Stockholms stad

Informationssäkerhet

Ledningens genomgång år 2024

Norra innerstadens stadsdelsförvaltning

Ledningens genomgång
Bilaga till Norra innerstadens SDF Verksamhetsplan 2024
Dnr: 2023/1137
Kontaktperson: Camilla Tebrand, ISAM

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 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

Denna rapportering ska ge information och underlag till förvaltningschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

Innehållsförteckning

1 Riktlinje för informationssäkerhet

Kommunfullmäktige har fastställt riktlinjerna för informationssäkerhet i staden. Riktlinjerna består dels av övergripande mål och principer för informationssäkerhetsarbetet och dels av följande sju fördjupade tillämpningsanvisningar:

1. Ansvar och roller inom informationssäkerhet
2. Kartläggning och klassning av information
3. Identitet och åtkomst
4. Anskaffning och utveckling av varor och tjänster
5. Drift och förvaltning av IT-tjänster
6. Incidenthantering och kontinuitetshantering
7. Loggning och spårbarhet.

Riktlinjen och tillämpningsanvisningarna ska tillämpas i arbetet med informationssäkerhet inom samtliga nämnder och bolagsstyrelser i Stockholms stad. Riktlinjen och tillämpningsanvisningarna ska även tillämpas i arbetet med dataskydd som följer av dataskyddslagstiftningen, det vill säga dessa krav samordnas inom ramen för samma styrdokument.

1.1 Lokal anvisning för informationssäkerhet

Lokal anvisning för informationssäkerhet för Norra innerstaden beslutas i samband med verksamhetsplan 2024.

1.2 Resultatet från egen uppföljning (IKP)

I förvaltningens tertialrapport 2 2023 rapporterades:

- att vissa avvikelser gällande det förvaltningsövergripande arbetet med informationssäkerhet att kontroller gällande utbildningar inte har kunnat genomföras
- att det förvaltningsövergripande rådet för informationssäkerhet och GDPR inte har kunnat implementeras efter att den nya förvaltningen har bildats

1.3 Verksamhetsplan

Aktiviteter som rör informationssäkerhet och dataskydd är implementerat i verksamhetsplan och arbetet med intern kontroll. I verksamhetsplan fastställs de aktiviteter, risker, kontroller och eventuella åtgärder som ligger till grund för informationssäkerhetsarbetet nästkommande år.

2 Uppföljning informationssäkerhetsarbete och dataskyddsarbete

Förvaltningens årshjul för informationssäkerhet följer arbetet med verksamhetsplan och de aktiviteter som fastställts, samt kontroller och eventuella åtgärder som identifierats i samband med väsentlighet- och riskanalysen.

Sammanställning och analys av det systematiska informationssäkerhetsarbetet redovisas i tertialrapporter, verksamhetsberättelse, väsentlighets- och riskanalys, intern kontrollplan, dataskyddsombudets årsrapport och i ledningens genomgång för informationssäkerhet.

2.1 Uppföljning 2023

2.1.1 Uppföljning Norra innerstadens stadsdelsförvaltning med start 1/7 2023

Vid halvårsskiftet 2023 bildades Norra innerstadens stadsdelsförvaltning.
Fokus efter sammanläggningen har varit att:

- kartlägga behov och nuläge
- hantera incidenter
- genomföra informationsklassningar för att få en samsyn utifrån metodiken
- fokusera på informationsklassningar av nya system
- inventera befintliga rutiner,
- identifiera behov av nya rutiner
- beskriva behovet av ett nätverk för dataskyddshandläggare

Inom staden har de obligatoriska utbildningarna i informationssäkerhet och dataskydd blivit certifierande.

2.1.2 Uppföljning av årsrapport för GDPR och verksamhetsplan visar:

2.1.2.1 Identifierade behov

- Starta upp nätverket för dataskyddshandläggare i syfte att ge ett mer ändamålsenligt och rättssäkert informationssäkerhetsarbete.

- Informera om vikten av att gå de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd.

- Att mer tydligt koppla samman informationssäkerheten med metodstödet pm3. För att omhänderta tillämpningsanvisningarna för informationssäkerhet krävs kunskap i stadens objektstyrning.

- Se över incidenthanteringsprocessen för så många typer av incidenter som möjligt (informations/IT-säkerhet, dataskydd, arbetsmiljö) som bidrar till snabb identifiering, bedömning, hantering och återställning.

- Säkerställa att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbete som pågår inom verksamheten
-

2.1.2.2 Risker som identifierats i GDPR-årsrapport

- Bristfälliga informationsklassningar – Risk att förvaltningen inte säkerställer att behandlingar genomgått informationsklassning och därmed att samtliga tekniska och organisatoriska åtgärder för att skydda registrerade inte är vidtagna.

- Bristfälliga konsekvensbedömningar – Risk att förvaltningen inte identifierar behandlingar av personuppgifter som innebär en hög risk för den registrerades integritet, rättigheter och friheter inte identifieras och att åtgärder för att förhindra att riskerna införlivas därmed inte vidtas.

- Bristande organisation för ett ändamålsenligt och rättssäkert informationssäkerhetsarbete

3 Utveckling av lokalt informationssäkerhetsarbete och dataskyddsarbete Informationsklassning

3.1 Verksamhetsplan 2024

Norra innerstadens stadsdelsförvaltning har bedömt att nedanstående arbetssätt ska ingå i intern kontrollplan

- behörighetshantering,
- implementering av lokal anvisning,
- incidenthantering,
- informationsklassning
- informationssäkerhet inom upphandlingsförfarandet
- registerförteckning över personuppgifter

Prioriterade områden:
- förankra, fastställa och implementera lokal anvisning för informationssäkerhet
- etablera nätverket för dataskyddshandläggare
- identifiera, utveckla och/eller revidera samt informera om rutiner och hanteringsanvisningar för att tydliggöra informationssäkerhet
- tillse att nya och befintliga informationstillgångar är klassade efter en framtagen prioriteringsordning
- tillse att handlingsplaner från klassning tas om hand, t ex behörighetshantering
- följer upp och utreder de incidenter som verksamheten anmäler i IA.
- utse objektledare för samtliga system
- informationssäkerhet i risk- och sårbarhetsanalys
- utveckla arbetet med kontinuitetsplanering
- utveckla arbetet med incidenthantering
- följa upp de obligatoriska utbildningarna i dataskydd och informationssäkerhet
- vara informerade och vara involverade i informationssäkerhetsarbetet som pågår centralt,

till exempel genom delta i normerande klassningar för system som omfattas av NIS enligt hälso- och sjukvårdslagen i samarbete med objektförvaltningen för aktuella system

- omvärldsbevaka och förbereda inför NIS2

3.2 Under 2025 ska Norra innerstadens stadsdelsförvaltning prioritera

- att etablera en rutin för regelbundna informationsklassningar och utbilda utsedda ansvariga att driva och genomföra dessa
- att etablera en gemensam incidenthanteringsprocess för så många typer av incidenter som möjligt (informations/IT-säkerhet, dataskydd, arbetsmiljö) som bidrar till snabb identifiering, bedömning, hantering och återställning.
- Utifrån RSA säkerställa kontinuitetsplaner finns.
- Följa upp och utvärdera den lokala anvisningen och om behov finns revidera den

3.3 Under 2026 ska Norra innerstadens stadsdelsförvaltning

Under 2026 ska förvaltningen prioritera:

- Revidering av lokal anvisning.
- Granska hur väl lokal rutin för regelbundna informationsklassningar följs.
- Öva utifrån kontinuitetsplaner.