Stockholms stad

# Ledningens genomgång 2026

## Enskede-Årsta-Vantörs stadsdelsförvaltning

**Beslutad av:** Stadsdelsdirektör
**Beslutad:** 2025-10-30
**Dokumentansvarig:** Informationssäkerhetssamordnare
**Diarienummer:** EÅV 2025/943

# Bakgrund

Enligt *Tillämpningsanvisning till stadens riktlinje för informationssäkerhet* ska förvaltningschefen årligen inhämta en rapport, kallad Ledningens genomgång, från förvaltningens informationssäkerhetssamordnare.

Ledningens genomgång innebär en genomlysning av informationssäkerhetsarbetet i verksamheten och ska resultera i beslut om förbättringar inför nästkommande verksamhetsår. Rapporten ska ge förvaltningschefen underlag för att bedöma om det lokala arbetet med informationssäkerhet och dataskydd är tillräckligt och har önskad effekt.

Planerade aktiviteter ska redovisas i Ledningens genomgång och i nämndens verksamhetsplan under mål 3.5: *Hög beredskap och stark rådighet ska råda i alla verksamhetsområden.*

**Enskede-Årsta-Vantörs stadsdelsförvaltning**
Avdelning ekonomi och lokaler

Slakthusplan 8 A
121 62 Johanneshov
Telefon 08-508 20 886
kajsa.sandberg@stockholm.se
start.stockholm

# Innehåll

# 1 Uppföljning av åtgärder från föregående verksamhetsår

Inför 2025 fastställdes fem prioriterade fokusområden för att stärka förvaltningens systematiska informationssäkerhetsarbete:

- Utredning och implementering av NIS2
- Översyn av rutin för personuppgiftsincidenter
- Ökad andel informationsklassade system
- Ökad andel medarbetare som har kunskap om informationssäkerhet genom bland annat stadens obligatoriska e-utbildningar
- Behörighetshantering

Arbetet med att utreda och analysera hur NIS2-direktivet ska implementeras i verksamheten har påbörjats. Den nya lagen, cybersäkerhetslagen, föreslås träda i kraft den 15 januari 2026. I väntan på myndighetsföreskrifterna har förvaltningen förberett sig genom att kartlägga vilka system som bedöms vara samhällskritiska och därmed kan komma att omfattas av lagstiftningen.

Rutinen för hantering av personuppgiftsincidenter har uppdaterats under året. Den reviderade rutinen innehåller förändringar avseende dataskyddsombudets roll och ansvarsområde. Den största förändringen innebär att det formella ansvaret för att bedöma och besluta om hur en personuppgiftsincident ska hanteras nu ligger hos respektive chef. Detta omfattar även beslut om huruvida incidenten ska anmälas till Integritetsskyddsmyndigheten (IMY) eller inte. Detta arbetssätt tillämpas redan i övriga stadsdelsförvaltningar inom Stockholms stad.

Under året har arbetet med att öka andelen informationsklassade system fortlöpt. Arbetet har förstärkts tillfälligt genom stöd av en informationssäkerhetshandläggare samt en extern konsult med kompetens inom området. Förvaltningen beräknar att samtliga informationstillgångar kommer att vara informationsklassade före årsskiftet.

Arbetet med att öka andelen medarbetare som har kunskap om informationssäkerhet, bland annat genom stadens obligatoriska e-utbildningar, pågår fortsatt inom förvaltningen. Vissa förändringar i arbetssätt kommer dock att ske under 2026 till följd av att Utbildningsplattformen, från och med den 1 januari 2026, inte längre kommer att skicka automatiska påminnelser till medarbetare om att förnya sina certifieringar i informationssäkerhet och dataskydd. Detta innebär att förvaltningen behöver införa nya rutiner för att påminna medarbetare om e-utbildningarna och

säkerställa att en hög andel medarbetare är certifierade. En ny rutin har tagits fram och kommer att implementeras under 2026.

