Stockholms stad

Informationssäkerhet

Ledningens genomgång

2026

Fastighetskontoret

Rapport Ledningens genomgång
Bilaga till Fastighetskontorets verksamhetsplan 2026
Dnr: FSK 2025/207

Kontaktperson: Patrik Pierd, säkerhetschef

Sammanfattning

- Under 2025 har fastighetskontoret fokuserat på att följa upp, detaljera och förtydliga oklarheter i tidigare arbete med fördelning av informationsansvar i verksamheten.
- Samtliga informationstillgångar och dess klassning (avseende konfidentialitet, riktighet och tillgänglighet) har dokumenterats i senaste versionen av KLASSA 4.0. Fastighetskontoret har även fortsatt framtagande av konkreta hanteringsinstruktioner till stöd för verksamheten, och som ska tillämpas av samtliga medarbetare beroende på informationens klassning.
- Baserat på informationstillgångarnas klassning har sedan kontorets verksamhetslokala system klassats inför övergången till den nya tekniska miljön hos TietoEvry i och med införandet av det nya systemtjänsteavtalet inom staden. Även detta är dokumenterat i KLASSA 4.0.
- Under 2024 har fastighetskontoret genomfört och fastställt en risk- och sårbarhetsanalys och levererats till stadsledningskontoret som en del i Stockholms stads risk- och sårbarhetsanalys. Analysens har främst varit fokuserad på konsekvensanalys utifrån samhällsviktig verksamhet och kritiska beroenden och inte perspektivet informationssäkerhet. Under 2026 kommer en riskanalys genomföras inom ramen för fastighetskontorets systematiska informationsklassningsarbete.
- Fastighetskontoret har under 2025 tagit fram en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom fastighetskontoret.
- Med utgångspunkt av fastighetskontorets säkerhetsskyddsanalys måste eventuella krav i säkerhetsskyddslagen (2018:585) beaktas och tas hänsyn till i arbetet med informationsklassningen och därmed även fastighetskontorets hanteringsinstruktioner. Arbetet har påbörjats, och fortsätter under 2026.
- Fastighetskontoret använder det stadsgemensamma systemet IA för att registrera och omhänderta incidenter och händelser. Under den senaste 12 månaders-perioden har 2 st. incidenter/händelser rapporterats avseende informationssäkerhet. Dessa två incidenter avser en personuppgiftsincident hos en extern leverantör samt en personuppgiftincident kopplat till Miljödatahändelsen. Det låga antalet av rapporterade informationssäkerhetsincidenter bedöms beror på att rutinen för att rapportera dataintrång och informationsförlust inte är tillräckligt etablerad i verksamheten.
- Fastighetskontorets arbete med internkontroll och väsentlighets- och riskanalys har under året genomförts enligt plan.
- En GDPR-årsrapport är under framtagande och ska vara klar i december 2025. Samtliga obligatoriska rapporteringsområden kommer att omhändertas.

Innehållsförteckning

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.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, så kallad Ledningens genomgång från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare eller om informationsklassningar och registerförteckning är genomförda.

Denna rapportering ska ge information och underlag till förvaltningschef/bolagschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltnings- och bolagschefer ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.

I anvisningar för nämndernas arbete med verksamhetsplan 2026 uppmanas samtliga nämnder och bolagsstyrelser ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet under de kommande tre åren. Denna ska biläggas verksamhetsplan. Planeringen för de kommande tre åren ska utgå från nämndens verksamhetsuppdrag i budget och följa ”Riktlinje för informationssäkerhet i Stockholms stad”.

Dessa aktiviteter ska redovisas både i Ledningens genomgång samt i nämndens verksamhetsplan under mål ”3.5. Hög beredskap och stark rådighet ska råda i alla verksamhetsområden”. För 2026 är området registerförteckning och informationsklassning särskilt prioriterat i Ledningens genomgång.

Inventering och informationsklassning är grunden i informationssäkerhetsarbetet. Alla nämnder och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar.

2. Ledningssystem för informationssäkerhet, LIS

Stockholms stads arbete med informationssäkerhet utgår från en så kallad ISO standard, SS-ISO/IEC 27001/2. Det är en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information från hot och risker. Standarden ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet, LIS, som skyddar informationstillgångarna och där informationssäkerhetsarbetet följer en tydlig process som är lättare att hantera, mäta och förbättra.

