Ledningens genomgång år 2025

Hägersten Älvsjö stadsdelsförvaltning

Beslutad 2025-12-02

Ledningens genomgång

Dnr: HÄ 2025/846

Kontaktperson: Mia Perzon Måringer, ISAM

1. Sammanfattning

Hägersten Älvsjö 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 medarbetar genomför de obligatoriska utbildningarna inom informationssäkerhet.

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 är styrning för viktiga processer tas fram och fastställs, som exempelvis behörighetshantering, leverantörsstyrning och incidenthanteringen.

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. ISAM:s förslag på förbättringar inom informationssäkerhetsarbetet är utifrån iakttagelser och insamlad information under året. Rapporteringen ska genomföras minst årligen.

Dokumentet biläggs nämndens verksamhetsplan och beslutas av nämnd.

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 15/1–2026. 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 cybersäkerhetsarbetet. Lagen berör nämnder och bolag inom

[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

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 15/1 2026 kommer att vara utpekad verksamhetsutövare[4] 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

ISAMs uppdrag har sedan 2024 fördelats mellan Hägersten-Älvsjö stadsdelsförvaltning och Skärholmens stadsdelsförvaltning. Under 2026 kommer det att utökas till en heltidstjänst i Hägersten Älvsjö.

1.2.3 Resultatet från revisioner

Revisionskontoret genomförde under 2025 en granskning av det arbete som Hägersten-Älvsjö stadsdelsförvaltning gjort för att säkerställa att skyddade personuppgifter inte röjs till obehöriga. Särskilt fokus riktades mot hanteringen inom verksamhetsområdena förskola respektive ekonomiskt bistånd. Utgångspunkten för granskningen var kommunfullmäktiges policy för skyddade personuppgifter samt riktlinjer för informationssäkerhet.

Granskningen visade att det finns rutiner för hantering av skyddade personuppgifter inom både verksamhetsområdena, men att nämnden bör stärka hanteringen av skyddade personuppgifter för att säkerställa att de inte röjs till obehöriga. Det saknas också en övergripande riskanalys som omfattar samtliga skyddade personuppgifter som nämnden hanterar samt styrning genom exempelvis anvisningar. Även uppföljning av att hanteringen sker på ett säkert och enhetligt sätt på såväl övergripande nivå som inom verksamhetsområdena förskola och ekonomiskt bistånd saknas.

[4] Alla bolag, nämnder, organisationer som berörs av lagen definieras i föreskrifterna som Verksamhetsutövare.

Sammantaget anser revisionskontoret därför att det finns en risk för att skyddade personuppgifter kan röjas till obehöriga.

Revisionskontoret rekommenderade nämnden att:

- Säkerställa att det finns en övergripande riskanalys gällande risk för röjning av skyddade personuppgifter inom hela nämndens verksamhet, och vid behov upprätta anvisningar för hanteringen av skyddade personuppgifter.
- Regelbundet följa upp att hanteringen av skyddade personuppgifter sker på ett säkert och enhetligt sätt inom nämndens verksamheter.

Arbetet med skyddade personuppgifter pågår utifrån Revisionskontorets rekommendationer.

1.2.4 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudets årsrapport tas fram årligen i samband med verksamhetsberättelsen och är ännu inte färdigställd för 2025. I dataskyddsombudets årsrapport för 2024 rekommenderades följande åtgärder

- Minimera risken att personuppgifter e-postas utan tillräckligt skydd genom att åtgärda de risker som kommit fram under projektet med TDialog.
- Gör en tydlig rutin för att ingå avtal med leverantörer där överföringar till tredje land sker.
- Fortsätt arbetet för att säkerställa att hanteringen av skyddade personuppgifter i förskolan sker på ett säkert sätt.
- Genomför fler informationsklassningar av system.

Av rekommendationerna har nämnden under 2025 arbetat med säkerställande av hantering av personuppgifter inom förskolan samt informationsklassning av system. I övrigt saknas åtgärder. Förvaltningen saknar en resurs som hjälper verksamheterna att arbeta operativt med efterlevnaden av lagkraven inom dataskydd. Kraven på dokumentation enligt dataskyddsförordningen är omfattande och kräver kompetens.
Exempelvis gällande de registrerades rättigheter som består av 8 principer[5] som förvaltningen ska kunna svara mot och ta fram informationen skyndsamt.

Konsekvensbedömningar genomförs inte systematiskt och kontinuerligt. Idag använder förvaltningen Draftit för att registrera personuppgiftsbehandlingar men saknar modulen för

[5] Beskrivs på IMYs webbsidor här: De registrerades rättigheter | IMY

konsekvensbedömningen. Modulen skulle underlätta för cheferna och möjliggöra ett enklare sätt att hålla ihop personuppgiftsbehandlingarna med genomförda konsekvensbedömningar enligt lagkraven.

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 där det finns en verksamhetspåverkan eller/och integritetspåverkan enligt lagkrav. I de fall externa leverantörer hanterar förvaltningens information så omfattas även de av kraven i anvisningen[6].

