Bilaga 3:7

Stockholms stad

Ledningens genomgång år 2024

Skarpnäcks stadsdelsförvaltning

Beslutad 2024-01-25

Ledningens genomgång

Dnr: SKA 2023/634

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 uppmanas 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 2024 är därför området registerförteckning och informationsklassning särskild prioriterat i Ledningens genomgång.

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 ska en så kallad lokal anvisning som beskriver stadens övergripande ledningssystem för informationssäkerhet tas fram under 2024.

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

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 informationshantering och vidtar åtgärder avseende arkiv och bevarande av handlingar.

Förvaltningen stärker systematik, organisation och kunskap i verksamheterna avseende dataskyddsarbete och personuppgiftshantering. Ett systematiskt arbetssätt införs för att bidra till att personuppgiftshanteringen i verksamheterna sker i

[1] Stockholms stads kvalitetsprogram (start.stockholm)

enlighet med gällande lagstiftning och stadens riktlinjer. På så sätt fortsätter förvaltningen att genomföra insatser där dataskydd blir en integrerad del av ledningsarbetet och samtliga verksamheters kvalitetsarbete.

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 Resultatet från egen uppföljning (VoR och IKP)

Förvaltningen har under 2023 infört fyra arbetssätt för systematiskt informationssäkerhetsarbete inom ramen för väsentlighets- och riskanalysen. De fyra arbetssätten har varit behörighetshantering, incidenthantering, informationsklassning och informationssäkerhet inom upphandlingsförfarande. I verksamhetsplan för 2024 stärker vi arbetet så att väsentlighets- och riskanalysen även omfattar arbetssättet implementering av lokal anvisning. Till förvaltningens interkontrollplan lyfts incidenthantering (rapportering av informationssäkerhetsincidenter) och informationsklassning (uppföljning av att de implementerade kraven för genomförda klassningar fortfarande är tillräckliga).

1.1.3 Kompetenslyft ledningsgrupp

Under hösten 2023 genomfördes en workshop, med konsultstöd, med förvaltningsledningen, informationssäkerhetssamordnaren och säkerhetssamordnaren. Detta resulterade i en handlingsplan för informationssäkerhet med sju prioriteringsområden:
Lokal anvisning, Planering och uppföljning, Informationsklassning, Behörighetshantering, Incidenthantering, Kontinuitetshantering och Anskaffning och utveckling av varor och tjänster.

1.1.4 Risker som identifierats i GDPR-årsrapport

I GDPR-årsrapport för 2022 har dataskyddsombudet identifierat risker relaterat till verksamheternas kunskaper om GDPR. Bristen bedömdes vara omfattande, och dataskyddsombudet gav i rapporten rådet till personuppgiftsansvarig att arbeta för att stärka kunskaper om GDPR bland chefer och medarbetare bland annat genom

genomförande av den obligatoriska grundutbildningen och ökad information till de som hade rollen som personuppgiftsredogörare.

Under år 2023 har förvaltningen arbetat enligt råden bland annat genom att dataskyddsombudet bjudits in till chefsforum där ombudet utbildat i GDPR samt informerat om föreslagen utveckling av dataskyddsorganisationen i förvaltningen med förtydligat ansvar för chefer samt förslag om införande av rollen dataskyddssamordnare (tidigare personuppgiftsansvarig) med ett bredare uppdrag att sprida kunskap och delta i nätverk med dataskyddsombudet.

1.1.5 Information om avvikelser (incidenter och andra händelser)

Avseende personuppgiftsincidenter under 2023 (hittills rapporterade) har en majoritet av dessa rapporterats inom 72-timmarsgränsen, men antalet som rapporterats senare än 72 timmar indikerar behov av ytterligare information. En ny rutin för personuppgiftshantering beslutas och publiceras i december

1.2 Förbättringar och Prioriteringar som föreslås för verksamhetens LIS

Lokal anvisning för informationssäkerhet
Förvaltningen ska under 2024 ta fram en lokalanvisning 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.

Förvaltningen sprider information om och implementerar av lokala styrdokument för dataskyddsarbetet som beslutas i december 2023.

Utbildningsinsatser för chefer och medarbetare
Förvaltningen ska sprida kunskap och utbildning till chefer och medarbetare. Staden har nya obligatoriska digitala utbildningar under 2024 med start januari nya nano utbildningar som kommer att skickas ut 1 gång per månad, nano utbildningarna är ca 5-7 minuter långa. Cheferna gör utbildningen själv medan medarbetarens ska göras tillsammans på t ex ett enhetsmöte eller APT.

Olika teman varje månad, varje tema har även en fråga som ska reflekteras i arbetsgrupp exempel: Varför är det viktigt med informationssäkerhet?

Genomföra inventering och klassning
Inventering och klassning ska genomföras enligt följande plan.

- 2024 – Fokus på att klassa verksamhetsprocesser som innehåller stora volymer av integritetskänsliga och känsliga personuppgifter. – Inventera vad som har informationssäkerhetsklassats och vad som inte har klassats. – Ta fram lokal rutin för regelbundna informationsklassningar.
  2024 – arbetet med registerförteckningen stärks genom införande av systematiskt arbetssätt med påminnelse om uppdatering samt periodisk granskning av arbetet.
  2024 – påbörja arbetet med riskanalyser av verksamheternas personuppgiftsbehandlingar, samt genomförande av konsekvensbedömningar för de behandlingar som sannolikt leder till hög risk enligt artikel 35 dataskyddsförordningen.

- 2025 – fokus på att klassa verksamhetsprocesser som omfattas av NIS. – Granska hur väl lokal rutin för regelbundna informationsklassningar följs.
  2025 - 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.

- 2026 – fokus på att klassa verksamhetsprocesser som är prioriterade enligt RSA. – Granska hur väl lokal rutin för regelbundna informationsklassningar följs.

  Följa upp behörigheter
  Genomföra rutin för kontroller för behörigheter och resursägare