Arbetet med att ta fram och införa rutiner för behörighetshantering är påbörjat och kommer även under 2026 att vara ett prioriterat område.

# 2 Ledningssystem för informationssäkerhet, LIS

Stockholms stads arbete med informationssäkerhet utgår från standarden ISO 27001. Det är en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information mot hot och risker. Standarden ger ett ramverk för hur ett ledningssystem för informationssäkerhet (LIS) ska implementeras för att skydda informationstillgångar samt skapa en it-process som är lättare att hantera, mäta och utveckla.

Stockholms stads informationssäkerhetsarbete regleras genom en tillämpningsanvisning som utgör en bilaga till stadens Kvalitetsprogram. Till riktlinjen finns även tillämpningsanvisningar som fastställts av stadsdirektören. Tillämpningsanvisningarna reglerar ansvar och roller inom stadens systematiska informationssäkerhetsarbete. För Enskede-Årsta-Vantörs stadsdelsnämnds räkning har förvaltningschefen fastställt en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet tillämpas inom förvaltningen.

Förvaltningens ledningssystem för informationssäkerhet påverkas av ett flertal interna och externa faktorer. Nedan redovisas de faktorer som under året haft, och som bedöms fortsatt ha, betydelse för förvaltningens informationssäkerhetsarbete.

## 2.1 Omvärldsbevakning

Cyber- och informationssäkerhet är prioriterade frågor eftersom den tekniska utvecklingen fortsätter att förändra förutsättningarna för informationshanteringen. En ökad användning av molntjänster, automatisering och AI skapar nya möjligheter, men innebär också nya risker kopplade till dataskydd, tillgänglighet och informationssäkerhet.

Inom staden aktualiserades frågan om informationssäkerhet ytterligare efter att en av stadens systemleverantörer i augusti 2025 drabbades av ett it-angrepp. It-angreppet ledde till att personuppgifter publicerades på Darknet. Händelsen tydliggör vikten av ett systematiskt informationssäkerhetsarbete inom hela staden.

I takt med att samhället har blivit mer digitaliserat har behovet av säkra it-system ökat. År 2016 antog EU därför det första NIS-direktivet som lade grunden för medlemsländernas arbete med att stärka skyddet av samhällsviktiga och digitala tjänster.

I slutet av 2022 antogs ett nytt EU-direktiv, NIS2, som innebär tydligare och skärpta krav på bland annat riskanalyser, säkerhetsåtgärder och rapportering. Direktivet ställer även högre krav på ledningens ansvar och delaktighet i organisationens cybersäkerhetsarbete samt omfattar fler sektorer än tidigare. Sanktionerna vid bristande efterlevnad blir också mer omfattande.

I Sverige föreslås den nuvarande lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ersättas av en ny cybersäkerhetslag. Den nya lagen föreslås träda i kraft den 15 januari 2026. Förvaltningen har under året börjat förbereda sig genom att kartlägga vilka system som bedöms vara samhällskritiska och därmed kan komma att omfattas av lagstiftningen.

## 2.2 Vad händer inom staden?

I Stockholms stads budget för 2026 lyfts informationssäkerhet och digital trygghet fram som prioriterade områden. Till följd av det dataläckage som drabbade staden i augusti 2025 har kommunstyrelsen beslutat att utveckla och stärka arbetet med informationssäkerhet i hela staden.

För ändamålet reserveras 15 miljoner kronor för en extern utvärdering av dataläckaget samt för en övergripande säkerhetsöversyn av stadens centrala system. Därutöver tillförs 7,7 miljoner kronor till stadsdelsnämnderna för att förstärka deras lokala arbete med informationssäkerhet.

## 2.3 Risk- och sårbarhetsanalys (RSA)

Risk- och sårbarhetsanalys (RSA) utgör grunden för stadens beredskaps- och säkerhetsarbete. Utgångspunkten för ett systematiskt säkerhetsarbete är att fokusera på verksamhetens bidrag till det som ska skyddas och värnas i samhället. Säkerhetsarbetet inom stadens verksamheter ska därför utgå från aktuella och verksamhetsanpassade risk- och sårbarhetsanalyser. Stadens arbete med RSA bedrivs i tvåårscykler. Den pågående cykeln omfattar åren 2024–2025.

