Stockholms stad

Ledningens genomgång informationssäkerhet

Farsta stadsdelsnämnd

Beslutad av förvaltningsledningen den 25 november 2025

.

Sammanfattning

Ledningens genomgång tas fram att ge nämnden en samlad bild av informationssäkerhetsläget och beslutsunderlag för kommande prioriteringar. Arbetet påverkas starkt av ett fortsatt oroligt säkerhetspolitiskt läge, nya krav genom NIS 2 och den nya cybersäkerhetslagen, EU:s AI-förordning samt en nationell cybersäkerhetsstrategi. Dessa regelverk innebär skärpta krav på systematik, ledningens ansvar, riskhantering, utbildning och incidentrapportering.

Stadens budget för 2026 förstärker ambitionerna inom informationssäkerhet, digitalisering och AI, och stadsdelen får riktade medel för att stärka arbetet. Även regeringen prioriterar frågan genom ny lagstiftning och riktade medel till kommunerna de kommande tre åren.

Genom RSA, intern kontroll (VoR/IKP), revisioner och GDPR-rapporten har flera brister identifierats, bland annat höga risker kopplade till behörighetshantering, avsaknad av konsekvensbedömningar, bristande dataskyddskunskap, otydliga ansvarsförhållanden och brister i rutiner, informationsklassning och PUB-avtal. Samtidigt har vissa framsteg gjorts, men behovet av fortsatt utveckling är stort.

För perioden 2026–2028 föreslås ett antal prioriterade förbättringsåtgärder:

2026

- Fokus på implementering av nya cybersäkerhetslagen/NIS 2.
- Årlig översyn och anpassning av lokal tillämpningsanvisning för informationssäkerhet.
    - Utbildningsinsatser för ledning, chefer och samtliga

medarbetare kring NIS 2, dataskydd, informationssäkerhet och konsekvensbedömningar.
- Stärka den systematiska förvaltningsorganisationen för IT-system, bland annat genom objektstyrgrupper enligt PM3.
- Inventering och informationsklassning av system, med mål om minst 12 system/processer under året, med prioritet på system med känsliga uppgifter.
- Uppdatera och ta fram rutiner för incidenthantering, personuppgiftsincidenter, informationsklassning och digitaliseringsinitiativ.
- Genomföra inventering av personuppgifts-behandlingar som kräver konsekvensbedömningar och ta fram plan för att genomföra dessa.

2027

- Årlig uppdatering av lokal tillämpningsanvisning i enlighet med stadens direktiv.
- Fördjupade, mer verksamhetsanpassade utbildningsinsatser till chefer och medarbetare.
- Fortsatt informationsklassning av system (mål: minst 12 per år) både inför nya införanden och av befintliga system enligt plan.
- Systematisk uppföljning av genomförda klassningar och tillhörande handlingsplaner.

2028

- Årlig uppdatering av lokal tillämpningsanvisning utifrån behov och förändrade krav.
- Fortsatt satsning på utbildning efter identifierade behov i verksamheterna.
- Vidare arbete med informationsklassning av system (minst 12 per år) och uppföljning av befintliga klassningar för att justera och säkerställa att åtgärder genomförs.

Sammanfattningsvis visar dokumentet att nämnden står inför ökade krav på informationssäkerhet, men också har tillgång till riktade resurser. Tyngdpunkten ligger på att bygga upp ett mer systematiskt, riskbaserat och långsiktigt informationssäkerhetsarbete med tydligare ansvar, bättre rutiner, mer utbildning och strukturerad informationsklassning.

Innehållsförteckning

1. Vad är Ledningens genomgång

Ledningens genomgång är en del av ledningssystemet för informationssäkerhet (LIS). LIS är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter.

Syftet med ledningens genomgången är att ge ledningen en bild av informationssäkerhetsläget samt underlag för att kunna besluta om hur arbetet ska bedrivas fortsättningsvis. Det vill säga en viktig kommunikation mellan ledningen och informationssäkerhets-samordnaren.

1.2 Faktorer som påverkar verksamhetens LIS

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Farsta stadsdelsförvaltning ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering.

