Ledningens genomgång år 2026

Skärholmen

Beslutad 2025-12-03
Reviderad [datum]

Ledningens genomgång

Dnr: SKHLM 2025/981

Kontaktperson: Maria Lindqvist Töyrä, ISAM

1. Sammanfattning

Skärholmens stadsdelsförvaltning ska i sitt ledningssystem för informationssäkerhet utgå ifrån gällande lagkrav samt de styrande dokument som stadens kommunfullmäktige har fastställt och är gällande för tiden. Tillsammans med förvaltningens fastställda lokala anvisningar för informationssäkerhetsarbetet utgör dessa dokument förvaltningens Ledningssystem för informationssäkerhet (LIS), som behöver utökas med fler anvisningar för att bygga det riskbaserade systematiska säkerhetsarbetet. Nya lagkrav som Cybersäkerhetslagen ställer höga krav på att förvaltningen ska ha ett systematiskt och riskbaserat informationssäkerhetsarbete där organisation och styrning är avgörande för ett framgångsrikt arbete.

Förvaltningens klassningar pågår och medarbetare genomför de obligatoriska utbildningarna inom informationssäkerhet och dataskydd.

För 2026 rekommenderas en rad åtgärdspunkter, där de viktigaste punkterna berör det grundläggande arbetet i informationssäkerhetsarbetet, det vill säga; kartlägga, klassificera och värdera verksamhetens information, att förvaltningens organisation inom informationssäkerhet är känd och efterlevs samt att styrning för viktiga processer tas fram och fastställs, som exempelvis behörighetshantering, leverantörsstyrning och incidenthantering.

Innehållsförteckning

1.1 Vad är Ledningens genomgång

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

Denna rapportering ska ge information och underlag till förvaltningschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Informationssäkerhetssamordnares förslag på förbättringar inom informationssäkerhetsarbetet är utifrån iakttagelser och insamlad information under året. Rapporteringen ska genomföras minst årligen.

Dokumentet ska diarieföras tillsammans med direktörens beslut.

1.2 Faktorer som påverkar verksamhetens LIS

1.2.1 Omvärldsbevakning – hot, trender och ny lagstiftning

Förvaltningens informationssäkerhetssamordnare (ISAM) bedriver löpande omvärldsbevakning utifrån informationssäkerhet och cybersäkerhet. Till stöd för omvärldsbevakning i staden finns även en central funktion för informationssäkerhet på stadsledningskontoret samt ett nätverk för informationssäkerhetssamordnare. I övrigt deltar ISAM i olika externa nätverk som i Kommuner i Sverige (KIS) som Sveriges regioner och kommuner (SRK) håller i, samt webinarier/konferenser om olika aktuella ämnen som Cybersäkerhetslagen (NIS2 och CER-direktiven).

1.2.1.1 Cybersäkerhetslagen, NIS2 samt CER-direktiven

Förväntas träda i kraft 15 januari 2026. Redan nu går det att ta del av föreskrifterna som är publicerade på MSB:s webbsidor[1] (Myndigheten för samhällsskydd och beredskap). Redan innan föreskrifterna gick ut på remiss har MSB punktmarkerat vissa områden där lagen kommer att ställa höga krav på

[1] Länk till MSB:s sida på internet om föreskrifterna gällande Cybersäkerhetslagen:
Remiss: Förslag till nya föreskrifter om incidentrapportering och informationsskyldighet enligt ny cybersäkerhetslag | MSB

cybersäkerhetsarbetet. Lagen berör nämnder och bolag inom Stockholms stad utifrån tillhörande i det MSB definierar som sektorn Offentlig Verksamhet.

Exempel där föreskrifterna förväntas ställa höga krav[2]:

- Säkerhet i hela digitala leverantörskedjan
  - Gäller även leverantörens underleverantörer
  - Avtal
  - Incidenthantering mellan förvaltningen och leverantörerna samt deras underleverantörer etc.

