Stockholms stad

Verksamhetsplan 2024

Bilaga 2:1

Ledningens genomgång år 2023

Exploateringskontoret

Ledningens genomgång
Kontaktperson: Johan Furugren

1 Sammanfattning

Krav på att genomföra momentet *Ledningens genomgång* ställs i Anvisningar för nämndernas arbete med verksamhetsplan 2024 och Tillämpningsanvisningar till stadens riktlinje för informationssäkerhet, dat. 2023-10-13.

Momentet finns även beskrivet i standarden för informationssäkerhet ISO-27000.

Ledningens genomgång innebär en genomlysning av befintligt ledningssystem för informationssäkerhet och förbättringsförslag med åtgärder att inplanera i verksamheten. Ledningens genomgång utgör ett styrande dokument som ska biläggas som redovisat mål i verksamhetsplanen och kommer att följas upp.

Föreslagna aktiviteter beskrivs i detta dokument. Arbetssättet är krav- och riskbaserat med ett 3-årigt perspektiv och ska medföra en serie av årliga och återkommande åtgärder.

Arbete med informationssäkerhet inom exploateringskontoret kommer att för perioden 2024-2026 främst vara fokuserat på inventeringar, informationsklassningar och registerförteckning. Även aktiviteter som stödprocesser, rutiner, utbildningar och kompetensfördjupningar kommer att ingå.

Innehållsförteckning

1.1 Faktorer som påverkar verksamhetens LIS

Stockholms stads arbete med informationssäkerhet ansluter till en global ISO standard, ISO 27001, för informationssäkerhet som systematiserar roller, processer och uppgifter med att skydda organisationers känsliga information från hot och risker. Standarden är ett ramverk, bl a för hur ledningssystem för informationssäkerhet, LIS, implementeras för att skydda informationstillgångar och skapa processtöd som underlättar att planera, hantera, mäta och förbättra arbetet.

Stockholms stads informationssäkerhetsarbete regleras i ett antal styrdokument, bl a i en övergripande Riktlinje för informationssäkerhet med en tillhörande bilaga av Tillämpningsanvisningar (fastställda av stadsdirektören), båda dokumenten utgör en bilaga till stadens Kvalitetsprogram. Tillämpningsanvisningarna stipulerar krav och reglerar ansvar och roller kopplat till Stockholms stads övergripande systematiska informationssäkerhetsarbete.

Exploateringskontoret har utarbetat en Lokal anvisning för informationssäkerhet som specificerar hur stadens övergripande ledningssystem och insatser kring informationssäkerhet appliceras inom förvaltningen.

För att exploateringskontoret ska nå målet att säkerställa en tillfredsställande operativ skyddsnivå måste arbetssätten bli mer transparenta och utformas systematiskt, krav- och riskbaserat kring området informationssäkerhet och dataskydd. Verksamheten inför ett lokalt LIS (ledningssystem för informationssäkerhet) som stöd för att verksamhetens interna aktiviteter och styrmedel för informationshantering ska kunna såväl identifiera, analysera som följa upp förekomsten av olika informationssäkerhetsrisker eller brister.

1.1.1 Omvärldsbevakning – hot, trender och ny lagstiftning

Generellt uppstår kontinuerligt fler hotbilder med olika typer av hotmedel och tekniker. Myndigheter tenderar att vara särskilt utsatta för oönskade aktiviteter.

En utökad lagstiftning, t ex en uppdatering av Säkerhetsskydds-förordningen har aktualiserats i slutet av 2021. Likaså har en omfattande rad initiativ och insatser från skyddsopererande myndigheter som MSB och SÄPO genomförts.

Säkerhetslagen brukar benämnas NIS2-direktivet införs under 2024 och ersätter tidigare NIS-direktiv (Directive on Security of Network and Information Systems).

Ett nytt överbryggningsavtal för personuppgiftsbehandlingar mellan amerikanska och europeiska organisationer och aktörer har godkänts av Europeiska dataskyddsmyndigheten (EDPB) och benämns *EU US Data Privacy Framework*, Hur Stockholms stad agerar på detta ramverk diskuteras och utreds för närvarande på central nivå.

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

Kvalitetsprogrammet betonar vikten av utökade krav och insatser för att säkerställa en god informationshantering. Uppdaterade tillämpningsanvisningar till riktlinjer för informationssäkerhet har publicerats.

Stadens **funktion för övergripande informationssäkerhet** och informationssäkerhetsansvarig (CISO) har en expanderad uppdragsbeskrivning och genomgått en organisatorisk förstärkning under 2023.

Staden har infört en s k *CERT-funktion* för att kunna respondera i lägen av allvarliga incidenter.

Ett *Informationssäkerhetsråd* finns upprättat med en mix av olika kompetensfält.

Systemet *KLASSA* har uppdaterats till ny version 4 vilken innefattar en tydligare kravställning och mer anpassade frågor rörande dataskydd.

