Ledningens genomgång år 2026

Norra innerstadens stadsdelsnämnd

Ledningens genomgång

Dnr: NI 2025/1801
Kontaktperson: Camilla Gezelius Tebrand

Sammanfattning

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef inhämta en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten redogör exempelvis för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare eller om informationsklassningar och registerförteckning är genomförda. Ledningens genomgång innehåller även planering för informationssäkerhetsarbetet under de kommande tre åren.
I och med att världsläget är fortsatt oroligt innebär det att säkerhetsfrågor inklusive informationssäkerhet står högt på agendan både globalt och nationellt och så även inom Staden, särskilt efter dataläckaget hos Miljödata. Under januari 2026 träder en ny Cybersäkerhetslag i kraft och senare under året införlivas även CER-direktivet i en lag. I budgeten för 2026 har Stockholms stad därmed höjt ambitionerna ytterligare för arbetet med informationssäkerhet. Ett större anslag har reserverats för att finansiera en förstärkning av nämndernas arbete med informationssäkerhet.
Under 2025 har Norra innerstadens förvaltning påbörjat implementering av kontinuitetshöjande åtgärder utifrån arbetet med RSA och det arbetet fortskrider även kommande år. Utöver det systematiska informationssäkerhetsarbetet under 2025 har ett fokusområde varit informationsspridning av dataskydd det vill säga hantering av personuppgifter och incidenter samt att genomföra konsekvensbedömningar.
Under det kommande året behöver det fokuseras på att säkerställa att Norra innerstadens förvaltning efterlever de nya lagarna som träder i kraft under 2026. Ett område är att nå ut till chefer och medarbetare med vilket ansvar som följer med en roll och vad de kan bidra med för att höja säkerhetsförmågan gällande informationssäkerhet och dataskydd. Den lokala anvisningen som beskriver hur vi arbetar med informationssäkerhet kommer att revideras och kommuniceras. Anvisningen kommer att hänvisa till förvaltningsövergripande rutiner för incidenthantering, informationsklassningar inför upphandling och inköp, behörighetshantering och rutin för löpande hantering av registerförteckning.

Innehållsförteckning

1. Vad är Ledningens genomgång

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 riktlinje som är en bilaga till stadens Kvalitetsprogram[1]. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna[2][3] reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Norra innerstadens stadsdelsförvaltning har stadsdelsdirektören fastställt en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom förvaltningen.

1.2 Faktorer som påverkar verksamheten

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Norra innerstadens 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

Världsläget är fortsatt oroligt vilket innebär att säkerhetsfrågor inklusive informationssäkerhet står högt på agendan både globalt och nationellt.

1.2.2 Sverige och EU

Vi lever i ett digitaliserat samhälle, där samhällsviktig verksamhet vilar på digital grund och är beroende av IT och information. Digitaliseringen medför sårbarheter för nya typer av hot och incidenter i system och kan leda till störningar som i sin tur kan ge samhällskonsekvenser. Det sker allt fler cyberattacker som syftar

[1] Stockholms stads kvalitetsprogram (start.stockholm)
[2] Riktlinje för informationssäkerhet i Stockholms stad
[3] Tillämpningsanvisning till stadens riktlinjer för informationssäkerhet

till att både stjäla information och destabilisera verksamheter vilket kan få både säkerhetsmässiga och ekonomiska konsekvenser. De senaste åren har vi fått flera exempel på när alltifrån regioner och kommuner till it-leverantörer drabbats av allvarliga incidenter som fått stor påverkan på samhället. Det här gör i dagsläget informations- och cybersäkerhet till en central fråga för både den enskilda verksamheten som för samhällets motståndskraft i stort.

Inom EU har arbetet med att stärka motståndskraften i samhällsviktig verksamhet prioriterats de senaste åren och det arbetet fortgår. Syftet är att stärka förmågan att upprätthålla viktiga samhällsfunktioner inom hela unionen och NIS2-direktivet[4] planeras att implementeras i svensk lag och träda i kraft 15/1 2026 (cybersäkerhetslagen). En ny nationell strategi för samhällets informations- och cybersäkerhet[5] togs fram under 2025 i syfte att höja den nationella cybersäkerheten. CER-direktivet[6] kommer att införlivas i svensk lagstiftning genom en ny lag, "Lagen om motståndskraft hos kritiska verksamhetsutövare" och beräknas träda i kraft under 2026.