Stockholms stads informationssäkerhetsarbete regleras i en tillämpningsanvisning som är en bilaga till stadens kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören. Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete.

Fastighetskontoret kommer under 2026 ta fram en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom fastighetskontoret.

2.1 Faktorer som påverkar verksamhetens LIS

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska fastighetskontoret ha ett konkret och verksamhetsförankrat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att den operativa verksamheten ska känna till vilken konfidentialitet aktuell information har och hur information med viss konfidentialitet ska hanteras. Dessutom ska det vara tydligt vem som ansvarar för en viss information och vad detta ansvar innebär.

2.1.1 Informationsinventering, informationsklassning samt etablering av informationsansvar

Information utgör en av fastighetskontorets viktigaste resurser. Utan information om byggnader, byggprojekt, underhållsplaner, hyresgäster, driftärenden m.m. kan inte verksamheten fungera. Det är därför enormt viktigt att informationen håller tillräckligt hög kvalitet och att den skyddas så att den inte kommer i orätta händer eller blir förvanskad.

Vi är vana att ha tydligt uttalat ansvar för fysiska resurser såsom: personal, ekonomi, kunder och byggnader m.m. – men för resursen information har detta uttalade ansvar tidigare saknats. Beslut om hur informationen ska hanteras och vilken kvalitet den ska ha bör tas i förhållande till, och vägas mot, andra verksamhetsbeslut som också är kostnadsdrivande.

För att kunna säkerställa rätt hantering av information krävs en beskrivning av informationen, så att alla i verksamheten vet vad vår informationsresurs omfattar och hur den ska hanteras.

Tidigare år har fastighetskontoret fokuserat på att kartlägga informationen som verksamheten använder, vilket har dokumenterats i IT-systemet Qualiware. Därtill har informationsansvariga utsetts i tre nivåer i organisationen: informationsägare, informationsförvaltare samt informationshandläggare. Ytterligare har samtliga informationsmängder klassats utifrån krav på konfidentialitet, riktighet och tillgänglighet. Kontoret har även påbörjat framtagande av konkreta hanteringsinstruktioner som verksamheten kan följa beroende på informationens klassning.

För att tydliggöra vilken information som hanteras i vilket IT-system har en matris tagits fram med hjälp av verktyget Qualiware.

Under denna period har samtliga generella informationstillgångar dokumenterats i IT-systemet KLASSA v. 4.0. Dessutom har kontorets verksamhetslokala system klassats i verktyget KLASSA 4.0. Baserat på detta har handlingsplaner tagits fram, som i sin tur kommer att användas för självvärdering. I samband med detta arbete har en metodanvisning tagits fram i syfte att få en enhetlig klassning av information och IT-system på fastighetskontoret.

2.1.2 Omvärldsbevakning – hot, trender och ny lagstiftning

Sverige befinner sig i en tid där den tekniska utvecklingen sker i mycket högt tempo. Det innebär fördelar och nya möjligheter för hela samhället, som förändras i takt med en tilltagande digitalisering. Vi blir mer effektiva, globala och tekniskt avancerade. Digitaliseringen har samtidigt blivit ett krav där effektivitet, globalisering och avancerad teknik även utvecklats till påbud som alla verksamheter behöver förhålla sig till.

I vår strävan efter att använda alla de möjligheter som den teknologiska utvecklingen erbjuder finns det dock en baksida. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer.

Utöver den ökade digitaliseringen har hotet från både främmande makt och våldsbejakande extremism har breddats och förändras i snabb takt i Sverige, vilket ger en komplex hotbild. Detta framgår tydligt av rapporten ”Hotbild för Stockholms stads säkerhetskänsliga verksamhet” *(Dnr: KS 2023/439)*.

Fastighetskontorets fortsätter utveckla arbetet med informationssäkerhet och behovet av nya arbetssätt och stöd utifrån ökade krav på cybersäkerhet och NIS 2-direktivet. Utvecklingen av artificiell intelligens skapar nya möjligheter och effektivisering inom kontoret. Det innebär även risker och sårbarheter som kontoret behöver beakta i samband nyttjande av information eller media som skapats med stöd av artificiell intelligens. Kontoret planerar att fastställa ett flertal rutinbeskrivningar som reglerar kontorets incidenthantering som berör informationssäkerhet, personuppgifter och IT-incidenter.

