Stockholms stad

Informationssäkerhet

- Ledningens genomgång 2024

Trafikkontoret

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/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 om 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 har 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 ska ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet under de kommande tre åren. Denna ska biläggas verksamhetsplan. Planeringen för de kommande tre åren ska utgå från nämndens verksamhetsuppdrag i budget och följa Riktlinje för informationssäkerhet i Stockholms 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 särskilt 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.

Innehållsförteckning

1. Ledningssystem för informationssäkerhet, 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. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. Trafikkontoret har under 2024 tagit fram en så kallad lokal anvisning, ”Trafikkontorets riktlinje för informationssäkerhetsarbete” som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom Trafikkontoret.

2. Trafikkontoret informationssäkerhetsarbete

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska Trafikkontoret 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.

Övergripande mål

Det övergripande målet med det systematiska informationssäkerhetsarbetet är att upprätthålla en väl avvägd informationssäkerhet med hänsyn till trafikkontoret och invånarnas behov. Informationssäkerhetsarbetet ska sträva efter rätt säkerhet, dvs. att balansera risker mot kostnader för skyddsåtgärder. Detta förutsätter att lagefterlevnaden inte äventyras.

Syftet med informationssäkerhetsarbetet är att säkerställa att trafikkontoret kan uppfylla sitt uppdrag som förvaltning genom att skydda kontorets informationstillgångar. Det innebär att skadebegränsa och skydda mot en stor mängd varierande hot såsom brand, ransomware, den mänskliga faktorn, stöld, intrång, lagöverträdelser etc.

Kommunfullmäktige har fastställt åtta vägledande mål och principer för informationssäkerhet. Dessa finns redovisade i stadsledningskontorets *Riktlinje för informationssäkerhet i Stockholms stad*. Nedan följer trafikkontorets tre övergripande informationssäkerhetsmål. Summerat omfattar dessa kommunfullmäktiges vägledning och klargör syftet med informationssäkerhetsarbetet hos trafikkontoret.

Informationssäkerhetsarbetet bidrar till att Trafikkontoret:

- Säkerställer och skyddar konfidentialitet, riktighet och tillgänglighet för kontorets informationstillgångar.
- Har invånarnas förtroende som en trygg och professionell organisation.
- Kontinuerligt säkrar efterlevnaden av personuppgiftslagen, offentlighets- och sekretesslagen samt andra tillämpliga lagar, förordningar och föreskrifter.

Styrning

Trafikkontorets ledningssystem för informationssäkerhet sätter ramarna för hur kontoret styr, genomför och följer upp informationssäkerhetsarbetet på ett systematiskt sätt. Mer konkret innebär detta mål och krav, metoder, rutiner, processer etc. Dessa ska medföra att vi arbetar styrt, riskbaserat och systematiskt där ledningen är medveten och engagerad med ständig förbättring i fokus.

Ledningssystemet för informationssäkerhet består av flera delar. Dels av styrdokument som är stadsövergripande och gäller för samtliga verksamheter. Dels av lokalt framtagna styrdokument som enbart gäller för den egna verksamheten. En beskrivning av de stadsövergripande styrdokumenten följer nedan.

- *Riktlinje för informationssäkerhet i Stockholms stad*. Styrdokumentet anger kommunfullmäktiges direktiv för stadens informationssäkerhetsarbete.
- Riktlinjen kompletteras med tillämpningsanvisningar som detaljerar krav för olika delområden i informationssäkerhetsarbetet, exempelvis informationsklassning eller behörighetshantering.
  Tillämpningsanvisningarna beslutas var och en för sig av kommunstyrelsen eller av den kommunstyrelsen delegerat rätten att fatta beslut om dessa till.
- Metodstöd, handböcker, mallar och utbildningsmaterial och liknande som ger stöd för olika analyser och aktiviteter som ska utföras i nämnder och styrelser.

Ansvar

Det absolut viktigaste ansvaret för informationssäkerheten har vi, alla medarbetare och chefer på trafikkontoret. Vi är alla ansvariga för att skydda personuppgifter och annan icke offentlig information som vi hanterar. Det är viktigt att:

- Påpeka eller flagga till överordnad när brister eller incidenter identifieras.
- Delta i information och utbildningar rörande informationssäkerhet.
- Följa de instruktioner och regler som rör hantering och skydd av personuppgifter och annan icke offentlig information.

Trafikkontoret följer stadsledningskontorets ”Instruktion för ansvar och roller”.
Ansvaret för att skydda informationen i staden är decentraliserat och följer linjeansvaret. Det innebär för trafikkontoret att förvaltningschefen har ansvar för att styra det operativa och lokala arbetet med informationssäkerhet där chefer med verksamhetsansvar ingår.