Nya digitala applikationer har införts för att öka säkerheten och kvalitet i distansarbete och kommunikation (t ex *Zoom X*, *Säkra meddelanden*).

1.1.3 Vad har verksamheten identifierat i RSA-arbetet

Arbetet med risk- och sårbarhetsanalys (RSA) bedrivs i tvåårscykler och en ny cykel inleds under 2024.

Exploateringsnämnden har i RSA-arbetet år 2022 identifierat några risker kopplat till informationssäkerhet. Ett längre bortfall ger givetvis större konsekvenser medan kortare bortfall endast påverkar verksamheten marginellt. I den RSA som planeras att genomföras under år 2024 kommer kontinuitetshantering att prioriteras och utredas för aktuell verksamhet.

1.1.4 Resultatet från egen uppföljning (VoR och IKP)

I nämndens Väsentlighets- och Riskanalys (VoR) för 2023 har under verksamhetsområdesmål 3.4 ”Medarbetare i Stockholm ska ges goda förutsättningar att göra ett bra jobb” det identifierats som en oönskad händelse att IT-infrastruktur och IT-stöd inte fungerar optimalt (RV 9). Denna punkt ingår även i internkontrollplanen (IKP).

Under 3.5 ”Hög beredskap och stark rådighet ska råda i alla verksamhetsområden” har under processen ”Systematiskt informationssäkerhetsarbete” identifierats fem oönskade händelser:

- Behörighetshantering - felaktig åtkomst till information (RV 9)
- Implementering av lokal anvisning - lokal anvisning avviker jämfört med stadens centrala anvisningar (RV 4)
- Incidenthantering - incidentrapportering görs inte enligt lagstiftning och övriga regler (RV 6)
- Informationsklassning - avvikelser i informations-hanteringen jämfört med informationsklassning. (RV 6)
- Informationssäkerhet inom upphandlingsförfarande – Nödvändiga krav ställs inte (RV 3)

Ingen av dessa punkter överfördes till internkontrollplanen för 2023.

1.1.5 Resultatet från revisioner

Under år 2023 har hittills inga rekommendationer från revisionen lämnats om informationssäkerhet. I årsrapport för 2022 kvarstår rekommendation från en Revisionsrapport från år 2019, *Implementering av dataskyddsförordningen*, där man menar att

nämnden endast delvis vidtagit åtgärder. Arbete pågår med att komplettera registerförteckningen.

1.1.6 Risker som identifierats i GDPR-årsrapport

I den årsrapport som Dataskyddsombudet (DSO) lämnade i samband med verksamhetsberättelsen, fanns ”brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga” för fyra av de sex obligatoriska rapporteringsområdena.

Registerförteckning
Data behöver uppdateras och kompletteras. Arbete pågår med att ta fram en plan för hur förteckningen ska kompletteras.

Styrdokument
Fler rutiner för dataskyddsarbetet bör utarbetas och de som finns, bör uppdateras. Det gäller registerföring, incidenthantering, konsekvensbedömning och de registrerades rättigheter.

Individens rättigheter
En skriftlig rutin tas fram för hur och av vem frågor om de registrerades rättigheter, inklusive begäran om registerutdrag, ska initieras, genomföras och följas upp.

Personuppgiftsincidenter
Befintlig rutin bör uppdateras, roller och ansvar klargöras samt göras känd i organisationen.

1.1.7 Information om avvikelser (incidenter och andra händelser)

Inga incidenter har hittills under året rapporterats i IA för exploateringskontoret.

2 Fokuspunkter för verksamhetens arbete med informationssäkerhet

2.1 Arbete och aktiviteter under innevarande period

Under 2023 har arbetet med informationssäkerhet och dataskydd fortskridit med bl a följande aktiviteter.

- Två separata genomgångar mellan förvaltningschef och informationssäkerhetssamordnare (och del av genomgång med dataskyddsombudet) har ägt rum för att informera och belysa grunder och status inom respektive område för informationssäkerhet och dataskydd.

- I samband med verksamhetsberättelse och bokslut tar förvaltningen del av dataskyddsombudets överlämnade årsrapport och stor hänsyn tas till eventuella rekommendationer till personuppgiftsansvarig som lämnas i rapporten.

- Framtagning och fastställande av *Lokal anvisning för informationssäkerhet inom exploateringskontoret*.

- Framtagning av *Rutin för personuppgiftsincidenter inom exploateringskontoret*.

- Kontroll av genomgångna obligatoriska e-utbildningar samtliga medarbetare.

- Beslut om att inte använda systemet DraftIT för registerförteckning och konsekvensbedömning.

2.2 Planerat och prioriterat arbete och aktiviteter under kommande perioder

2.2.1 Verksamhetsår 2024

Under 2024 förslås som prioriterade åtgärder att genomföras följande aktiviteter:

1. Att skapa teknisk plattform för lokalt LIS (samarbetsyta).

2. Sammanställa personuppgiftsbiträdesavtal med bilaga till lokalt LIS.

3. Att inventera och dokumentera vilka informations-klassningar som är genomförda och lagra dokumentationen i annat system än KLASSA 4. Säkerställa att samtliga informationstillgångar har en objektledare och att klassningars handlingsplaner fullföljs.