- Incidenthantering
  - Tidsramar som ska följas
  - Gemensam anmälningsprocess

- Ledningens deltagande och engagemang där ledningen ska
  - Utbilda sig så de har tillräckligt med kunskap[3]
  - Leda och styra arbetet med cybersäkerhet
  - Ta fram interna regler och arbetssätt (systematiskt riskbaserat arbete integrerat med verksamheten),
  - Säkerställa dokumentation
  - Utpeka roller som Samordnare, informationsägare samt systemägare eller motsvarande

- Krav på dokumentation för att bevisa efterlevnaden av föreskrifterna inklusive beslut på 5 år.

I föreskrifterna finns även ett säkerhetskrav som tydliggör att verksamhetsutövare ska arbeta systematiskt och riskbaserat med informationssäkerhet.

Vid bristande förmåga att efterleva lagkraven kan tillsynsmyndigheter tilldela sanktionsavgifter. Förvaltningen kommer att ha olika tillsynsmyndigheter utifrån den verksamhet som berörs.

[2] Föreskrifterna är på remiss och kan komma att förändras fram tills 10/12–25.
[3] CISO:s förslag på utbildning som MSB har tagit fram: Ledningsperspektiv på informations- och cybersäkerhet | MSB

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

1.2.2.1 Budget

I budget för år 2026 höjs ambitionerna för arbetet med informationssäkerhet ytterligare. För stadsdelsnämnderna reserveras 7,7 miljoner kronor för att finansiera en förstärkning av nämndernas arbete med informationssäkerhet.

1.2.2.2 Stadsledningskontorets arbete

Centralt i staden pågår ett arbete med att se över kopplingen mellan NIS2, CER-direktivet och nuvarande styrande dokument. Stadens styrande dokumenten är fortfarande gällande men kommer att uppdateras för att efterleva lagkraven. En möjlig förändring är att kommunfullmäktige efter den 15 januari 2026 kommer att vara utpekad verksamhetsutövare för staden och därmed genomföra anmälan för alla nämnder och bolag. Det fråntar inte nämndens ansvar för informationssäkerhetsarbetet, utan nämnden kommer även fortsättningsvis ha samma ansvar som verksamhetsutövaren har.

1.2.2.3 Personalförändringar

ISAM:s uppdrag har sedan 2024 fördelats mellan Hägersten-Älvsjö stadsdelsförvaltning och Skärholmens stadsdelsförvaltning, där Skärholmen haft 30 procent av tjänsten. Under 2026 kommer det att utökas till en heltidstjänst i Skärholmens stadsdelsförvaltning.

Informationssäkerhetsarbetet är ett förändringsarbete som handlar om att införa säkerhetsåtgärder så som olika processer och anpassa dem efter förvaltningens förutsättningar och ordinarie arbetssätt. Informationssäkerhetsarbetet mellan förvaltningarna ser olika ut och sker på olika sätt vilket har lett till en mer utmanande arbetssituation är förväntat för ISAM.

Förvaltningen stärker informations- och dataskyddsarbetet ytterligare genom att även utöka med en heltidsanställd IT-säkerhetsansvarig.

1.2.3 Resultatet från revisioner

Skärholmens stadsdelsförvaltning har inte haft någon revision rörande informationssäkerhet under 2025.

1.2.4 Risker som identifierats i GDPR-årsrapport

Årsrapporten som Dataskyddsombudet tog fram i januari 2025 visade framförallt på följande som sina huvudsakliga rekommendationer:

- Förvaltningen behöver fortsätta och utöka arbetet med registerförteckningen.

- Förvaltningens konsekvensbedömningar behöver bli både fler och tydligare och dessutom visa kopplingen mellan behandlingarna i registerförteckningen och genomförda konsekvensbedömningar.

- Området Styrdokument behöver ses över och uppdateras samt göras mer tillgängligt och informativt för verksamheten så att det blir lätt att göra rätt.

- Arbete med informationsklassningar behöver prioriteras och utökas.

- Förvaltningen behöver säkerställa att samtliga medarbetare går stadens obligatoriska e-utbildningar.

Dataskyddsombudet uppmanar även stadsdelen att gå igenom avtalskatalogen för att se vilka avtal som är aktuella för stadsdelsförvaltningen. För att säkerställa korrekta PUB-avtal.

