Ledningens genomgång år 2025

Kungsholmens stadsdelsnämnd

Beslutad 202512

Ledningens genomgång

Dnr: KUNG 2025/540

Kontaktperson: Frida Mattsson

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 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 samt om informationsklassningar och registerförteckning är genomförda.
Denna rapportering ska ge information och underlag till förvaltningschef och övrig förvaltningsledning att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

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 reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Kungsholmens 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 verksamhetens informationssäkerhetsarbete

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Kungsholmens 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 och trender

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

[1] Stockholms stads kvalitetsprogram (start.stockholm)

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 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[2] implementeras i svensk lag och väntas träda i kraft under januari 2026.

NIS2 syftar till att uppnå en hög gemensam cybersäkerhetsnivå inom EU gällande nätverk- och informationssystem. Offentlig förvaltning är en av de sektorer som omfattas av NIS2.

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

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

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

CERT[3] Stockholm har tagits i drift under 2025 och är stadens gemensamma funktion för att förebygga, upptäcka och hantera it-

[2] Det här är NIS2-direktivet | MSB
[3] Computer Emergency Response Team - samordnas av funktion vid S:t Erik Kommunikation AB

säkerhetsincidenter. Funktionen är ett komplement till det IT-säkerhetsarbete som redan bedrivs inom varje förvaltning och bolag.

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

Förvaltningen hade under informationssäkerhetsmånaden en kampanj som syftade till att höja medvetenheten om informationssäkerhet och dataskydd.
ISAM och DSO har bjudits in till klassningar inför upphandling av digitala verktyg vilket kan ses som en god utveckling i det systematiska informationssäkerhetsarbetet.
Informationsklassningar har genomförts på befintliga informationstillgångar och ISAM samt DSO har även deltagit på flera normerande klassningar centralt.
Cirka 16% av förvaltningens medarbetare har genomfört de obligatoriska utbildningarna i informationssäkerhet och dataskydd.

1.3.1 Risker som identifierats i GDPR-årsrapport

- Otydlighet i hantering av registerförteckningen
- De lokala anvisningarna för informationssäkerhet är inte kända för alla och rollerna inte tillsatta

1.3.2 Information om avvikelser (incidenter och andra händelser)

1 NIS- incident har rapporterats till MSB
21 personuppgiftsincidenter varav
3 rapporterats till IMY
Informationsincidenter:
6 incidenter om phishing är rapporterade i IA
2 inbrott är rapporterade
3 rapporterade förluster av tjänstekort,
6 förluster av personliga mobiltelefoner
3 förluster av personliga datorer

1.4 Prioriterat arbete som föreslås

2026 –

NIS2
Säkerställa efterlevnad av nya cybersäkerhetslagen

Uppdatera Lokal anvisning
Revidera Lokal anvisning för informationssäkerhet

Informationsklassning
informationsklassningar genomförs på informationssystem som innehåller känslig information och personuppgifter

Behörighetsrutin
Ta fram en förvaltningsövergripande rutin för behörighetshantering

Rutin för informationssäkerhetsincident
Ta fram en rutin för informationssäkerhetsincident

Registerförteckning
Ta fram rutin för löpande uppdatering av registerförteckning

2027 –

- Genomföra informationsklassningar.
- Säkerställa efterlevnaden av lagar och stadens riktlinjer för informationssäkerhet.
- Omvärldsbevaka
- Vid behov göra en översyn av lokala rutiner