Ledningens genomgång år 2024

Enskede-Årsta-Vantörs stadsdelsnämnd

Beslutad 2023-11-23

Ledningens genomgång

Dnr: EÅV 2023/980

Kontaktperson: Linnea Kleiner

Bakgrund

Enligt *Tillämpningsanvisning till stadens riktlinje 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 eller om informationsklassningar och registerförteckning är genomförda.

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

Enligt *Anvisningar för nämndernas arbete med verksamhetsplan 2024* ska samtliga nämnder och bolagsstyrelser ta fram en *Ledningens genomgång* med en planering för informationssäkerhetsarbetet under de kommande tre åren. Dokumentet ska biläggas verksamhetsplanen. Planeringen för de kommande tre åren ska utgå från nämndens verksamhetsuppdrag i budget och följa *Riktlinje för informationssäkerhet i Stockholms stad*. En riskanalys ska även genomföras för att identifiera vilka aktiviteter som ska prioriteras till år 2024.

Aktiviteter ska redovisas i *Ledningens genomgång* och i nämndens verksamhetsplan under mål *3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden*.

Anvisningarna fastställer att området registerförteckning och informationsklassning är särskilt prioriterat i *Ledningens genomgång* för år 2024. 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.

Innehållsförteckning

1 Status för åtgärder från ledningens tidigare genomgångar

Förvaltningen har påbörjat arbetet med att ta fram en incidentrutin, arbetet kommer fortsätta 2024. Informationsklassning har haft stort fokus under året och antalet informationsklassade system har ökat med 20 procentenheter, från 30 procent till 50 procent, sedan 2022. Förvaltningen har även arbetat med behörighetshantering och stickprovskontroller. Under december har förvaltningsledningen och informationssäkerhetssamordnare deltagit i en kompetenshöjande satsning med konsulter genom stadsledningskontoret.

2 Ledningssystem för informationssäkerhet, LIS

Stockholms stads arbete med informationssäkerhet utgår från 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 Stockholms stads Kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För Enskede-Årsta-Vantörs stadsdelsnämnd räkning har förvaltningschef fastställt en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom förvaltningen.

3 Faktorer som påverkar

3.1 NIS-direktivet

Den 14 december 2022 antog EU-kommissionen två nya EU-direktiv: direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) och direktivet om kritiska entiteters motståndskraft (CER-direktivet).

NIS2-direktivet omfattar nya sektorer. Den 23 februari 2023 fattade regeringen beslut om att ge en särskild utredare i uppdrag att föreslå de anpassningar av svensk rätt som är nödvändiga för att NIS 2-direktivet och CER-direktivet ska kunna genomföras. Uppdraget ska redovisas senast 23 februari 2024 och kommer tydliggöra innebörden av NIS-2 för kommuner. Direktiven ska börja tillämpas den 18 oktober 2024.

3.2 Tredjelandsöverföring

I juli 2023 fattade EU-kommissionen ett beslut om adekvat skyddsnivå för USA, förutsatt att organisationen/leverantören omfattas av EU-U.S. Data Privacy Framework. Det nya EU-beslutet ger kommuner större möjligheter att använda USA-ägda molntjänster.

Stadens styrgrupp för informationssäkerhet uppmanar fortsatt till återhållsamhet kring amerikanska molntjänster och har tagit fram ett nytt inriktningsbeslut för molntjänster. Inriktningsbeslutet innebär bland annat att inga stora införanden av nya stadsgemensamma molntjänster kommer att genomföras i dagsläget som en följd av det senaste EU-beslutet.

3.3 Finansborgarrådets förslag till budget 2024

Stockholms stads budget 2024 fastställer att informationssäkerhetsarbetet och incidenthanteringsförmågan behöver utvecklas för att stärka förmågan till god informationshantering som en förutsättning och ett led i kvalitets- och utvecklingsarbetet.

Förvaltningen bedömer att det är centralt med ett ökat fokus på informationssäkerhet till följd av det rådande omvärldsläget.

3.4 Intern kontroll

Syftet med intern kontroll är att skapa förutsättningar för en ändamålsenlig och effektiv användning av skattemedel samt för att upprätthålla service med hög kvalitet till kommuninvånarna.

Genom en tillräcklig intern kontroll skapas förutsättningar att förebygga, upptäcka och åtgärda oönskade händelser och därmed minimera risker i verksamheten samt säkra tillgångar och förhindra förluster och oegentligheter som skadar stadens anseende. Arbetet med intern kontroll är en del av stadens kvalitetsarbete.

Den interna kontrollen ska vara utformad för att med rimlig grad av säkerhet kunna uppnå följande:

- att verksamheten är ändamålsenlig och effektiv
- att information om verksamhet och ekonomi är tillförlitlig och rättvisande
- att lagar, förordningar, föreskrifter och styrdokument följs.

Utöver nämndens egna identifierade processer ska nämnden, enligt stadens anvisning, ha med den obligatoriska stadsövergripande processen *Systematiskt informationssäkerhetsarbete* i sin väsentlighets- och riskanalys och bedöma om de ska med i internkontrollplanen. För 2024 har förvaltningen bedömt att endast *behörighetshantering* kommer ingå i interkontrollplanen.