1.2.1 Omvärldsbevakning – hot, trender och ny lagstiftning

Orolig omvärld
I takt med att det säkerhetspolitiska läget har försämrats och cyberhoten och sårbarheterna ökat, både sett till antal och komplexitet, ställs allt högre krav på Stockholms stad och därmed även Sveriges förmåga att säkra, skydda och stärka informationssäkerhetsarbetet.

För att möta de komplexa utmaningarna i den digitala miljön föreslår regeringen en betydande satsning på nationell cybersäkerhet i budgetpropositionen för 2026. Satsningen uppgår till totalt 300 miljoner kronor under 2026, 350 miljoner kronor under 2027 och 400 miljoner kronor under 2028.

NIS 2
I slutet av 2022 beslutade EU om ett nytt direktiv som ska ersätta nuvarande NIS. Det nya direktivet har fått namnet NIS 2. De stora förändringarna i NIS 2 är följande:

- Fler sektorer och hela organisation omfattas

- Enhetlig kravställan och kram på säkerhetsåtgärder
- Kraftigare sanktioner
- Enhetlig incidentrapportering
- Krav på ledningens ansvar

I Sverige kommer NIS2 att införas genom en ny lag, cybersäkerhetslagen, från och med den 15 januari 2025. I samband med att den nya lagen börjar gälla kommer också ett antal föreskrifter att utfärdas och som kommer vara styrande i tillämpningen av lagen.

Syftet med NIS2-direktivet är att öka motståndskraften mot cybersäkerhetsrisker genom att ställa krav på en hög gemensam cybersäkerhetsnivå för nätverks- och informationssystem inom hela EU. Det handlar om att verksamheter som ansvarar för viktiga samhällsfunktioner ska ha ett systematiskt informationssäkerhetsarbete som leder fram till att lämpliga riskhanteringsåtgärder vidtas.

Idag omfattas stadsdelsförvaltningen av NIS inom hälso- och sjukvård. En ny sektor i NIS 2 är offentlig sektor och i den nya cybersäkerhetslagen framgår det att kommunal verksamhet faller inom ramen för offentlig verksamhet. Därmed omfattas samtliga av förvaltningens verksamheter av den nya lagen.

Det kommer ställa ökade krav på organisering, systematik och ambitionsnivå vad gäller det systematiska informationssäkerhetsarbetet men också vad gäller utbildning av ledning och medarbetare. Utpekade tillsynsmyndigheter kommer påbörja tillsyn från den dagen som lagen träder i kraft.

I statens budget för 2026 avsätts 200 miljoner kronor till kommunerna för implementering av NIS 2. Samma summa ligger i plan även för de kommande tre åren.

AI-förordningen
Utvecklingen av AI går fort och det finns stora möjligheter för verksamheten i och med det. Det finns också stora risker med användandet av AI och det kommer ställa höga krav på informationsklassningar och dataskyddsarbete för att hinna med i samma takt.

EU:s AI Act har successivt trätt i kraft från och med 1 augusti 2024 men får full tillämpning från 2026. Regelverket markerar en ny era för hur artificiell intelligens får användas inom hela EU och

omfattar aktörer i hela kedjan - från tillverkare till installatörer och distributörer. AI-system delas in i fyra risknivåer som styr hur olika system för AI får användas, och förbjuder vissa delar helt och hållet. Specifika krav ställs på de system som har hög risk, exempelvis de som används inom utbildning, brottsbekämpning och infrastruktur.

För svenska organisationer och företag blir det nödvändigt att genomföra riskbedömningar och åtgärder för att uppfylla kraven. Sanktionerna vid överträdelser kan uppgå till sju procent av den globala årsomsättningen – vilket gör det viktigt att agera i tid.

Ny cybersäkerhetsstrategi
Under 2025 beslutade regeringen om en en nationell strategi för cybersäkerhet. Strategin utgår från nationella behov, är en del i implementeringen av NIS 2-direktivet och dess allriskperspektiv för att hantera en bredd av utmaningar. I strategin redogörs för ett antal hot och sårbarheter som påverkar Sveriges cybersäkerhet och utifrån de har man formulerat tre pelare som anger inriktning för Sveriges cybersäkerhetsarbete de kommande fem åren:

- pelare A: Systematiskt och effektivt cybersäkerhetsarbete,
- pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet
- pelare C: Förmåga att förhindra och hantera cybersäkerhets-incidenter.

