Stockholms stad

Ledningens genomgång 2026

Stadsarkivet

Ledningens genomgång

Dnr: SSA 2025/6370

Kontaktperson: Gustav Fors och Emelie Geuken

1 Sammanfattning

Den information som Stadsarkivet hanterar ska vara korrekt och tillgänglig för dem som behöver använda den men den behöver samtidigt skyddas från att röjas för obehöriga, förvanskas eller förstöras. Detta är kärnan i Stadsarkivets informations-säkerhetsarbete, informationen som Stadsarkivet förvarar och hanterar behöver skyddas så att den kan användas.

I denna genomgång har relevanta dokument granskats för att belysa vilka åtgärder som behöver vidtas inom informationssäkerhets-området på Stadsarkivet. Denna granskning har lett till ett antal föreslagna prioriterade aktiviteter för de kommande tre åren.

Kommande ny lagstiftning innebär att Stadsarkivet behöver arbeta mer aktivt med att stärka informationssäkerhetsarbetet. Framförallt genom att öka kunskapen om dessa frågor hos ledningen och genom att förtydliga ansvarsfördelningen avseende informationssäkerhetsfrågor.

Genomgången berör inte informationssäkerhet inom säkerhetsskyddsarbetet. Detta hanteras enligt stadens tillämpningsanvisning för säkerhetsskydd, KS 2023/751.

Innehållsförteckning

1.1 Faktorer som påverkar verksamhetens LIS

Stockholms stads informationssäkerhetsarbete utgår från standarden ISO 27001. Den utgör en grund för ett ledningssystem för informationssäkerhet, LIS, som är ett arbetssätt för hur en verksamhet bör arbete med informationssäkerhetsfrågor. I Stockholms stad regleras informationssäkerhetsarbetet av ”Riktlinje för informationssäkerhet i Stockholms stad” med tillhörande tillämpningsanvisningar. Den kommande cybersäkerhetslagen kommer också få påverkan på informationssäkerhetsarbetet.

1.1.1 Omvärldsbevakning – hot, trender och ny lagstiftning

Världsläget fortsätter att vara oroligt och säkerhetsfrågor inklusive informationssäkerhetsfrågor står högt på agendan både globalt och nationellt. Under året har Stockholms stad, och ett stort antal andra myndigheter, drabbats av en storskalig personuppgiftsincident på grund av en cyberattack mot en leverantör.

NIS2 och CER-direktiven har trätt i kraft och ska implementeras i svensk lag. NIS2 syftar till att uppnå en gemensam standard för informationssäkerhet inom EU medan CER syftar till att stärka motståndskraften för samhällsviktig verksamhet inom EU. Offentlig förvaltning är en av de sektorer som omfattas av NIS2 såväl som CER, vilket gör att Stadsarkivet likt Stockholms stads övriga förvaltningar omfattas. En ny cybersäkerhetslag där NIS2-direktivet implementeras ska enligt regeringens förslag träda i kraft den 15 januari 2026.

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

Enligt majoritetens förslag till budget för 2026 ska varje nämnd och bolag i Stockholms utveckla och stärka arbetet med informationssäkerhet samt beakta risker och sårbarheter med generativ AI och syntetisk media.

Det pågår ett flertal projekt för att utreda hur staden kan använda AI som Stadsarkivet behöver bevaka och delta i.

1.1.3 Vad har verksamheten identifierat i RSA-arbetet

I Stadsarkivets senaste risk- och sårbarhetsanalys tas risker avseende obehöriga intrång i systemen eDok och e-arkivet upp. Dessa intrång skulle kunna leda till att information röjs, förvanskas eller förstörs. Dessa risker minimeras genom löpande arbete med

simulerade tester för att utvärdera och fastställa systemens säkerhet. En stor del av ansvaret åligger stadens centrala leverantör Vivicta. Även gällande de fysiska arkivlokalernas säkerhet finns det risker som kan leda till att information röjs, förvanskas eller förstörs. I arbetet med lokalsäkerheten behöver det säkerställas att obehöriga inte får tillgång till lokalerna samt att de är skyddade för yttre förhållanden så som klimatförändringar.

Under 2026 inleds en ny RSA-cykel enligt stadens handbok för risk- och sårbarhetsanalys.

