Stockholms stad

Ledningens genomgång

Kulturförvaltningen

KUL 2025/1815

Sammanfattning av rapporten

Kulturförvaltningen har en bra grund för sitt systematiska informationssäkerhetsarbete. Informationstillgångarna är inventerade och prioriterade. Kritiska informationsmängder är informationsklassade enligt Stockholms stads metodik.

Ett utvecklingsområde för 2026 är att skapa rutiner för löpande uppföljning av riskanalyser, kontinuitetsplaner och handlingsplaner. Detta stärker informationssäkerheten i system och verksamhetsprocesser, och skapar motståndskraft mot störningar och attacker. Uppföljningen bör även inkludera leverantörer och underbiträden.

Under 2026 föreslås en översyn över förvaltningens lokala rutin för administration av behörigheter. Korrekta behörigheter innebär att rätt personer har rätt åtkomst till rätt information vid rätt tid.

Förvaltningen bör även skapa tydligare rutiner för att säkerställa att informationssäkerheten beaktas vid upphandling av framför allt systemstöd.

En ökad hotbild mot offentlig sektor gör att dessa områden är särskilt prioriterade.

2025-12-12

Jenny Ekman, informationssäkerhetssamordnare
kulturförvaltningen

Kulturförvaltningen
Administrativa staben

Askebykroken 13
Box 8100
16308 SPÅNGA
Telefon 08-508 319 44
kultur@stockholm.se
start.stockholm

Innehåll

Ledningssystem för informationssäkerhet

Information är en grundläggande och avgörande tillgång i en organisation. Därför måste vi skydda vår information så att

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

Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk som riktlinjer och anvisningar, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd som skal- och brandskydd. Stockholms 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. Standardens ramverk beskriver 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 för Stockholms stads systematiska informationssäkerhetsarbete. I december 2023 fastställde kulturdirektören en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet hanteras inom kulturförvaltningen.

Ledningens genomgång

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

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet (KS 2023/1192) ska förvaltningschef årligen inhämta en rapport, så kallad Ledningens genomgång, från informationssäkerhetssamordnaren.

Vad påverkar kulturförvaltningens informationssäkerhetsarbete?

Omvärld och ny lagstiftning

Myndigheten för samhällsskydd och beredskap (MSB) konstaterar att cyberattackerna mot offentlig sektor ökar i både omfattning och komplexitet. För att möta hoten behöver organisationer som kulturförvaltningen prioritera cybersäkerhet på ledningsnivå, stärka det systematiska informationssäkerhetsarbetet och åtgärda brister i verksamhetskritiska system.

Inom EU pågår en harmonisering av lagstiftningen för digitala tjänster, cybersäkerhet och datahantering, det digitala regelverket.

Mest relevant för kulturförvaltningen är NIS2-direktivet, som troligtvis införs i svensk rätt 2026 genom ny cybersäkerhets-reglering. Kraven skärps för riskanalyser, incidentrapportering och säkerhetsåtgärder. Kulturförvaltningen omfattas och följer MSB:s vägledning. AI-förordningen trädde i kraft 2024 och blir fullt tillämplig 2026. Förordningen bygger på en riskbaserad modell där högrisk-AI omfattas av särskilda krav.

EU–U.S. Data Privacy Framework (2023) möjliggör överföringar av personuppgifter till USA. Integritetsskyddsmyndigheten betonar dock att rättsläget är osäkert på sikt och att risk- och konsekvens-bedömningar fortsatt är nödvändiga innan amerikanska molntjänster används.

Vad händer inom staden?

Staden behöver genomföra en rad normerande informations-klassningar, det vill säga informationsklassningar av stadsgemensamma system. Normerande klassningar är en förutsättning för att kulturförvaltningen ska kunna ta sitt ansvar som informationsägare och personuppgiftsansvarig. Utan tillgång till information om it-säkerheten i stadens centrala tjänster är det omöjligt för kulturförvaltningen att bedöma informationssäkerhetsrisker. I dagsläget saknas dock normerande klassningar för viktiga system som staden tillhandahåller inom till exempel hr och ekonomi.

Stockholms stad har sedan våren 2025 infört en ny så kallad zonmodell och ett nytt regelverk för nätverkskommunikation, vilket medför ett ökat skydd i stadens miljö. Regelverket styr kommunikation mot centrala system och definierar även krav mot leverantörer av molndrift.