1.2.5 Information om avvikelser (incidenter och andra händelser)

Enligt Stadens tillämpningsanvisningar för informationssäkerhet ska alla incidenter med påverkan eller *risk för påverkan* på stadens informationshantering och individ i samband med personuppgiftsbehandling rapporteras. Det gäller både incidenter i nämnder/styrelser och för driftsrelaterade incidenter när de har en verksamhetspåverkan eller/och integritetspåverkan enligt lagkrav. I de fall externa leverantörer hanterar förvaltningens information så omfattas även de av kraven i anvisningen[4].

IA är stadens rapporteringsverktyg samt dokumentationsplats var närmast ansvarig chef för inrapporterad incident ska utreda incidenten inom en månad och beskriva vidtagna åtgärder.

Det finns anledning att tro att incidenter inte rapporteras in i tillräcklig utsträckning. En ökning har dock skett under året i takt med att förvaltningen har haft informationssäkerhet på agendan i olika forum.

[4] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet kap 6. Incidenthantering och kontinuitetshantering

Inträffade incidenter
I augusti skedde ett större IT-angrepp mot systemleverantören Miljödata. Vilket förvaltningen i likhet med stadens övriga förvaltningar och bolag drabbades av. Det omfattade personuppgifter från många kommuner och regioner och även flera privata företag. Personuppgifter från angreppet har publicerats på Darknet. I stor utsträckning är det uppgifter om anställda och före detta anställda som har läckt.

Även uppgifter om personer med skyddad identitet har läckt. Darknet är en del av internet där det förekommer en hel del kriminella hotaktörer som kan dra nytta av uppgifterna för kriminella aktiviteter. Även om incidenten är över så är det inte säkert att uppgifterna någonsin kommer att kunna försvinna helt.

Förvaltningen har även identifierat ett antal incidenter rörandes nätfiske samt handhavande fel kring tjänstekort och handlingar i pappersform. Rapporteringsgraden av dessa situationer ökar vilket indikerar en ökad medvetenhet hos förvaltningens medarbetare.

2. Förbättringar som föreslås

Nedan följer exempel på förbättringsaktiviteter för kommande år.

2.1 Cybersäkerhetslagen

Lagen ställer viktiga krav på ledningens deltagande och engagemang eftersom det är en avgörande del för informationssäkerhetsarbetets framgångsfaktor. Arbetet med informationssäkerhet genomförs redan i förvaltningen men det behöver bli mer systematiskt och riskbaserat. Förvaltningens chefer och medarbetare behöver guidning och stöd i att hitta systematik i arbetet och inkludera det i den ordinarie verksamheten.

Förbättringsförslag:

- Att förvaltningsledningen genomgår utbildning för att stärka sina kunskaper i NIS2 och cybersäkerhetslagen.
- ISAM tar fram förslag på prioritering av informationssäkerhetsprocesser utifrån cybersäkerhetslagen, som förvaltningens ledningsgrupp kan besluta om.
- ISAM tar fram ett förslag till organisation för informationssäkerhet inom förvaltningen som förvaltningens ledningsgrupp kan besluta om.

- Fortsatt stärka chefers kompetens inom informationssäkerhet.
- ISAM arbetar in brister i informationssäkerhetsarbetet i förvaltningens ordinarie processer och rutiner.

2.2 Organisation och resurser

Förvaltningens resurser för arbetet med informationssäkerhet har hittills bestått en informationssäkerhetssamordnare på 30 procent och ett dataskyddsombud på 20 procent. Under 2026 kommer förvaltningen att förstärka arbetet genom att tjänsten som informationssäkerhetssamordnare tillsättas på heltid och en tjänst som IT- säkerhetsansvarig som arbetar mer operativt med dataskydd och IT-säkerhet på heltid rekryteras.

Mycket av arbetet med informationssäkerhet utgår ifrån linjearbetet och att cheferna har ansvar för sin del av arbetet. Till stöd har ett nätverk med informationssäkerhets- och GDPR-ambassadörer funnits som har träffats ett antal gånger per år.
Arbetet med ambassadörerna har inte gett önskad effekt på grund av att det inte finns tillräckligt med kunskap i sakfrågorna (både informationssäkerhet och dataskydd är svårgreppade ämnen som kräver tid för inlärning).