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

På fastighetskontoret är informationssäkerheten ett prioriterat verksamhetsområde vilket återspeglas i både KF-mål och nämndmål. KF-mål som berör informationssäkerhet är framförallt 3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden. För detta KF-mål har fastighetskontoret tagit fram följande nämndmål och förväntade resultat för informationssäkerhet.

Informationssäkerhet i kontorets verksamhet
Fastighetskontorets fokus på informationssäkerhet fortsätter under 2026. Under året har en lokal anvisning för informationssäkerhet tagits fram och fastställts med utgångspunkt ur stadens uppdaterade tillämpningsanvisningar. Kontoret kommer också tydliggöra ansvar för olika roller för informationssäkerhet i kontorets delegationsordning. Utbildning inom informationssäkerhet fortsätter under året med fokus på både nyanställda och nuvarande medarbetare.

Förväntat resultat:

- Fastställd lokal anvisning i enlighet med kraven i stadens tillämpningsanvisningar för informationssäkerhet
- Ansvarsfördelning för informationssäkerhet är tydligt reglerad i kontorets delegationsordning
- Kompetenshöjande åtgärder inom informationssäkerhet har genomförts

Dessutom planerar fastighetskontoret under 2026 att genomföra förvaltningsspecifika aktiviteter såsom ta fram rutinbeskrivningar, instruktioner och mallar samt arbetssätt för systematiska kontroller och inventeringar av fastighetskontorets informationssäkerhetsarbete.

2.1.4 Vad har verksamheten identifierat i RSA-arbetet

Utgångspunkten för ett systematiskt säkerhetsarbete är att ha fokus på det som är verksamhetens bidrag till det som ska skyddas och värnas. Därför ska säkerhetsarbetet i stadens alla verksamheter utgå från aktuella och verksamhetsanpassade risk- och sårbarhetsanalyser (RSA).

Varje förvaltning och bolag i staden ska genomföra risk- och sårbarhetsanalyser för sina områden, och därigenom identifiera

- De viktiga samhällsfunktioner som de ansvarar för
- Vilka typer av händelser som kan få en negativ påverkan på den viktiga verksamheten
- Genomföra kontinuitetshantering för att minimera konsekvenserna och snabbt återgå till normalläge om något skulle inträffa.

Under 2024 har fastighetskontoret genomfört och fastställt en risk- och sårbarhetsanalys och levererats till Stadsledningskontoret som en del i Stockholms stads risk- och sårbarhetsanalys. Analysens har främst varit fokuserad på konsekvensanalys utifrån

samhällsviktig verksamhet och kritiska beroenden och inte perspektivet informationssäkerhet. Under 2026 kommer en riskanalys genomföras inom ramen för fastighetskontorets systematiska informationsklassningsarbete.

2.1.5 Resultatet från egen uppföljning

Intern kontroll (IK) bidrar till att verksamheten når sina mål (effektivitet, säkerhet och stabilitet), att informationen och rapporteringen om verksamheten och ekonomin är tillförlitlig och rättvisande och att verksamheten efterlever lagar, regler, avtal mm. Den interna kontrollen behöver följas upp och analyseras. Resultatet återkopplas till ansvarig nämnd. Nämnderna ska bedöma och rapportera den interna kontrollen i verksamhetsberättelsen. Nämndernas bedömningar ligger till grund för en samlad bedömning som kommunstyrelsen gör i årsredovisningen.

Det finns inte ett formellt krav på att arbeta med interna kontrollplaner. Men verktyget har blivit etablerat som arbetsmetod. En kontrollplan hjälper till att ”ha koll på kollen”.

Fastighetskontorets arbete med Väsentlighets- och riskanalys och Internkontrollplan genomförs enligt instruktion från Stadsledningskontoret, där systematiskt informationssäkerhetsarbete är ett område. Hela verksamheten är indelade i processer t.ex. systematiskt informationssäkerhetsarbete och under respektive process finns minst ett arbetssätt/en delprocess t.ex. behörighetshantering.

Fastighetskontorets arbete med internkontroll och väsentlighets- och riskanalys har under året genomförts enligt plan och risker har identifierats och värderats under den obligatoriska processen systematisk informationssäkerhet.