Strategin innehåller därtill mål som tar sikte på ett antal områden för att åstadkomma förflyttningar under strategins löptid och bemöta de hot och sårbarheter som redogjorts för i strategin. Kommunerna har inte ett utpekat ansvar i genomförandet men berörs av genomförandet, bland annat kopplat till mål 2 i strategin som handlar om *Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering.*

Av strategin framgår också att kommuner, i enlighet med 14 kap. 2 § regeringsformen, ansvarar för sin egen cybersäkerhet och har en central roll för Sveriges cybersäkerhet.

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

Stadens budget
I stadens budget för 2026 förstärks skrivningarna och ambitionerna när det gäller AI, digitalisering samt informationssäkerhet. Bland annat står det att staden ska utveckla och stärka arbetet med

informationssäkerhet samt beakta risker och sårbarheter med generativ AI och syntetisk media. Stadsdelana tilldelas 7,7 miljoner kronor för att finansiera en förstärkning av nämndernas arbete med informationssäkerhet. Sannolikt är det en del av de statliga medel som avsätts till kommuner och regioner under 2026 för införandet av NIS 2. Den statliga finansieringen ligger kvar även 2027 och 2028 medan stadens förstärka stöd endast avser 2026.

Vidare står det i budgeten att en sammanhållen digitaliseringsutveckling med gemensamma lösningar är prioriterat. Facknämnderna ska ta ett samordnande ansvar inom sina ansvarsområden. Stadsdelsnämnderna ska fortsätta att bidra till utveckling och digitalisering genom att bidra i det portföljarbete som socialnämnden och äldrenämnden har initierat. I klartext betyder det att stadsdelarna behöver bygga mottagarorganisationer för digitalisering.

1.2.3 Vad har verksamheten identifierat i RSA-arbetet

Nämnden har under 2024 genomfört RSA, Risk- och sårbarhetsanalys, steg 1-4. Under steg 1-4 har nämnden identifierat risker kopplade till informationssäkerhet. Under 2025 har nämnden genomfört steg 5 och 6 som handlar om att vidta åtgärder i enlighet med de identifierade riskerna.

1.2.4 Resultatet från egen uppföljning (VoR och IKP)

I väsentlighet- och riskanalysen finns nedanstående processer från SLK samt hur stadsdelsförvaltningen har arbetat med dem under 2024.

- Behörighetshantering
- Implementering av lokal anvisning
- Incidenthantering
- Informationsklassning
- Informationssäkerhet inom upphandlingsförfarande

Utöver SLK:s risker har nämnden själva identifierat konsekvensbedömningar och registerförteckningen som två väsentliga processer som värderats och bedömts.

I värderingen av risker konstaterades höga risker i alla processerna men särskilt med fokus på behörighetshantering och avsaknaden av konsekvensbedömningar. Dessa hamnade i internkontrollplanen. I de genomförda granskningarna konstateras att det finns stort behov av utbildning och kunskap vad gäller såväl konsekvensbedömningar som ansvarsfördelningen kopplat till informationssäkerhet

(implementering av lokala tillämpningsanvisningar). Förvaltningsledningen beslutade om att vidta åtgärder för att åtgärda identifierade brister.

Inför 2025 har ungefär samma risker styrts från stadsledningskontoret och värderats på snarlikt sätt som tidigare då de åtgärder som planerats ännu inte vidtagits kombinerat med att det kommer komma ny lagstiftning som ställer större krav på nämndens verksamheter.

1.2.5 Resultatet från revisioner

Under 2024 har behörighetshanteringen i sociala system granskats av revisionen. Revisionen konstaterar att det finns brister och rekommenderar nämnden att

- Upprätta rutiner för tilldelning, ändring, borttagning och uppföljning av användares behörigheter i Sociala system.
- Säkerställa att egenkontroller av behörigheter i Sociala system genomförs och dokumenteras.
- Säkerställa att uppföljning sker av genomförda egenkontroller

I revisionernas årsrapport för 2024 så har revisionen gjort uppföljningar på två tidigare granskningar avseende informationssäkerhet och dataskydd. I dessa uppföljningar konstatera att vissa brister kvarstår. Nämnden rekommenderas att säkerställa att incidentrapporter för verksamhet som omfattas av NIS delges stadsledningskontorets informationssäkerhetsfunktion.

