal anvisning för informationssäkerhet
- Skapa en planering för återkommande översyner över rutiner som inventering av personuppgiftsbehandlingar i registerförteckningen, registerutdrag och incidenthantering.
- Översyn av processen för hantering av incidenter i samband med ev införande av nytt verktyg för incidenthantering inom staden.

1.3.2 Kompetenshöjning och kommunikation

Kulturförvaltningen följer löpande upp deltagandet i obligatoriska grundkurser i informationssäkerhet respektive dataskydd.

2024

- Utbildnings- och informationsinsatser gentemot nyckelroller som systemansvariga, projektledare, system- och informationsägare inom ramen för projektet Digitalt kompetenslyft. Informationssäkerhet är ett prioriterat område 2024, med särskilt fokus på rollen som informations- och systemägare.
- Uppföljning av deltagandet i stadens nya gemensamma e-utbildningar i informationssäkerhet och dataskydd

2025-2026

- Vidareutveckla arbetet med ”ledningens genomgång” genom att involvera informationsägare löpande under året och höja medvetenheten om såväl risker som pågående åtgärder inom det egna ansvarsområdet.

2026

- Etablera en process för kontinuerliga utbildningar i informationssäkerhet efter att projektet Digitalt kompetenslyft avslutats.

1.3.3 Inventering och informationsklassning

Inventering och klassning av information är framför allt ett löpande arbete, men under de kommande åren planeras även en rad förbättringsåtgärder och fokusområden.

2024

- Revision av informationsklassningar av prioriterade informationsmängder, med fokus på uppföljning av riskhantering och handlingsplaner för att etablera ett systematiskt och riskbaserat löpande informationssäkerhets-arbete.
- Förberedande arbete inför upphandling av nytt biblioteksystem, som stödjer en av förvaltningens mest skyddsvärda informationsmängder.
- Förenkla processen för tröskelanalyser och därigenom identifiera behov av konsekvensbedömningar enligt GDPR.

2025

- Löpande översyn av befintliga informationsklassningar, handlingsplaner och riskbedömningar.
- Förbättrad hantering av förvaltningsgemensamma säkerhetskrav och kontroller som återkommer i handlingsplaner för olika verksamhetsprocesser och system, till exempel generella rutiner för behörighetshantering.
- Vidareutveckla processen för risk- och konsekvensbedömningar, inklusive förberedande tröskelanalyser.

2026 –

- Löpande översyn av befintliga informationsklassningar, handlingsplaner, riskbedömningar och konsekvensbedömningar.
- Arbeta för att samtliga processer inkluderar informationssäkerhet som en naturlig del