Ledningens genomgång år 2026

Skarpnäcks stadsdelsförvaltning

Beslutad 2025-12-18

Ledningens genomgång

Dnr: SKA

Kontaktperson: Boris Graje Informationssäkersamordnare, Julia Ögren Dataskyddsombud

1 Sammanfattning

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 Stockholm 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 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 med 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 2024 uppmanades samtliga nämnder och bolagsstyrelser att ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbete under de kommande tre åren. Denna ska biläggas till verksamhetsplan. Planeringen för de återkommande tre åren ska utgå från nämndens verksamhetsuppdrag i budget och följa Riktlinje för informationssäkerhet i Stockholm stad.

Dessa aktiviteter ska redovisas både i Ledningens genomgång samt i nämndens verksamhetsplan under mål 3.5. Inventering och informationsklassning är grunden i informationssäkerhetsarbetet. För att stärka informationssäkerhetsarbetet ska förvaltningen under 2026 utreda formerna för ett införande av PM3 som systemförvaltning.

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.

---

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet
[2] anvisningar-for-namndernas-arbete-med-verksamhetsplan-2024.pdf (stockholm.se)

Innehållsförteckning

1.1 Faktorer som påverkar Skarpnäcks stadsdelsförvaltning, LIS

Stockholms stads arbete med informationssäkerhet utgår från en så kallad ISO standard, ISO 27001. 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 ger en IT-process som är lättare att hantera, mäta och förbättra.

Stockholms stads informationssäkerhetsarbete regleras i en tillämpningsanvisning som är en bilaga till stadens Kvalitetsprogram[1]. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Skarpnäcks stadsdelsförvaltning har en så kallad lokal anvisning som beskriver stadens övergripande ledningssystem för informationssäkerhet tagits fram under 2025.

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Skarpnäcks 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.

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

I stadens budget för 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.

Förvaltningen utvecklar arbetet med en systematisk informationshantering och arkiv, vilket ger ett effektivt stöd och bidrar till att utveckla verksamheternas kvalitet i linje med stadens kvalitetsprogram. Förvaltningen utvecklar arbetet för en god

[1] Stockholms stads kvalitetsprogram (start.stockholm)

informationshantering och vidtar åtgärder avseende arkiv och bevarande av handlingar.

Förvaltningen stärker systematik, organisation och kunskap i verksamheterna avseende dataskyddsarbete och personuppgiftshantering. Detta sker bland annat genom att genomföra utbildningar och utveckla och tillgängliggöra gemensamma och verksamhetsspecifika rutiner.

För att säkerställa en god kännedom om gällande lagar och rutiner kommer förvaltningen arbeta för att fler chefer och medarbetare genomför stadens utbildning i informationssäkerhet och dataskydd.

Förvaltningen fortsätter att utveckla det systematiska informationssäkerhetsarbetet genom att implementera de arbetssätt som tagits fram tidigare år och som beskrivs i den lokala anvisningen. I detta arbete kommer intensifiering av genomförande av informationsklassningar inta en central del.

1.1.2 Risker som identifierats i GDPR-årsrapport

I GDPR årsrapport för 2024 identifierade dataskyddsombudet risker kopplade till låga kunskaper om dataskyddsregler samt hanteringen av känsliga personuppgifter som kan innebära hög risk för registrerades fri- och rättigheter. Risken kopplat till hanteringen av känsliga personuppgifter bedömdes vara allvarlig och krävde omgående insatser från ledning och övriga chefer. Dataskyddsombudet gav i rapporten rådet att den allvarliga risken kunde avhjälpas av att förvaltningen utifrån ett riskbaserat arbetssätt, klassar och konsekvens bedömer system och behandlingar där känsliga personuppgifter hanteras i stora mängder så att risker kan förebyggas på det sätt som dataskyddsförordningen kräver.

1.1.3 Information om avvikelser (incidenter och andra händelser)

Avseende personuppgiftsincidenter under 2025 (hittills inrapporterade) har en majoritet av dessa rapporterats inom 72-timmarsgränsen. Det relativt stora antalet som rapporterats senare än 72 timmar indikerar dock ett förbättringsbehov. Felskickade e-postmeddelanden, felskickad post och felaktig hantering av fysiska dokument innehållande personuppgifter står för majoriteten av de inrapporterade incidenterna.

Under året har nämnden, tillsammans med resten av staden samt en mängd andra organisationer, drabbats av en större personuppgiftsincident rörande personaldata i ett kommande

arbetsmiljösystem. Berörda har informerats och de åtgärder som krävs har vidtagits samtidigt som incidenten har anmälts till myndigheterna. Staden arbetar fortsatt med att utreda vad som hänt och varför.