Vidare konstaterar revisionen att det fortsatt finns brister inom nämndens dataskyddsarbete som behöver hanteras. Nämnden har stärkt arbetet vad gäller registerförteckningen, även om det fortsatt finns behov av komplettering, samt ökat antalet genomförda konsekvensbedömningar. Behovet är dock fortfarande stort och arbete kvarstår för att identifiera alla behandlingar som kräver konsekvensbedömningar. Brister finns även fortsatt kopplat till klassning av informationstillgångar, upprättandet av PUB-avtal samt behov av förtydliganden i rutiner och styrdokument.

Sammantaget visar uppföljningen av tidigare granskningarna att nämndens informationssäkerhetsarbete har stärkts i flera delar men att det fortsatt finns behov av att utveckla och stärka arbetet ytterligare.

1.2.6 Risker som identifierats i GDPR-årsrapport

I GDPR:s årsrapport 2024 konstateras följande övergripande risker:

- Bristen på konsekvensbedömningar (inklusive tekniska och organisatoriska säkerhetsåtgärder) och hantering av känsliga personuppgifter
- Medarbetarnas kunskaper om dataskydd är bristfälliga
- Avsaknad av, och otydligheter kring tecknandet av, av pub-avtal
- Ansvarsfördelningen inom Stockholms stad, det vill säga att det råder oklarheten kring incidenter i stadsgemensamma system men också hanteringen av personuppgiftsansvaret kring stadsgemensamma system.

1.2.7 Information om avvikelser (incidenter och andra händelser)

Under 2025 har en NIS-incidenter rapporterats vilket är i paritet med tidigare år.

15 antal personuppgiftsincidenter vilket är en nedgång jämfört med tidigare. Här märker framför allt incidenten i Miljödata ut sig på ett sätt att den hade reell påverkan på förvaltningens arbete när samtliga medarbetares fick personuppgifter röjda.

1.3 Förbättringar som föreslås för verksamhetens

Nedan presenteras identifierade behov och prioriteringar under 2026-2028.

1.3.1 Prioriteringar under 2026

Under 2026 behöver stort fokus ligga på implementeringen av nya cybersäkerhetslagen.

Uppdatera Lokal anvisning

Lokal tillämpningsanvisning ska ses över årligen och under året kommer den även anpassas utifrån behov och nya krav till följd av nya cybersäkerhetslagen/NIS 2.

Utbildningsinsatser för chefer

Utbildning av ledningen för att leva upp till utbildningskravet i NIS 2. Utöver det även genomföra utbildning riktat till förvaltningens samtliga chefer när det gäller NIS 2, nya rutiner och arbetssätt kopplat till det samt vad gäller konsekvensbedömningar.

Utbildningar medarbetare
En grundbult i säker informationshantering är det personliga agerandet i det dagliga arbetet. Medarbetarna i Farsta behöver veta hur de ska handskas med information på ett säkert sätt, och följa riktlinjer som finns för informationssäkerhet. Därför ska samtliga medarbetare genomgå stadens webb-utbildning inom dataskydd och informationssäkerhet.

Utveckla det systematiska arbetet
Utveckla och stärka befintlig förvaltningsorganisation för IT-system och tjänster för att möjliggöra ökad systematik i informationssäkerhetsarbetet. Genom att skapa objektstyrgrupper i enlighet med stadens tillämpningsanvisningar för PM3 skapas förutsättningar för att på ett bättre sätt fånga in vad som händer i organisationen och därmed kunna göra prioriteringar vad gäller förvaltningens resurser.

Genomföra inventering och klassningar
Under 2026 är fokus på nya införanden kopplat till socialtjänstlagen, införande av nya system kopplat till återtagandet av parkdrift i egen regi samt andra planerade införanden. Utöver det behöver Farsta lägga ta fram en plan för att genomföra informationsklassningar av system som sedan tidigare är införda men inte informationsklassade. Under året ska en inventering göras och en plan för genomförande tas fram. Prioriteringen bör utgå från att system med mycket känslig information och mycket personuppgifter ska genomföras först.