NIS2 (The Directive on security of network- and informationsystems part 2) syftar till att uppnå en hög gemensam cybersäkerhetsnivå inom EU gällande nätverk- och informationssystem. *CER (Directive on the recilience of critical entities)* ska säkerställa att störningar eller avbrott bland samhällsviktiga verksamheter kan förebyggas, motverkas, och hanteras. Man kan säga att CER omfattar samhällsviktig verksamhet som måste upprätthållas utöver nätverk och informationssystem (NIS).

Offentlig förvaltning är en av de sektorer som omfattas av NIS2 och kommer även att omfattas av CER, vilket medför att Stockholms Stads förvaltningar och bolag omfattas.

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

Det omfattande dataläckage[7] som drabbat stora delar av det offentliga Sverige under året visar på ett behov av att göra mer för att öka säkerheten. Dataläckaget kommer att utvärderas externt och

[4] Det här är NIS2-direktivet | MSB
[5] Nationell strategi för cybersäkerhet
[6] CER-direktivet - MSB
[7] Miljödataincidenten, augusti 2025

utifrån den utvärderingen finns det anledning att kunna göra en säkerhetsöversyn av relevanta delar av stadens centrala system.

CERT[8] Stockholm har tagits i drift under 2025 och är stadens gemensamma funktion för att förebygga, upptäcka och hantera it-säkerhetsincidenter. Funktionen är ett komplement till det it-säkerhetsarbete som redan bedrivs inom varje förvaltning och bolag.

I budget för 2026 höjs ambitionerna ytterligare för arbetet med informationssäkerhet. Ett större anslag reserveras för att finansiera en förstärkning av nämndernas arbete med informationssäkerhet.

Budgeten för 2026 tar även upp att verksamheter behöver utveckla och stärka arbetet med att beakta risker och sårbarheter med generativ AI och syntetisk media.

1.3 Vad har hänt inom förvaltningen under 2025 gällande informationssäkerhet och dataskydd

1.3.1 RSA-arbetet

Förvaltningens RSA-arbete har under 2025 fokuserat på att planera, påbörja implementering och även övning av de kontinuitetshöjande åtgärder av det som identifierades under 2024. Under kommande år fortgår dessa aktiviteter samtidigt som en ny RSA-cykel påbörjas 2026.

1.3.2 Resultat av 2025 års arbete med informationssäkerhet och dataskydd

- Förvaltningens chefer fick en introduktion på ett chefsmöte av bland annat innehållet i den lokala anvisningen för informationssäkerhet och information om vart dokumentet är publicerat.
- 13 stycken genomgångar av informationssäkerhet med extra fokus på personuppgiftshantering har hållits under året med olika verksamheter inom förvaltningen.
- 6 stycken nätverksträffar med förvaltningens utsedda dataskyddshandläggare har genomförts under året. Även

[8] Computer Emergency Response Team - samordnas av funktion vid S:t Erik Kommunikation AB

andra roller inom IT, inköp och upphandling och arkiv har deltagit.
- Årets uppmärksamhet under cybersäkerhetsmånaden fokuserade på informationsutskick i form av en affisch till hemtjänsten, äldreboenden och förskolor.
- Genomförandet av obligatorisk utbildningarna ”Informationssäkerhet för medarbetare i staden” och ”Grundutbildning i dataskydd” har en genomförandegrad på drygt 15 procent.[9] Det har skett en viss ökning jämfört med tidigare år.
- Incidenthantering
    - Arbete med framtagande av en övergripande incidenthanteringsprocess gällande informationssäkerhet har utformats och kommer att introduceras i början av 2026.
    - Förvaltningen har hanterat följande typer av incidenter inom informationssäkerhet under 2025.
        - Personuppgiftsincidenter
            - 41 stycken anmälda i IA varav 18 stycken har anmälts till IMY.
        - NIS-incidenter
            - inga incidenter har rapporterats.
        - IT-säkerhetsincidenter
            - MStart
        - Övriga informationssäkerhetsavvikelser
            - olika bluffmejl och sms
            - stöld av digitala enheter

- Informationsklassning
    - 17 stycken informationsklassningar (lokala och normerande) har under året hanterats eller är i slutfasen.
    - 2 stycken har avbrutits på grund av osäkra förhållanden[10]
    - Behovet av konsekvensbedömning enligt GDPR fastställs regelmässigt i samband med informationsklassning. Under året har nio konsekvensbedömningar med tillhörande riskanalys genomförts.

- Informationssäkerhet inom upphandlingsförfarandet

[9] ”Informationssäkerhet för medarbetare i staden” antal certifierade 463 stycken. ”Grundutbildning i dataskydd” antal certifierade 452 stycken.
[10] ”Säkra meddelanden” och ”Säkra digitala möten”

- Under 2025 har samarbetet med inköp- och upphandlingsansvariga fördjupats. Det har medfört att beställare av tjänster och system har fått information om att kontakta ISAM och DSO innan beställning genomförts. Informationsklassningar har därmed hanterats enligt stadens tillämpningsanvisning för informationsklassning.