I Enskede-Årsta-Vantörs stadsdelsnämnds tertialrapport 2 år 2025 rapporterades det att förvaltningens arbete med RSA fortlöper i enlighet med plan.

## 2.4 Väsentlighets- och riskanalys samt interkontrollplan

Syftet med intern kontroll är att skapa förutsättningar för en ändamålsenlig och effektiv användning av skattemedel samt att upprätthålla service med hög kvalitet till kommuninvånarna.

Genom en tillräcklig intern kontroll skapas förutsättningar att förebygga, upptäcka och åtgärda oönskade händelser och därmed minimera risker i verksamheten samt säkra tillgångar och förhindra förluster och oegentligheter som skadar stadens anseende. Arbetet med intern kontroll är en del av stadens kvalitetsarbete.

Den interna kontrollen ska vara utformad för att med rimlig grad av säkerhet kunna uppnå följande:

- att verksamheten är ändamålsenlig och effektiv
- att information om verksamhet och ekonomi är tillförlitlig och rättvisande
- att lagar, förordningar, föreskrifter och styrdokument följs.

Utöver nämndens egna identifierade processer ska nämnden, enligt stadens anvisning, ha med den obligatoriska stadsövergripande processen ***s****ystematiskt informationssäkerhetsarbete* i sin väsentlighets- och riskanalys**.** Nämnden ska vidare bedöma vilka risker som har som har ett så högt riskvärde att de även ska följas upp i nämndens internkontrollplan (IKP).

I 2025 års väsentlighets- och riskanalys identifierades fem risker kopplade till de fem obligatoriska stadsövergripande delprocesserna. Endast en av dessa, behörighetshantering, togs även upp i nämndens internkontrollplan. Risken hanteras genom att uppdatera förvaltningens rutiner för behörighetshantering. Arbetet har påbörjats och kommer färdigställas under 2026.

Inför 2026 har sex risker identifierats i nämndens väsentlighets- och riskanalys. De identifierade riskerna är kopplade till centrala processer inom förvaltningens informationssäkerhetsarbete, såsom behörighetshantering, styrning och incidentrapportering.

# 3 Åtgärder inför kommande verksamhetsår

Inför kommande verksamhetsår planerar förvaltningen att vidta ett antal åtgärder för att stärka ledningssystemet för informationssäkerhet. Åtgärderna utgår från identifierade utvecklingsområden, internkontrollens resultat samt kommande krav i lagstiftning och direktiv.

## 3.1 2026

Under 2026 kommer förvaltningen särskilt fokusera på:

- Utredning och implementering av NIS2.
- Implementera ny rutin för att påminna medarbetare i förvaltningen om att göra de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd.
- Öka andelen medarbetare som har kunskap om informationssäkerhet och dataskydd.
- Uppdatera och implementera nya rutiner för behörighetsadministration.
- Genomföra informationsklassning av nya system samt uppdatera informationsklassningar av befintliga system.

## 3.2 2027

Under 2027 kommer förvaltningen särskilt fokusera på:

- Öka andelen medarbetare som har kunskap om informationssäkerhet och dataskydd.
- Översyn och uppdatering av lokala rutiner.
- Revidering och översyn av kontinuitetsplaner.
- Genomföra informationsklassning av nya system samt uppdatera informationsklassningar av befintliga system.

## 3.3 2028

Under 2028 kommer förvaltningen särskilt fokusera på:

- Öka andelen medarbetare som har kunskap om informationssäkerhet och dataskydd.
- Genomföra informationsklassning av nya system samt uppdatera informationsklassningar av befintliga system.

*Beslutad av förvaltningschef Anders Carstorp*
*2025-10-30*