Förbättringsförslag:

- En översyn görs av organisationen för informationssäkerhetsarbetet.
- Utökade resurser för informationssäkerhet och dataskydd
- Ett tydliggörande av roller och arbetssätt för att ISAM, IT säkerhetsansvarig och klassningsledare kan stödja förvaltningens arbete inom området.
- Årshjul för möten i ambassadörsnätverket tas fram, med fokus på informationssäkerhetsarbetet utifrån ambassadörernas avdelningar.
- ISAM ska säkerställa att deltagarna i ambassadörsnätverket förstår uppdraget samt får en tydlig instruktion och rätt förutsättningar för att kunna konkret arbeta med informationssäkerhet på hemmaplan.

2.3 Kartläggning, klassificering och värdering

Varje verksamhet inom förvaltningen ska enligt Tillämpningsanvisning till stadens riktlinje för informationssäkerhet[5] kartlägga och värdera sina informationstillgångar. Detta beskrivs även i Handbok för informationsklassning[6] som ett steg innan informationsklassningsarbetet. Syftet är att verksamheterna ska identifiera och dokumentera vilken information som är av betydelse för verksamheten samt avgöra vilka klassningar som är prioriterade utifrån den insamlade informationen. Utan att genomföra detta grundläggande steg så får verksamheten inte ett korrekt värde på informationen och klassningsarbetet kan ge ett felaktigt eller missvisande värde.

Förbättringsförslag

- Ta fram en lokal anvisning för att kartlägga, klassificera och värdera information som ska godkännas av Stadsdelsdirektören[7] samt en prioriteringsordning av klassningar.
- Förvaltningsledningsgruppen bör fastställa det framtagna förslaget på prioriteringsordningen gällande klassningsarbetet.

2.4 Behörighetshantering

Enligt Skärholmens stadsdelsförvaltnings lokala anvisning för informationssäkerhet är varje informationsägare inom förvaltningen ansvarig för hantering av behörigheter inom sitt ansvarsområde. Detta innebär att verksamhetsansvarige (samma som informationsägare) ska säkerställa att behörigheter tilldelas enligt gällande lagkrav samt begränsat utefter roll och ansvar samt behovet av tillgång till information för att genomföra sina arbetsuppgifter. I behörighetsansvaret ingår att följa upp och avsluta behörigheter som inte längre är gällande. Inom Skärholmens stadsdelsförvaltning finns en administrativ enhet som avlastar informationsägare med behörighetstildelning och kontroller utifrån beslut av informationsägaren. Revision gällande behörigheter görs två gånger per år av administrativa enheten samt vid avslut av anställning inom Skärholmens stadsdelsförvaltning. Behörigheter dokumenteras av administrativa enheten.

[5] Kap 2. Kartläggning och klassning av information s. 11 (44).
[6] Kap 2. Vad innebär en informationsklassning s. 3 (26).
[7] Pågår och förväntas vara klar Q1 2026.

Förbättringsförslag:

- En tydlig behörighetsblankett avseende ny/ändring/avslut av behörighet som ska fyllas i av informationsägare och som skickas till administrativa enheten för behandling.
  Utförare: förslagsvis IT tillsammans med informationsägare.

2.5 Leverantörsstyrning- Anskaffning och utveckling av varor och tjänster

För att kunna ställa rätt krav på leverantörer är det viktigt att genomföra ett bra förarbete, där informationssäkerhetsarbetet är en del. När klassningsarbetet är färdigt för en verksamhet, blir den tillsammans med en konsekvensbedömning grunden för de krav som ställs på leverantören redan i upphandlingen. På det sättet kan förvaltningen säkerställa att gällande lagkrav efterlevs. Cybersäkerhetslagen ställer också höga krav på avtalsuppföljningen för att säkerställa att leverantörer håller sig till de rutiner och riktlinjer som förvaltningen har angett.

Förbättringsförslag:

- ISAM tillsammans med upphandlingsfunktionen ska ta fram en checklista för anskaffning och utveckling av varor och tjänster där informationssäkerhetskraven finns med, för att säkerställa regelefterlevnaden i stadens styrande dokument.