3.5 Risk- och sårbarhetsanalys (RSA)

Risk- och sårbarhetsanalyser är en analys av händelser som kan inträffa, identifiering av samhällsviktiga verksamheter och beroenden, analys av risker och sårbarheter samt behov av åtgärder.

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. Förvaltningen följer stadens risk- och sårbarhetscykel och instruktioner. Analys och framtagande av åtgärder genomfördes under 2022. Införande av valda åtgärder samt uppföljning har skett under 2023. En ny cykel inleds under 2024 där ytterligare fokus kommer läggas på informationssäkerhet i samarbete med förvaltningens säkerhetssamordnare.

4 Resultatet från egen uppföljning

4.1 Internkontrollplan (IKP)

I Enskede-Årsta-Vantörs stadsdelsnämnds tertialrapport 2023 rapporterades att förvaltningen fortsatt arbetet med att stärka behörighetshanteringen. Vissa avvikelser hade identifierats vid stickprovskontroller. Två avvikelser identifierades även vid stickprovskontroll av ansvarsområden inom informationssäkerhet, som då var åtgärdade.
Stickprovskontroller kommer fortsätta under 2024 och behörighetsrutiner kommer ses över för att säkerställa en god informationshantering.

4.2 Revisionsresultat

4.2.1 Revisionsrapport

I revisionsrapport Nr 5/2019 lämnade stadsrevisionen rekommendation avseende *Implementering av dataskyddsförordningen.* Nämnden rekommenderades att informationsklassificera sina informationstillgångar samt att regelbundet och systematiskt inventera sina personuppgiftsbehandlingar.

I årsrapporten för 2022, dnr RVK 2023/22, ansågs nämnden ha vidtagit åtgärder. Stadsrevisionen framförde att det i dataskyddsombudets årsrapport framkom att registerförteckningen till största del är fullständig och aktuell samt att det finns en rutin för inventering av personuppgiftsbehandlingar. Vidare anges att informationstillgångarna har klassificerats.

4.3 Risker som identifierats i GDPR-årsrapport

Avseende *Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar* bedömde inte dataskyddsombudet att bristerna var lika omfattande i årsrapporten 2022 som 2021 samt att de brister som återstår inte är nämnvärda. Detta eftersom informationssäkerhetssamordnaren hade upprättat en prioritetsordning för informationsklassningarna och påbörjat arbetet enligt dataskyddsombudets rekommendation i 2021 års årsrapport.

Dataskyddsombudet fastställde samtidigt flertalet rekommendationer till nämnden:

1. Ge informationssäkerhetssamordnaren i uppdrag att, i samråd med dataskyddsombudet, uppdatera rutinen för hantering av personuppgiftsincidenter
2. Ger informationssäkerhetssamordnaren i uppdrag att, i samråd med dataskyddsombudet, tydliggöra vem som ska vara dokumentägare för handboken för behandling av personuppgifter
3. Ge informationssäkerhetssamordnaren, i samråd med dataskyddsombudet, i uppdrag att se över resterande styrdokument och uppdatera dem vid behov
4. Ge informationssäkerhetssamordnaren i uppdrag att ta fram en skriftlig rutin för vad som ska göras vid förlust av arbetstelefon eller arbetsdator

Under 2023 har informationssäkerhetssamordnaren tydliggjort ägarskap av dokument (2) och sett över resterande dokument (3). Under 2024 kommer rutin för hantering av personuppgiftsincidenter (1) samt en ny rutin för informationssäkerhetsincidenter (4) tas fram i enlighet med verksamhetsplan 2024.

5 Möjligheter till förbättring av verksamhetens LIS

Förvaltningen ser möjligheter att förbättra verksamhetens systematiska informationssäkerhetsarbete efter förslag från kompetenslyftet från december 2023. Arbetet kommer ske prioriterat utifrån Deloittes handlingsplan.

5.1 Prioritering av åtgärder

5.1.1 2024

Under 2024 kommer Enskede-Årsta-Vantörs stadsdelsförvaltning fokusera på:

- Särskilt fokus på informationsklassning av verksamhetsprocesser som omfattas av NIS-direktivet
- Öka antalet medarbetare som har kunskap om informationssäkerhet genom bland annat stadens obligatoriska e-utbildningar
- Utredning och implementeringen av NIS-2
- Översyn av incidentrutiner
- Behörighetshantering
- Tydliggöra informationssäkerhetens roll i inköpsprocessen i samarbete med upphandlare

5.1.2 2025

Under 2025 kommer Enskede-Årsta-Vantörs stadsdelsförvaltning fokusera på:

- Särskilt fokus på informationsklassning av verksamhetsprocesser som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter
- Öka antalet medarbetare som har kunskap om informationssäkerhet genom bland annat stadens obligatoriska e-utbildningar
- Fortsatt arbete med NIS-2
- Revidera och se över kontinuitetsplaner
- Behörighetshantering

5.1.3 2026

- Särskilt fokus på informationsklassning av verksamhetsprocesser som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter
- Öka antalet medarbetare som har kunskap om informationssäkerhet genom bland annat stadens obligatoriska e-utbildningar
- Översyn av lokala rutiner

Fastställd av förvaltningschef Anders Carstorp
2023-11-23

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

Undertecknad av
Anders Carstorp

Datum
2023-11-23 15:51:22

Elektronisk underskrift

underskrift.stockholm.se