1.1.4 Resultatet från egen uppföljning (VoR och IKP)

Enligt Stadsarkivets väsentlighets- och riskanalys för 2025 finns följande brister rörande systematiskt informationssäkerhetsarbete under KF:s mål för verksamhetsområde 3.5 *Hög beredskap och stark rådighet ska råda i alla verksamhetsområden*:

Behörighetshantering

Implementering av lokal anvisning

Incidenthantering

Informationsklassning

Informationssäkerhet inom upphandlingsförfarande

Av dessa brister har implementering av lokal anvisning och informationsklassning tagits med i internkontrollplanen.
En kontrollpunkt är att följa upp att klassningar av information i de lokala system som ska föras över till det nya systemtjänsteavtalet har gjorts. Detta har genomförts som ett led i överföringen till det nya systemtjänsteavtalet. Det kvarstår dock flera frågor angående de lokala systemen som behöver följas upp, vilka delvis är beroende av resultatet av stadens projekt långSIKT. En lokal anvisning har ännu inte implementerats, vilket bör prioriteras under 2026.
En mer detaljerad genomgång av dessa brister och föreslagna åtgärder finns i avsnitt 1.2 i genomgången.

1.1.5 Resultatet från revisioner

I Stadsrevisionens årsrapport avseende Kulturnämnden 2024 lyfts att Stadsarkivet behöver ta fram en lokal anvisning för informationssäkerhet och att informationsklassningar av de informationstillgångar som ännu inte har klassats behöver genomföras.

1.1.6 Risker som identifierats i GDPR-årsrapport

I den senaste årsrapporterna från dataskyddsombudet har ett flertal risker identifierats. Bland annat konstateras det att alla informationstillgångar inte är klassade och att det saknas tydliga rutiner för när och hur informationsklassningar och konsekvensbedömningar ska göras. Gällande Stadsarkivets system eDok och e-arkiv Stockholm görs informationsklassningar kontinuerligt och handlingsplanerna följs upp i form av exempelvis penetrationstester och framtagande av rutiner. Men för övriga informationstillgångar saknas det fortfarande rutiner och en tydlig ansvarsfördelning för dessa frågor.

1.1.7 Information om avvikelser (incidenter och andra händelser)

Det finns brister i incidentrapporteringen vad gäller så väl personuppgiftsincidenter som övriga informationssäkerhetsincidenter. När det gäller större potentiella incidenter så tas dessa om hand enligt fastställda rutiner. Men det är få incidenter som rapporteras. Förbättrade rutiner behövs för incidentrapportering för att säkerställa att fler incidenter fångas upp och hanteras. Enheten IT och digitalisering har under året tagit fram interna rutiner för incidentrapportering, liknande rutiner behöver implementeras för hela Stadsarkivet. Utbildningsinsatser kring vad som utgör en incident behöver också genomföras.

1.2 Uppföljning av föreslagna förbättringar inför 2025

Följande förbättringar föreslogs i ledningens genomgång inför 2025:

Färdigställa och implementera lokal anvisning för informationssäkerhet

En inventering har visat att Stadsarkivet saknar en lokal anvisning för informationssäkerhet. En lokal anvisning krävs för att beskriva hur stadens övergripande ledningssystem för informationssäkerhet omhändertas i den egna verksamheten. För att en lokal anvisning ska fungera i praktiken behöver det säkerställas att de roller och ansvarsområden som fastställs har tillräckliga resurser för att anvisningen ska kunna tillämpas. Stadsarkivets ledning behöver utreda vilka behov som finns för att informationssäkerhets- och dataskyddsarbetet ska fungera.

En lokal anvisning har ännu inte implementerats. I ledningens genomgång 2025 föreslogs att Stadsarkivets ledning skulle utreda vilka behov som finns för att informationssäkerhets- och dataskyddsarbetet ska fungera. En dokumentcontroller har anställts i syfte att stärka Stadsarkivets internkontroll och informations-hantering. Det kvarstår att göra en genomgående analys av vilka resurser som behövs för att Stadsarkivet ska kunna bedriva ett mer systematiskt informationssäkerhetsarbete, förslagsvis görs detta i samband med att den lokala anvisningen tas fram.

Genomföra inventering och klassning
Inventering och klassning ska genomföras enligt följande plan.

- *Uppdatering av registerförteckning över personuppgifts-behandlingar enligt dataskyddsförordningen.*
- *Fokus på att inventera och klassa informationstillgångar som innehåller stora mängder personuppgifter.*
- *Behovet av och möjligheten till att ta in konsultstöd för att genomföra vissa klassningar samt upprätta en grund för en ny registerförteckning bör utredas.*

Registerförteckningen har delvis uppdaterats. Det behövs dock tydligare rutiner för när och hur uppdateringar ska ske för att säkerställa att den löpande hålls uppdaterad.