Identifiering av informationssäkerhetsrisker

Den övergripande metodiken för identifiering, bedömning och hantering av informationssäkerhetsrisker för staden är etablerad av stadsledningskontoret
Klassningsprocessen på Trafikkontoret startar med en kartläggning och avgränsning av informationsbehandlingen. Detta för att kunna definiera tydligt vad som klassas och inte. Exempelvis kan gränserna utgöras av information in i ett system och information ut ur ett system. Ett annat exempel kan vara från det att behandlingen ansvarar för skyddet till att ansvaret lämnas över eller tillbaka. Registerförteckningen, där personuppgifter och dess behandling kartläggs och förtecknas, ger en bra utgångspunkt för informationsklassningen

KLASSA
Det verktyg som staden valt för grundläggande identifiering och bedömning av informationssäkerhetsrisker heter KLASSA. Verktyget är framtaget av Sveriges kommuner och regioner (SKR) och bygger på den internationella informationssäkerhets standarden SS-ISO/IEC 27001/2. Utöver detta så hanterar verktyget frågeställningar och krav från dataskyddsförordningen (GDPR) samt offentlighets- och sekretesslagen (OSL).

Risk och sårbarhetsanalys (RSA)
Verktyget KLASSA har statiska frågor och tar inte hänsyn till alla olika situationer och lösningar som en given hantering av information har. För att fånga de skiftande situationer och lösningar genomför man en RSA.

Handlingsplan
Resultatet av KLASSA tillsammans med resultatet av RSA:n, utgör sedan ett underlag för funna informationssäkerhetsbrister. Utifrån dessa tas en handlingsplan fram, som sedan utgör en checklista för att hantera funna brister.

Trafikkontorets informationssäkerhetsläge
Nedan kontrollpunkter ingår i den systematiska mätning och uppföljning av informationssäkerhetsläget. Dessa redovisas per informationsbehandling och grupperas per förvaltningsobjekt och system/behandling.

- Datum för senast genomförda KLASSA
- Datum för senast genomförda RSA
- Datum för senast genomförda behörighetskontroll
- Registerförd enligt GDPR, registerförteckningen
- Genomförd konsekvensbedömning enligt GDPR
- Informationsklassningsprotokoll finns
- System skiss/beskrivning finns
- Ansvarsroller namnsatta enligt pm3
- Antal ohanterade punkter, ”uppfyller delvis” (gula), i handlingsplanen
- Antal ohanterade punkter, ”uppfyller inte alls” (röda), i handlingsplanen

3. Planering av informationssäkerhetsarbete kommande tre åren

Generella prioriteringsområden

Utifrån kraven från kommunfullmäktige genom stadsledningskontoret (SLK) har trafikkontoret följande aktuella utmaningar i närtid.

Genomförande av informationssäkerhetsklassningar för alla informationsbehandlingar. Prioritet är satt till att först säkra IT-system som är unika för trafikkontoret. Därefter stadens gemensamma system utifrån trafikkontorets nyttjande och sist övriga informationsbehandlingar.

Utifrån kraven från SLK har en lokal anvisning för informationssäkerhet utformats. En i stort sett färdig riktlinje för informationssäkerhet på trafikkontoret har tagits fram. Dock skrevs denna innan kravet från SLK och dokumentet behöver verifieras mot den mall som SLK tagit fram.

Skapa en summerad bild av inträffade säkerhetsincidenter på årsbasis. Denna summerade och analyserade bild ska sedan presenteras för ledningen en gång per år.

Säkra att informationssäkerhetsklassningar genomförs i alla upphandlingar som hanterar information.

Fortsätta arbetet med att verka för att de IT-system som är unika för trafikkontoret placeras i den nätverkssäkerhetszon, som speglar konfidentialitetsvärdet, satt i tillhörande informationsklassning.

Prioriteringar 2024

Den lokala anvisningen ”Trafikkontorets riktlinje för informationssäkerhetsarbete” som tagits fram ska fastställas av förvaltningschefen. Förvaltningen ska under 2024 följa upp att den lokala anvisningen följs, främst med fokus på att;
Chefer**,** årligen ser till att samtliga medarbetare och konsulter genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd följer upp och utreder de incidenter som verksamheten anmäler i IA.
Objektledare**,** tillser att informationstillgångar är klassade och att handlingsplaner från klassning tas om hand för systemet.

Övriga prioriterade områden under 2024;

- Att fortsätta inventera och dokumentera vilka informationsklassningar som är genomförda och fortsatt arbetet med registerförteckning.
- Genomförande av informationsklassningar utifrån framtagen prioriteringslista.
- Fortsätta utveckla rutiner för att tydliggöra informationssäkerhet i inköpsprocessen
- Säkerställ att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbete som pågår inom verksamheten, särskilt för nya digitala tjänster som erbjuds.
- Kompetenshöjande satsningar inom området informationssäkerhet för ledningsgruppen och andra nyckelroller.

Prioriteringar 2025

- Vidareutveckla och effektivisera den rutin som finns för regelbundna informationsklassningar
- Ta fram 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 att kontinuitetsplaner finns.

Prioriteringar 2026

- Revidering av den lokala anvisningen ”Trafikkontorets riktlinje för informationssäkerhetsarbete”
- Granska hur väl lokal rutin för regelbundna informationsklassningar följs.
- Öva utifrån kontinuitetsplaner.