1.2 Förbättringar och Prioriteringar som föreslås för verksamhetens LIS

Lokal anvisning för informationssäkerhet
Förvaltningen har under 2025 tagit fram en lokal anvisning för informationssäkerhet. Med grunden av handlingsplanens 7 prioriteringsområden:
Lokal anvisning, Planering och uppföljning, Informationsklassning, Behörighetshantering, Incidenthantering, kontinuitetshantering och Anskaffning och utveckling av varor och tjänster.

Utbildningsinsatser för chefer och medarbetare
Förvaltningen ska sprida kunskap och utbildning till chefer och medarbetare.

- Förändring för e-utbildningar och certifiering, från och med den 1 januari 2026 kommer det inte längre att skickas ut automatiska påminnelser till medarbetare. Istället behöver Skarpnäcks SDF själva informera medarbetare om att de ska gå utbildningarna. Utbildning i informationssäkerhet och dataskydd kommer fortsatt vara ett krav för stadens medarbetare. Skarpnäcks SDF behöver ta fram en rutin för at informera medarbetarna om att de ska gå utbildningarna.

Genomföra inventering och klassning

- 2026 – Utreda formerna för ett införande av PM3- styr och samverkansmodell för underhåll och utveckling av IT stöd.
- Fokus på att klassa verksamhetsprocesser som är prioriterade enligt RSA. – Granska hur väl lokal rutin för regelbundna informationsklassningar följs.
- Fokus på att klassa verksamhetsprocesser som omfattas av NIS2. – Granska hur väl lokal rutin för regelbundna informationsklassningar följ
- Fokus på att riskanalyser av verksamheternas personuppgiftsbehandlingar genomförs och dokumenteras, samt att konsekvensbedömningar genomförs för de behandlingar som sannolikt leder till hög risk enligt artikel 35 dataskyddsförordningen.

- Förändring för e-utbildningar och certifiering, från och med den 1 januari 2026 kommer det inte längre att skickas ut automatiska påminnelser till medarbetare. Istället behöver Skarpnäcks SDF själva informera medarbetare om att de ska gå utbildningarna. Utbildning i informationssäkerhet och dataskydd kommer fortsatt vara ett krav för stadens medarbetare. Skarpnäcks SDF behöver ta fram en rutin för at informera medarbetarna om att de ska gå utbildningarna.
- Fortsatt fokus på att klassa verksamhetsprocesser som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter. – Underhåll inventeringen vad som har informationssäkerhetsklassats och vad som inte har klassats. Ta fram lokal rutin för regelbundna informationsklassningar.
- Fortsatt arbetet med riskanalyser av verksamheternas personuppgiftsbehandlingar, samt genomförande av konsekvensbedömningar för de behandlingar som sannolikt leder till hög risk enligt artikel 35 dataskyddsförordningen.
- 2027 – Fortsatt fokus på att klassa verksamhetsprocesser som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter. – Underhåll inventeringen vad som har informationssäkerhetsklassats och vad som inte har klassats. Ta fram lokal rutin för regelbundna informationsklassningar.
- Fortsatt arbetet med riskanalyser av verksamheternas personuppgiftsbehandlingar, samt genomförande av konsekvensbedömningar för de behandlingar som sannolikt leder till hög risk enligt artikel 35 dataskyddsförordningen.
- Fokus på att klassa verksamhetsprocesser som är prioriterade enligt RSA. – Granska hur väl lokal rutin för regelbundna informationsklassningar följs.
- Fokus på att klassa verksamhetsprocesser som omfattas av NIS2. – Granska hur väl lokal rutin för regelbundna informationsklassningar följ
- 2028 – Fortsatt fokus på att klassa verksamhetsprocesser som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter. – Underhåll inventeringen vad som har informationssäkerhetsklassats och vad som inte har klassats. Ta fram lokal rutin för regelbundna informationsklassningar.
- Fortsatt arbetet med riskanalyser av verksamheternas personuppgiftsbehandlingar, samt genomförande av konsekvensbedömningar för de behandlingar som sannolikt leder till hög risk enligt artikel 35 dataskyddsförordningen.

- Fokus på att klassa verksamhetsprocesser som är prioriterade enligt RSA. – Granska hur väl lokal rutin för regelbundna informationsklassningar följs.
- Fokus på att klassa verksamhetsprocesser som omfattas av NIS2. – Granska hur väl lokal rutin för regelbundna informationsklassningar följ

- **Följa upp behörigheter**

  Genomföra rutin för kontroller för behörigheter och resursägare