Målet är att under 2026 genomföra informationsklassning av minst 12 system eller processer. Därutöver ska informationsklassningsprotokoll genomföras för minst 18 befintliga verksamhetssystem för att göra en initial bedömning av vilken information och dess skyddsvärde som finns i respektive system. Målet är att genomföra informationsklassningsprotokoll på samtliga system inom en treårsperiod.

Följa upp befintliga klassningar
Ett stort antal informationsklassningar är genomförda. Enligt stadens tillämpningsanvisningar ska genomförda klassningar följas upp årligen. Rutin för detta saknas i förvaltningen och sådan behöver tas fram, parallellt med att arbetet med att följa upp klassningar inleds. Ta fram rutin för uppföljning av befintliga klassningar samt påbörja arbetet.

Uppdatera och ta fram rutiner
I och med NIS 2 behöver ett antal rutiner utvecklas och tas fram. Nedan är prioriterade under 2026.

Uppdatera rutin för informationssäkerhet och utvecklingsinitiativ
Det finns en framtagen rutin för digitaliseringsinitiativ. Den behöver förankras och bakas ihop med en ny rutin för informationsklassningar. Det finns en inarbetad rutin för informationssäkerhet. Den behöver dock dokumenteras och förankras.

Uppdatera rutin incidenthantering så att den överensstämmer med nya cybersäkerhetslagen
Uppdatera befintlig rutin för NIS-incidenter efter nya krav. Även stödmaterial för ifyllande av NIS-rapporter behöver uppdateras.

Uppdatera rutin för personuppgiftsincidenter med behov av uppföljning
Befintlig rutin behöver uppdateras med fokus på uppföljning av incidenter.

Konsekvensbedömning
GDPR:s årsrapport samt genomförda internkontroller pekar på behovet av fler konsekvensbedömningar. För att kunna göra det behöver förvaltningen inventera vilka personuppgiftsbehandlingar som behöver konsekvensbedömas samt ta fram en plan för att genomföra dem.

1.3.2 Prioriteringar under 2027

Uppdatera Lokal tillämpningsanvisning för informationssäkerhet
Uppdatera lokal tillämpningsanvisning i enlighet med stadens direktiv och förändrade behov.

Utbildningsinsatser för chefer och medarbetare
Se över behovet och möjligheten att göra riktade insatser till verksamheterna. De obligatoriska utbildningarna är inte tillräckliga för att möta kraven och det har identifierats behov av att anpassa utbildningarna utifrån de olika verksamheternas natur och behov.

Genomföra inventering och klassningar
Fortsätta informationsklassa system inför införanden men också beta av tidigare införda system utifrån den inventering och prioritering som gjorts under 2026.

Målet är genomföra informationsklassning av minst 12 system eller processer. Därutöver ska informationsklassningsprotokoll genomföras för minst 18 befintliga verksamhetssystem för att göra en initial bedömning av vilken information och dess skyddsvärde som nämnden har i respektive system/process. Målet är att genomföra informationsklassningsprotokoll på samtliga system inom en treårsperiod.

Följa upp befintliga klassningar
Inom ramen för befintlig organisation följa upp samtliga genomförda klassningar för att göra justeringar och säkerställa handlingsplanens omhändertagande.

1.3.3 Prioriteringar under 2028

Uppdatera Lokal tillämpningsanvisning för informationssäkerhet
Uppdatera lokal tillämpningsanvisning i enlighet med stadens direktiv och förändrade behov.

Utbildningsinsatser för chefer och medarbetare
Se över behovet och möjligheten till utbildning inom förvaltningens verksamhet.

Genomföra inventering och klassningar
Fortsätta informationsklassa system inför införanden men också beta av tidigare införda system utifrån den inventering och prioritering som gjorts under 2026.

Målet är genomföra informationsklassning av minst 12 system eller processer. Därutöver ska informationsklassningsprotokoll genomföras för minst 18 befintliga verksamhetssystem för att göra en initial bedömning av vilken information och dess skyddsvärde som nämnden har i respektive system/process. Målet är att under 2028 ha KRT-värden på samtliga system.

Följa upp befintliga klassningar
Inom ramen för befintlig organisation följa upp samtliga genomförda klassningar för att göra justeringar och säkerställa handlingsplanens omhändertagande.

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Karin Kollberg	2025-11-28