Stockholms stad

Bilaga 6
Dnr T2025-03764

Informationssäkerhet

- Ledningens genomgång år 2025

Trafikkontoret

Ledningens genomgång är en årlig, strukturerad översyn där ledningen bedömer hur ett visst arbete eller system fungerar, identifierar förbättringsbehov och säkerställer att verksamheten följer uppsatta mål och krav. Den utgör beslutsunderlag för prioriteringar och utveckling inför kommande år.

Bilaga till Trafikkontorets Verksamhetsplan 2026
Kontaktperson: Rolf Pettersson, 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/bolagschef inhämta en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten ska 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 att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

Enligt stadsledningskontorets (SLK) anvisningar för förvaltningars arbete med verksamhetsplan 2026 gäller följande för ”Informationssäkerhet – ledningens genomgång”:

Samtliga nämnder ska ta fram en Ledningens genomgång med planering för informationssäkerhetsarbetet under det kommande året som biläggs verksamhetsplanen.
Planeringen ska utgå från nämndens verksamhetsuppdrag i budget och följa *Riktlinje för informationssäkerhet i Stockholms stad*.

Innehållsförteckning

1 Inledning

Denna del sätter ramarna för ledningens genomgång. Syftet med kapitlet är att ledningen ska förstå syftet med genomgången och kopplingen till stadens övergripande informationssäkerhetsarbete.

Stockholm stads arbete med informationssäkerhet utgår från ISO/IEC 27001, som ger ett ramverk för hur ett ***ledningssystem för informationssäkerhet*** (LIS) ska införas och följas upp. Stadens övergripande styrning beskrivs i ***Riktlinje för informationssäkerhet***, som är bilaga till ***Kvalitetsprogrammet***.

Till riktlinjen finns även fastställda tillämpningsanvisningar som tydliggör roller, ansvar och krav på ett systematiskt informationssäkerhetsarbete. Varje förvaltning ska dessutom ha en lokal anvisning som beskriver hur det övergripande ledningssystemet omsätts i den egna verksamheten.

En central del i styrmodellen är **ledningens genomgång** – en årlig och strukturerad genomlysning av informationssäkerhetsarbetet. Syftet är att förvaltningschef eller bolagschef ska försäkra sig om att arbetet bedrivs ändamålsenligt, följer stadens riktlinjer och ger avsedd effekt.

Underlaget tas fram av informationssäkerhetssamordnaren och ska bland annat redogöra för utvecklingen av lokala rutiner för incidenthantering, utbildningsinsatser, genomförda informationsklassningar och status för registerförteckningar.

Ledningens genomgång ska ge ett samlat beslutsunderlag inför kommande år, inklusive vilka förbättringar som behöver genomföras. Från och med arbetet med verksamhetsplan 2026 ska varje nämnd bifoga både rapporten och en planering för kommande års informationssäkerhetsarbete. Denna planering ska utgå från nämndens uppdrag i budgeten och helt följa stadens riktlinje för informationssäkerhet.

2 Förändringar i interna och externa förutsättningar

Syftet med kapitlet är att ledningen ska få en uppdaterad bild av förändringar som påverkar informationssäkerheten, t.ex. nya lagkrav, hotbilder, organisatoriska förändringar eller teknisk utveckling.

2.1 Interna förutsättningar

Förändringar i organisationens processer och förvaltningsmodell

Översyn av trafikkontorets förvaltningsmodell ”Vintergatan” har under året initierats. Förvaltningsmodellen är till stor del varit baserad på pm3. Det finns ett fortsatt behov av att stärka samverkan mellan objekten och linjeverksamheten och resurser har tillförts organisationen.

Dataskydd

I staden så är det operativa arbetet för dataskydd och informationssäkerhet integrerat. Detta angreppsätt förenklar väsentligt då de olika lagkraven, såsom GDPR och kommande cyberssäkerhetslag, ställer likartade krav på säkerhetsåtgärder.

Trafikkontorets registerförteckning nyttjas idag inte till sin potential och inte på det sätt som stadens riktlinje för informationssäkerhet föreskriver. En huvudanledning till detta är att registerförteckningens indelning ”processer” inte är mappade med verksamhetens processer.

Behovet av att nyttja kontorets registerförteckning i informationssäkerhetsarbetet ökar. Det är särskilt viktigt att IoT och AI registerförtecknas utifrån personuppgiftsbehandlingen, då dessa verktyg behöver konsekvensbedömmas avseende dataskydd enligt GDPR artikel 35 (Internet of Things - innebär att kommunens fysiska objekt – som gatubelysning, sensorer i fastigheter eller trygghetslarm – kopplas upp för att automatisera drift och ge realtidsdata för bättre service).

Ett samarbete har under 2025 skett med Trafikverket inom ramen för Trafik Stockholm och ingående parter har tagit fram ett avtal för gemensamt personuppgiftsansvar.