Det finns anledning att tro att incidenter inte rapporteras in i tillräcklig utsträckning. Det baseras på att det sker en ökning av rapporterade incidenter efter att ISAM haft/ varit på olika dragningar ex chefsforum eller inför ledningsgrupper. Dessa minskar dock med tiden och chefer och medarbetare behöver ständigt påminnas om att anmäla incidenter. ISAM:s iakttagelser är att verksamheten förstår och rapporterar incidenter som rör känsliga uppgifter men inte de incidenter som rör harmlösa uppgifter (exempelvis offentliga uppgifter). Enligt Dataskyddsförordningen måste den personuppgiftsansvariga göra en bedömning om det är en personuppgiftsincident eller inte. Om det är en personuppgiftsincident ska den personuppgiftsansvarige så fort som möjligt bedöma riskerna för de registrerade.

IA är stadens rapporteringsverktyg samt dokumentationsplats. Närmast ansvarig chef för inrapporterad incident ska utreda incidenten inom en månad och beskriva vidtagna åtgärder. Även här behöver utredning och åtgärder göras mer utförligt.

Inträffade incidenter

I augusti skedde ett större it-angrepp mot systemleverantören Miljödata. 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.

---

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

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.

2. Föreslagna förbättringar

2.1 Organisation och resurser

Förvaltningens resurser för arbetet med informationssäkerhet har hittills bestått en informationssäkerhetssamordnare på 70% och ett dataskyddsombud på 20%. Under 2026 kommer informationssäkerhetssamordnaren att arbeta heltid med frågan, vilket är en förstärkning av resurser.

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.

Förbättringsförslag:

- En översyn görs av organisationen för informationssäkerhetsarbetet.

Att rapportera incidenter är en förutsättning för det riskbaserade informationssäkerhetsarbetet. Rapporteringen är även till för att ge information till förvaltningens ledningsgrupp om var det finns sårbarheter och ifall dessa behöver prioriterade eller om akuta säkerhetsåtsåtgärder behöver vidtas för att minska riskerna att samma incident inträffar igen.

Förbättringsförslag:

- ISAM tar fram en förvaltningsövergripande anvisning som godkänns av stadsdelsdirektören
- förvaltningens ledningsgrupp säkerställer att avdelningarnas verksamheter tar fram lokala rutiner för hantering av incidenter (anpassade efter deras verksamheter och efterlevnaden av lagkrav).

2.2 Cybersäkerhetslagen

Cybersäkerhetslagen ställer viktiga krav på ledningens deltagande och engagemang som avgörande framgångsfaktor för informationssäkerhetsarbetet. Nämndens arbete med informationssäkerhet är i dagsläget inte tillräckligt systematiskt eller riskbaserat. Chefers kännedom om ansvar och uppdrag inom området behöver förbättras.

Förbättringsförslag:

- Stadsdelsnämndens förvaltningsledning ska genomgå utbildning för att stärka sina kunskaper i NIS2 och cybersäkerhetslagen (aktivitet i VP 2026).
- 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.
- ISAM har en genomgång av de lokala tillämpningsanvisningarna för informationssäkerhet på chefsforum.
- ISAM tar fram en anvisning för behörighetsstyrning (aktivitet i VP 2026).
- ISAM arbetar in brister i informationssäkerhetsarbetet i förvaltningens ordinarie processer och rutiner, exempelvis i 2C8 och upphandlingsprocessen.

2.3 Kartläggning, klassificering och värdering

Varje verksamhet inom förvaltningen ska enligt Tillämpningsanvisning till stadens riktlinje för informationssäkerhet [7] kartlägga och värdera sina informationstillgångar. Detta beskrivs även i Handbok för informationsklassning[8] 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.

[7] Kap 2. Kartläggning och klassning av information s. 11 (44).
[8] Kap 2. Vad innebär en informationsklassning s. 3 (26).

Förbättringsförslag

- ISAM tar fram en lokal anvisning för att kartlägga, klassificera och värdera information som ska godkännas av stadsdelsdirektören[9]
- ISAM föreslår 2-4 verksamheter[10] som prioriteras i arbetet med att genomföra kartläggning, klassificering och värderingsarbete under 2026, som förvaltningsledningen beslutar om.

2.4 Behörighetshantering

Enligt Hägersten Älvsjös lokala anvisning för informationssäkerhet är varje informationsägare inom förvaltningen ansvariga 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. Behörigheter ska dokumenteras av verksamheten och beslutas av informationssägaren.

Förbättringsförslag:

- ISAM tillsammans med HR och IT tar fram en behörighetsstruktur för förvaltningens behörigheter.

- ISAM tar fram och fastslår förvaltningsövergripande anvisning för behörighetshantering som stöd för verksamheterna vid framtagande av verksamhetsövergripande rutiner för behörighetshantering. Anvisningen bör koppla ihop med behörighetsstrukturen när den är fastslagen.

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

[9] Pågår och förväntas vara klar Q1 2026.
[10] Kan slås ihop och göras på områdes- alt avdelningsnivå om verksamheterna arbetar med samma arbetsuppgifter.

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[11] (Aktivitet i VP 2026).

[11] Tillämpningsanvisningar för stadens riktlinjer i informationssäkerhet Kap 4.