1.3.3 Hantering av risker som identifierats i GDPR-årsrapport

- Bristfälliga informationsklassningar – otydlig information om vad som är planerat, genomfört och vad nästa steg är i processen.
    - Arbete har under året fokuserat på att göra en tydligare prioriteringslista över vilka informationsklassningar som genomförts och kommer att genomföras. I början på 2026 ska listan vara uppdaterad för kända informationstillgångar. Listan kommer att revideras löpande utifrån förvaltningens behov.

- Bristfälliga konsekvensbedömningar – inga konsekvensbedömningar genomfördes under 2024 inom förvaltningen.
    - Rutinmässig bedömning av behov av konsekvensbedömning enligt GDPR infördes i april 2025
    - Bedömning görs genom tröskelanalys i de fall det finns tveksamheter om konsekvensbedömning behöver göras
    - Som mallar för tröskelanalys, konsekvensbedömning samt riskanalys används nya mallar som framtagits av IMY (Integritetsskyddsmyndigheten)
    - Under året har nio konsekvensbedömningar genomförts

- Revidera rutin för att tillgodose de registrerades rättigheter och komplettera process med tydlig ansvarsfördelning mellan olika roller i processen
    - Rutin har reviderats och kompletterats med process med ansvarsfördelning
    - Det nya arbetssättet implementerades i april 2025

    - Rutinen har därefter justerats vid ett par tillfällen efter att den testats i praktiken och förbättringsområden identifierats

1.4 Förbättringar som föreslås för verksamheten

Under 2026 ska förvaltningen prioritera att:

- säkerställa efterlevnaden av befintlig och ny lagstiftning (Cybersäkerhetslagen och kommande CER-direktivet) samt Stadens riktlinjer och tillämpningsanvisningar gällande informationssäkerhet,
- revidera och kommunicera ”Lokal anvisning för informationssäkerhet”,
- fastställa krav på säkerhetsåtgärder vid informationsklassningar inför inköp- och upphandling, vid licensförnyelse och vid uppföljning av befintliga informationstillgångar,
- informationsklassningar genomförs på informationssystem, tjänster och som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter samt verksamhetsprocesser som är prioriterade enligt RSA,
- ta fram en förvaltningsövergripande rutin för behörighetshantering
- färdigställa lokal rutin som knyter an till den lokala upphandlingsprocessen med syfte att beakta informationssäkerhetskrav vid införande av nya tjänster och system,
- rutin för löpande uppdatering av registerförteckning formuleras och implementeras,
- färdigställa, implementera och kommunicera en förvaltningsövergripande incidenthanteringsrutin gällande informationssäkerhet.

Arbete kommer även att ske med att:

- genomföra träffar för dataskyddsnätverket
- genomföra kunskapshöjande åtgärder för chefer och medarbetare med fokus på:
    - införskaffande av nya tjänster och system
    - incidenthantering
    - hantering av behörigheter
    - leverantörsuppföljning
- verka för att verksamheter tar eget ansvar för löpande översyn av befintliga klassningar i samråd med ISAM och DSO

- ISAM och DSO deltar i staden övergripande nätverk och omvärldsbevakar och fördjupar oss inom informationssäkerhet och dataskydd.
- Inventering av förekomst av information som ges till registrerade inför påbörjad personuppgiftsbehandling och stötta verksamheterna i kompletteringar där brister upptäcks.

Förbättringsaktiviteter för 2027:

- Fortsätta med det systematiska informationssäkerhetsarbetet
    - genomföra informationsklassningar
    - planera, genomföra och följa upp informationssäkerhetshöjande åtgärder
    - säkerställa att efterlevnaden av lagar och Stadens riktlinjer för informationssäkerhet
    - omvärldsbevaka
    - vid behov översyn av lokala rutiner

Förbättringsaktiviteter för 2028:

- genomföra informationsklassningar
- planera, genomföra och följa upp informationssäkerhetshöjande åtgärder
- säkerställa att efterlevnaden av lagar och Stadens riktlinjer för informationssäkerhet
- omvärldsbevaka
- vid behov översyn av lokala rutiner

Underskriftens äkthet valideras här: https://underskriftpas.stockholm.se/validera

Signerad av
Jesper Ackinger

Signaturdatum
2025-11-24 12:32:08

Elektronisk underskrift

underskrift.stockholm.se