Ett flertal informationsklassningar har genomförts under året. Bland annat för eDok och e-arkivet som är de tillgångar som innehåller flest personuppgifter.

Konsultstöd har tagits in för att leda klassningar och ta fram rutiner, dock ej med önskat resultat. Rekommendationen att se över hur det ska säkerställas att det finns tillräckliga resurser för att driva det arbetet framåt kvarstår därför.

Rutiner för behörighetstilldelning och behörighetsuppföljning
Nya rutiner för tilldelning och uppföljning av behörigheter till system, databaser, gruppdiskar etc. behöver implementeras under 2025.

Nya rutiner för behörighetstilldelning och behörighetsuppföljning har delvis tagits fram och implementerats. Bland annat avseende e-arkivet. Dessa rutiner är ändamålsenliga och det bör utredas om de kan användas även till fler system och informationstillgångar.

Utredning av NIS2 och kommande nationell lagstiftning
En genomlysning av hur NIS2 och tillkommande svensk lagstiftning

påverkar Stadsarkivet och vilka åtgärder som detta innebär behöver genomföras under året.

Informationssäkerhetssamordnaren har följt utvecklingen av den kommande cybersäkerhetslagen under året. Då den försenats har en fullständig analys av hur den kommer påverka Stadsarkivet inte kunnat göras. Stadsarkivet behöver invänta kommande föreskrifter samt stadens centrala riktlinjer på området men även avsätta resurser för att aktivt arbeta löpande med frågor kopplade till lagstiftningen.

1.3 Förbättringar som föreslås för verksamhetens LIS

Föreslagna aktiviteter för de kommande tre åren
Dessa åtgärder föreslås utöver de kompletteringar som nämns i uppföljningen ovan:

2026

Implementera lokal anvisning för informationssäkerhet
En lokal anvisning för informationssäkerhet finns ännu inte på plats. Under 2026 ska en lokal anvisning vara implementerad. Ledningen behöver säkerställa att tillräckliga resurser för att genomföra detta finns på plats och att anvisningen följs i den löpande verksamheten.

Utbildning för ledningsgruppen
Enligt 2 kap. 4 § i förslaget till cybersäkerhetslag ska de personer som ingår i ledningen för en verksamhetsutövare genomgå utbildning om säkerhetsåtgärder. Då ansvaret för informationssäkerhetsarbetet ytterst ligger hos ledningen, i Stadsarkivets fall ledningsgruppen, behöver samtliga i ledningsgruppen genomgå utbildningar för få bättre förståelse för informationssäkerhetsfrågor.

Översyn av arbetet med RSA
Under 2026 inleds en ny omgång inom stadens RSA-process. I detta arbete behöver informationssäkerhetsfrågor ingå på ett tydligare sätt än tidigare.

Ta fram en prioriteringslista för informationsklassningar
En fastställd prioriteringslista för de informationsklassningar som behöver göras kommer underlätta det systematiska

informationssäkerhetsarbetet och säkerställa att tillräckliga resurser finns för att utföra dem.

2027

Förbättrad incidentrapportering
Idag rapporteras få incidenter överlag på Stadsarkivet. Vare sig det gäller informationssäkerhet, dataskydd eller arbetsmiljö. Rutiner finns på plats men de följs inte i tillräcklig grad. En översyn av dessa rutiner och utbildningsinsatser krävs för att rapporteringen ska öka.

Utifrån RSA säkerställa att kontinuitetsplaner finns
RSA-arbetet ska utmynna i olika typer av kontinuitetshanteringsåtgärder. Det behöver säkerställas att dessa finns på plats inom ramen för informationssäkerhetsarbetet.

Öva utifrån framtagna kontinuitetsplaner
De framtagna kontinuitetsplanerna behöver i den mån det är möjligt testas.

2028

Informationssäkerhet inom upphandlingsförfarande
En genomlysning av hur Stadsarkivet arbetar med informationssäkerhet i samband med upphandlingar bör genomföras.

Översyn av leverantörsberoenden
En inventering av vilka leverantörsberoenden som finns kopplat till Stadsarkivets informationshantering och om tillräckliga avtal finns på plats.

Godkänd av

Lennart Ploom
Stadsarkivarie