2.1.6 Risker som identifierats i GDPR-årsrapport

GDPR-årsrapport skrivs vanligtvis av ansvarigt dataskyddsombud och omfattar följande obligatoriska rapporteringsområden:

- Registerförteckning
- Styrdokument
- Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- Konsekvensbedömningar
- Individens rättigheter
- Personuppgiftsincidenter

En GDPR-årsrapport är under framtagande och ska vara klar i december 2025. Samtliga obligatoriska rapporteringsområden enligt ovan kommer att omhändertas.

2.1.7 Information om avvikelser (incidenter och andra händelser)

Fastighetskontoret använder det stadsgemensamma systemet IA för att hantera incidenter och händelser som kan orsaka eller har orsakat skada på människa, miljö eller egendom. Alla anställda kan gå in och skapa ett ärende via Intranätet. Via IA-systemet hanteras idag främst

incidenter om medarbetare och personal *(rapporteras löpande i förvaltningsgruppen)* men dessutom incidenter som berör den byggda miljön t ex om det ska bli ett försäkringsvärde.

Nuvarande system har följande möjlighet till kategorisering:

- Riskobservation
- Tillbud
- Olycksfall
- Färdolycksfall
- Arbetssjukdom
- Egendom/säkerhet och Miljö*

**Under kategorin egendom/säkerhet anges t ex dataintrång och informationsförlust som exempel.*

Under den senaste 12 månaders-perioden har 2 st. incidenter/händelser rapporterats avseende informationssäkerhet. Dessa två incidenter avser en personuppgiftsincident hos en extern leverantör samt en personuppgiftincident kopplat till Miljödatahändelsen. Det låga antalet av rapporterade informationssäkerhetsincidenter bedöms bero på att rutinen för att rapportera dataintrång och informationsförlust inte är tillräckligt etablerad i verksamheten.

Nuvarande IT-system, IA, för registrering av incidenter är fokuserat på HR-incidenter. En översyn av detta system bör genomföras, så att även informationssäkerhetsincidenter kan kategoriseras (med underkategorier) och följas upp.

3. Förbättringar som föreslås för verksamhetens LIS

3.1 Förbättringsaktiviteter under 2026

- Fortsatt kartläggning och klassning av tillkommande information som verksamheten använder.
- Löpande uppföljning och komplettering av informationsansvar samt utbildning i organisationen.
- Färdigställande av hanteringsinstruktioner som verksamheten kan följa baserad på informationens klassning.
- Fokusera på att planera för, och genomföra, riskreducerande åtgärder för samhällsviktig verksamhet med utgångspunkt av resultatet av föregående års risk- och sårbarhetsanalys (RSA).
- Genomföra en riskanalys inom ramen för fastighetskontorets systematiska informationsklassningsarbete.
- Framtagande och fastställande av en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom fastighetskontoret.

- Informationsklassningen med hänsyn till eventuella styrningar från säkerhetsskyddslagen *(2018:585)* och med eventuella tillkommande säkerhetsåtgärder.
- Tydliggöra ansvarsfördelning för informationssäkerhet i kontorets delegationsordning.
- Generella obligatoriska kompetenshöjande åtgärder inom informationssäkerhet.
- Riktade kompetenshöjande åtgärder inom informationssäkerhet utifrån identifierade målgrupper.

3.2 Förbättringsaktiviteter under 2027

- Implementera nya arbetssätt inom informationssäkerhetsområdet, och vid behov revidera och justera befintliga arbetssätt. Löpande kontroll och uppföljning upp det systematiska informationssäkerhetsarbetet inom fastighetskontoret.
- Uppdatera/revidera fastighetskontorets riskanalys.
- Uppföljning av genomförda och planerade aktiviteter.
- Ta fram förvaltningsspecifika mål för det systematiska informationssäkerhetsarbetet.
- Generella obligatoriska kompetenshöjande åtgärder inom informationssäkerhet.

3.3 Förbättringsaktiviteter under 2028

- Fortsätta implementera och tillämpa nya arbetssätt inom informationssäkerhetsområdet, och vid behov revidera och justera befintliga arbetssätt. Löpande kontroll och uppföljning upp det systematiska informationssäkerhetsarbetet inom fastighetskontoret.
- Uppdatera/revidera fastighetskontorets riskanalys.
- Uppföljning av genomförda och planerade aktiviteter.
- Ta fram förvaltningsspecifika mål för det systematiska informationssäkerhetsarbetet.
- Generella obligatoriska kompetenshöjande åtgärder inom informationssäkerhet.