Stockholms stad

Dnr 2025-21650

Ledningens genomgång 2026

Miljöförvaltningen

2025-11-07

Ledningens genomgång

Kontaktperson: Jonas Arnqvist

1 Sammanfattning

Fokus på informationssäkerhet har under året 2025 ökat mycket på grund av en kombination av ökat beroende av digitala system och ökade risker för oönskade störningar.

Miljöförvaltningen har länge arbetat med objektförvaltning av system men i takt med att antalet digitala system och tjänster ökat har behovet av en ny och tydligare systematiserad objektförvaltning blivit aktuell. Ett utkast till ny övergripande modell har tagits fram med förtydligande om ansvar.

Miljöförvaltningens dataskyddsgrupp har genomfört 11 ordinarie möten under året där informationssäkerhetsfrågor med särskilt fokus på dataskydd (GDPR) avhandlats löpande.

Kontinuitetsplanering inklusive krisledningsövning har genomförts i olika grupper och dokumenterats.

Personuppgiftsincidenter har hanterats löpande och skyndsamt i tät samverkan med dataskyddsombudet. En av incidenterna har uppmärksammats särskilt, den s.k. miljödataincidenten. Det kunde dock konstaterats att individer knutna till miljöförvaltningen inte drabbats av allvarliga konsekvenser.

Innehållsförteckning

1.1 Faktorer som påverkar verksamhetens Ledningssystem för informationssäkerhet

Ledningssystemet för informationssäkerhet (LIS) omfattar stadens systematiska arbete för styrning av informationssäkerhetsarbetet.

1.1.1 Omvärldsbevakning – hot, trender och lagstiftning

Ökat fokus på kontinuitetsplanering vid risk för större avbrott i verksamheten. Förvaltningen följer utvecklingen på lagstiftningsområdet och anpassar riskanalysen efter denna.

NIS2-direktivet är en EU-reglering som ska stärka cybersäkerheten. I Sverige blir det en ny lag, cybersäkerhetslagen, som väntas börja gälla 15 januari 2026.

1.1.2 Stadens övergripande riktlinjer

Stadens riktlinje för informationssäkerhet består dels av övergripande mål och principer för informationssäkerhetsarbetet, dels av följande sju fördjupade tillämpningsanvisningar:

- Ansvar och roller inom informationssäkerhet
- Kartläggning och klassning av information
- Identitet och åtkomst
- Anskaffning och utveckling av varor och tjänster
- Drift och förvaltning av it-tjänster
- Incidenthantering och kontinuitetshantering
- Loggning och spårbarhet.

1.1.3 Vad har verksamheten identifierat i RSA-arbetet

Tillgången till IT-system, främst handläggningssystemet Ecos har identifierats som en sårbarhet. En handlingsplan för systemet finns upprättad. Möjliga lösningar för att skyndsamt kontakta medarbetare om stadens IT-system är otillgängliga har diskuterats.

1.1.4 Resultatet från egen uppföljning (VoR och IKP)

Väsentlighets- och riskanalys (VoR) och Internkontrollplan (IKP) revideras årligen och bifogas till nämndens verksamhetsplan. Internkontrollplanen följs upp i samband med tertialrapport 2 och verksamhetsberättelsen (VB). Nytt för 2026 är att stadsledningskontoret tar fram stadsövergripande processer och delprocesser som är obligatoriska för nämnderna att riskanalysera, dels inom informationssäkerhet och dels inom andra områden. Därutöver kan nämnderna ta fram egna processer och delprocesser och identifiera risker inom dem.

Systematiskt informationssäkerhetsarbete är en stadsövergripande och obligatorisk process. Där ingår delprocesserna fastställa krav

genom informationssäkerhetsklassning, fastställa lokal anvisning för informationssäkerhet, informationssäkerhet inom upphandlingsförfarande, lokal rutin för behörighetshantering och rutin för incidenthantering. Inga av riskerna som identifierades här bedömdes allvarlig nog att ta med i internkontrollplanen.

Den lokala process som har identifierats är IT-funktionalitet och delprocessen systemförvaltning. Risken som har identifierats relaterar till Ecos prestanda och funktionalitet, där ett nytt arbetssätt för dokumentation av driftstörningar ska införas. Denna risk ingår i internkontrollplanen 2026.

1.2 Förbättringar som föreslås för verksamhetens LIS

- Uppdatera Lokal anvisning för förvaltningens informationssäkerhetsarbete, årligen.
- Informera om rutinen för personuppgiftincidenter, årligen.
- Genomföra inventering och klassning (se nedan).

2026

Fortsätta att inventera och klassa prioriterade verksamhetsprocesser och system (egna och centrala system där normerande klassningar genomförts av objektägare i staden).

Genomföra en förändring av objektstyrningen med objektstyrgrupper.

Konsolidera och dokumentera rutiner i anslutning till nya cybersäkerhetslagen (NIS2).

2027 – fortsätta att klassa prioriterade verksamhetsprocesser

2028 – fortsätta att klassa prioriterade verksamhetsprocesser