Funktionen för informationssäkerhet på stadsledningskontoret har inlett en genomlysning av stadens gemensamma incidenthanterings-process för bättre stöd i registrering, uppföljning och rapportering. Även den stadsövergripande CERT-funktionen (Computer Emergency Response Team) stärker stadens förmåga att hantera it-incidenter och informationssäkerhetsincidenter.

En allvarlig personuppgiftsincident under hösten 2025 tydliggjorde behovet av att klargöra personuppgiftsansvaret mellan kommunstyrelsen och kulturnämnden när det gäller anställda, vars uppgifter hanteras i stadens centrala system.

I budgeten för 2026 prioriteras informationssäkerhet genom utökade anslag för informationssäkerheten i stadens centrala system.

Informationssäkerhet i risk- och sårbarhetsanalys

Kulturförvaltningens risk- och sårbarhetsanalys (RSA) identifierar risker för otillgängliga systemstöd och förlorad information på grund av exempelvis elavbrott och cyberattacker. Riskerna kan minskas med till exempel kontinuitetsplanering, redundans och säkerhetskopior. För att motverka brister i lokala verksamhets-system behöver arbetet med informationsklassning och riskhantering fortsätta.

Resultatet från egen uppföljning (VoR och IKP)

I förvaltningens tertialrapport 2 2025 rapporterades inga väsentliga avvikelser inom informationssäkerhet. Behörighetskontroller har genomförts i prioriterade verksamhetssystem för att säkerställa att användarkonton är aktuella och relevanta. Kontroller har även genomförts av informationsklassningar och registerförteckning.

I 2026 års väsentlighets- och riskanalys (VoR) redovisar förvaltningen förebyggande hantering av informationssäkerhets-risker, bland annat:

- uppföljning av informationsklassningar, riskanalyser och handlingsplaner för informationssäkerhet.
- förtydligande av rutiner för behörighetsadministration.
- kravställning så att informationssäkerhetskrav tillgodoses i upphandlingar.
- uppföljning av att obligatoriska utbildningar i informationssäkerhet och dataskydd genomförs.
- information till medarbetare om vikten av att rapportera incidenter.

Resultatet från revisioner

Stadsrevisionen konstaterar i årsrapporten för 2024 att rekommendationerna från 2019 nu är åtgärdade: informations-

klassificering, inventering av personuppgiftsbehandlingar och styrning av dataskyddsarbetet.

En kvarstående brist när det gäller informationsklassning rör dock stadens gemensamma systemstöd inom exempelvis ekonomi, hr och dokumenthantering. Det saknas fortfarande normerande informationsklassningar från stadsledningskontoret, vilket gör att förvaltningen inte kan informationsklassificera informations-tillgångarna lokalt på förvaltningen.

Risker som lyfts i dataskyddsombudets årsrapport

Dataskyddsombudet lyfter följande tre rekommendationer till kulturnämnden i årsrapporten för 2025:

- Verksamheten arbetar metodiskt och systematiskt med informationsklassningar. Det finns dock ett behov av att se över andra delar av verksamhetens säkerhetsarbete. Särskilt gäller detta incidenthanteringsprocessen och regelbunden uppföljning av brister i verksamheten.
- Bedömningen är att det finns ett behov av att lyfta vikten av att anmäla misstänkta personuppgiftsincidenter.
- Givet den tekniska utvecklingen och att allt fler leverantörer väljer att lagra data i molntjänster ser vi att behovet av såväl tydliga kravställningar som regelbunden uppföljning av leverantörers val av tekniska lösningar och nyttjande av underbiträden blir alltmer påtagligt.

Information om avvikelser

Kulturförvaltningen har en etablerad process för hantering av avvikelser och incidenter. Utbildningsinsatser har ökat medvetenheten och fler incidenter har rapporterats under 2025. Fem incidenter har anmälts till Integritetsskyddsmyndigheten (IMY).

Ett flertal av dessa incidenter rörde hanteringen av skyddade personuppgifter i ansökningar till kolloverksamhet, vilket föranledde en översyn av systemstödet. Kulturförvaltningen har även under 2025 tagit fram en lokal anvisning för hantering av skyddade personuppgifter.