4. Genomföra omklassningar av befintliga lokala verksamhets-system. Planeringsfasen för övergången av server- och applikationsdriftstjänster för Lokala System från det nuvarande GSIT-avtalet till stadens nya Systemtjänsteavtal startar i januari 2024 och överföringen sker 2025. Informationsklassningarna måste vara genomförda innan överföringen till förvaltning under nytt avtal kan ske 2025.

5. Att inventera system- och applikationsbaserade person-uppgiftsbehandlingar och uppdatera registerförteckning. Registerförteckningen ska omformas och införas i lokalt LIS. Fokus på verksamhetsprocesser som kan innehålla volymer av integritetskänsliga och känsliga personuppgifter.

6. Etablera process för registerutdrag. Individers rättigheter till begäran om tillgång av registrerade personuppgifter (registerutdrag) har av Europiska dataskyddsstyrelsen (EDPB) valts ut som ett fokusområde för 2024 och det är därmed ett område som kommer att prioriterats av dataskyddsmyndigheterna under året.

7. Att inventera och tilldela informationsägare till respektive system- och applikation.

8. Följa upp utbildningsinsatser för chefer och introduktion för nyanställda/konsulter. Planera kompetenshöjande insatser och medverka som stöd i verksamhetskopplade frågor.

9. Erbjuda och genomföra fler generella och mer funktions-specifika e-utbildningar kring informationssäkerhet och dataskydd. Vissa kurser blir obligatoriska för funktioner och roller. I januari 2024 kommer två nya e-utbildningar att lanseras, en paketering för chefer och en paketering för medarbetare. Båda paketeringarna består av åtta delavsnitt

som kommer att släppas löpande under året. Dessa kommer att vara obligatoriska och komplettera befintliga utbildningar.

Tabell 2.1 Tillgängliga e-utbildningar 2023
Chefer, ledningsgrupp och medarbetare med specialistområden

Namn	Beskrivning	Krav	Typ
Informationssäkerhet för medarbetare i staden	*Grundutbildning inom informationssäkerhet.*	*Obligatorisk för samtliga*	*Certifiering*
Informationssäkerhet – Fördjupning	*Fördjupningskurs inom informationssäkerhet*		*E-lärande*
Informationssäkerhet för chefer	*Utbildning för roll som chef*		*E-lärande*
Informationssäkerhet: Ledningsgruppens ansvar	*Utbildning för förvaltningschef och ledningsgrupp*		*E-lärande*
Förberedelse inför informationsklassning	*Deltagare i klassningar*		*E-lärande*
Grundutbildning i dataskydd		*Obligatorisk för samtliga*	*Certifiering*
Fördjupning i dataskydd – överföring till tredje land		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – rättslig grund		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – personalfrågor		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – webbpublicering och e-post		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – känsliga personuppgifter		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – offentlighet och sekretess		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – registerutdrag		*Obligatorisk för berörda roller*	*E-lärande*

2.2.2 Verksamhetsår 2025-2026

Under 2025 och 2026 förslås som prioriterade åtgärder att genomföras följande aktiviteter:

1. Kontinuitetsplanering för att motverka risker som är identifierade och prioriterade enligt RSA.

2. Utvärdera om förvaltningsspecifik utbildning ska tas fram för exploateringsprojekt: Informationssäkerhet inom projektverksamhet.

3. Eventuellt införande av intern normerande informations-klassning för projektstödsystem. Kartläggning vilka externa normerande klassningar som finns att tillgå, t ex centrala system och plattformar.

4. Genomföra övningar av incidenter och provtryckningar av säkerhetsmekanismer i processer inom verksamhetens delar och hos it-leverantör.

5. Fortsätt arbete med ett informationsmodeller och arkitektur som medger integrerat systemstöd i lokala verksamhetssystem för underlättande av funktioner och informationskontroll.

6. Utöka identifiering av externt påverkande krav eller lagar, myndigheter, generell omvärldsbevakning och bredda/stärka förvaltningens kompetensförsörjning. Samverkan med andra förvaltningar och organisationer.

7. Utreda behov och lokalt stöd för informationssäkerhet i geodatahantering och GIS-plattformar för kartstöd.

8. Regelbunden revidering av lokala processer och styr- och stöddokumentation.

9. En cyklisk plan (årshjul) för aktiviteter vidareutvecklas. Planen ska synkroniseras med dataskyddsombudets aktiviteter.

Observera att några kan omformas och fler kan tillkomma.

Fastställt av förvaltningschef och informationssäkerhetsansvarig Thomas Andersson 2023-11-23.

Informerat och delgivet ledningsgrupp 2023-11-10.