Förbättringar och åtgärder

Utifrån nämnda observationer och rekommendationer föreslås ett fortsatt fokus på att etablera ett riskbaserat och systematiskt informationssäkerhetsarbete i enlighet med Stockholms stads riktlinje för informationssäkerhet.

Inventering och informationsklassning

Inventering och informationsklassning utgör grunden för att prioritera insatser och välja adekvata säkerhetsnivåer med avseende på konfidentialitet, riktighet och tillgänglighet. Dataskyddsombudet konstaterar att förvaltningen arbetar metodiskt med informationsklassning, men att utökad uppföljning behövs.

2026

- Löpande översyn av informationsklassningar, inklusive framdrift i handlingsplaner för informationssäkerhet.
- Förbättrad hantering av förvaltningsgemensamma säkerhetskrav och kontroller som återkommer i handlingsplaner för olika verksamhetsprocesser och system, till exempel generella rutiner för behörighetshantering.

2027–2028

- Säkerställa att informationsklassning ingår i väsentlighets- och riskanalys (VoR) och internkontrollplan (IKP).
- Verka för att etablera normerande informationsklassningar för stadens gemensamma, centrala system i samverkan med andra förvaltningar och stadsledningskontoret.

Riskhantering och kontinuitet

Kraven på systematiska riskanalyser och kontinuitetsplanering i hela leveranskedjan ökar i och med NIS2-direktivet och nya cyberhot. Kulturförvaltningen har en stor andel verksamhetskritiska molntjänster, vilket ställer krav på regelbunden uppföljning av leverantörer.

En samordnad incidentrutin med gemensamt systemstöd för it-incidenter, informationssäkerhetsincidenter och personuppgiftsincidenter skulle vara av stort värde för kulturförvaltningen, men frågan behöver adresseras stadsövergripande. Utredning pågår fortfarande inom stadsledningskontoret.

2026

- Särskilt fokus på uppföljning av riskanalyser och kontinuitetsplanering för kritiska system och processer som identifierats i risk- och sårbarhetsanalys (RSA).
- Översyn över processen för upphandling och system-införande för att säkerställa korrekt kravställning gentemot leverantörer.
- Lokal anvisning för informationssäkerhet samt arbetssätt för it-upphandlingar kan behöva revideras för att förtydliga

ansvaret för informationssäkerhet vid upphandlingar och hos leverantörer.

2027–2028

- Etablering av processer för regelbunden uppföljning av informationssäkerheten hos it-leverantörer, exempelvis leverantörers val av tekniska lösningar och nyttjande av underbiträden.
- Säkerställa återställningsförmåga i kritiska system.
- Översyn av rutinen för hantering av incidenter i samband med eventuellt införande av nytt verktyg för incident-hantering inom staden.

Kompetenshöjning och kommunikation

En stark säkerhetskultur och kompetenta medarbetare är en avgörande framgångsfaktor för att stå emot cyberattacker och värna förvaltningens information. Kulturförvaltningen har genomfört en omfattande satsning på digital kompetensutveckling 2024–2025 genom projektet Digitalt kompetenslyft, som medfinansierats av Europeiska socialfonden (ESF).

2026

- Stärka säkerhetsmedvetenheten genom fortsatt satsning på nanolärande, alltså regelbundna, men korta e-utbildningar.
- Ta tillvara på erfarenheter utifrån kompetensutvecklings-insatser som har genomförts inom ramen för projektet Digitalt kompetenslyft.
- Etablera en process för kontinuerliga utbildningar i informationssäkerhet efter att projektet Digitalt kompetenslyft avslutats.
- Informera medarbetare om vikten av att rapportera incidenter.

2027–2028

- 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.
- Följa upp att medarbetare tar del av stadens gemensamma, årliga utbildningar inom informationssäkerhet och dataskydd.

GDPR och personuppgifter

Dataskyddsarbetet bör fortsatt vara integrerat i arbetssätten för övergripande informationssäkerhet. Regelbunden uppdatering av registerförteckningen och uppföljning av exempelvis leverantörers underbiträden sker i samband med årliga informationsklassningar.

2025–2027

- Förtydliga planering för återkommande översyner över rutiner som inventering av personuppgiftsbehandlingar i registerförteckningen och behovet av tröskelanalys.
- Verka för tydligare fördelning av personuppgiftsansvaret mellan kulturnämnden och kommunstyrelsen i samverkan med stadsledningskontoret.