Kameraprojekt
Under 2025 har en inventering av kameror/sensorer genomförts och att kontoret har tagit fram övergripande process för kamerabevakning - från behov av kamera, intresseavvägning enligt GDPR, beslut, informationsklassning och fler steg fram till drift och underhåll. Eftersom antalet kameror är mycket stort så enades ”Kameranätverket” att en gruppering bör göras i några få huvudgrupper av kameror. Därmed kan förenkling ske genom att enbart respektive huvudgrupp informationsklassas för att specificera relevanta säkerhetsåtgärder.

AI
AI är fortsatt ett omoget område, juridisk, tekniskt och affärsmässigt men utvecklingen går snabbt och vi behöver hänga med, testa och lära oss.

Trafikkontoret är ansvarig för sin informationsbehandling, oavsett om det sker med traditionell IT eller med hjälp av AI. Informationssäkerhetsaspekterna behöver därmed beaktas och flera initiativ har tagits för att bredda kompetens och förståelse kring AI. Trafikkontoret har utsett en samordnare av AI-frågor. Från ett informationssäkerhetsperspektiv är det av vikt att en policy för allmänt tillgänglig generativ AI tas fram och beslutas för trafikkontoret, dels för att ge vägledning avseende beaktande som bör göras utifrån ett säkerhetsperspektiv men även för att fler medarbetare ska våga och vilja testa AI-tekniker. Notera att andra områden inom AI kommer att ge nytta för trafikkontoret, dock är allmänt tillgänglig generativ AI det område som i närtid lär beröra flest medarbetare vid kontoret.

Myndigheten för digital förvaltning (Digg) och Integritetsskydds-myndigheten (IMY) har tillsammans tagit fram riktlinjer (not, eg tips och idéer) för hur offentlig förvaltning bör använda generativ AI, se riktlinje för generativ AI. Här adresseras en bredd av områden, exempelvis följande:

- Inför en AI-policy, förbered verksamheten inför AI-förordningen, GDPR, informationssäkerhet, etc.

Informationssäkerhetskrav vid upphandling
Informationsklassning och tillhörande riskanalyser nyttjas av staden för att kravställa och verifiera informationssäkerhetskrav vid upphandling av IT-tjänst. Metodik för detta har etablerats under året och är nu ett rekommenderat arbetssätt i staden. Kravställan görs relativt enkelt med hjälp av SKR:s verktyg KLASSA vid en så kallad A-klassning och verifiering sker med hjälp av upphandlad leverantör/-ers deltagande vid informationsklassning typ B. Från och med december 2025 så adresserar verktyget KLASSA även säkerhetskraven enligt kommande cybersäkerhetslag.

2.2 Externa förutsättningar

Nya lagar och regulatoriska krav

- **Cybersäkerhetslagen (genomförandet av NIS 2 i svensk lag):** Under 2025 har lagstiftningsarbetet fortsatt med lagrådsremiss och proposition, men ingen ny lag har ännu beslutats. Fokus har legat på att förtydliga kravbilden för samhällsviktiga aktörer inför kommande implementering. Den nya lagen är föreslagen att träda i kraft 15 januari 2026 och ersätter NIS 1 i svensk lag. Till skillnad från lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS1) så träffar Cybersäkerhetslagen hela trafikkontoret och ställer väsentligt högre säkerhetskrav på verksamheten.
- **CER (Critical Entities Resilience – har ännu inget namnförslag till lag av Regeringen):** Här har processen avstannat sedan utredarens rapport. Inga nya förslag har framkommit under året på hur regleringen kan genomföras i svensk lag. Den kommande lagen är planerad att träda i kraft vid halvårsskiftet 2026. Kritiska aktörer som träffas av CER kommer också att bli subjekt under Cybersäkerhetslagen. För Trafikkontoret är det fortfarande något oklart vad det innebär. Kraven på säkerhetsåtgärder för informationssäkerhet förväntas huvudsakligen bli desamma, kraven på riskhantering och kontinuitet kan dock komma att utvidgas något.

Hotbild – sammanvägd bild från ansvariga cybersäkerhetsmyndigheter
Här följer en sammanvägd bild från ansvariga cybersäkerhetsmyndigheter från deras publicerade årsrapporter från 2024 och 2025. Myndigheterna är ENISA (Den Europeiska Cybersäkerhetsbyrån), MSB, Säpo, MUST och FMV. Hoten och rekommendationerna är analyserade utifrån en generisk svensk

kommun och inte anpassade till Stockholm Stad eller Trafikkontoret.

Förändringar i hotbilden under 2025
Hotbilden för svenska kommuner under 2025 präglas av en tydlig förskjutning från enskilda IT-incidenter till ett mer sammansatt säkerhetsläge där cyber-, fysisk påverkan, kriminalitet och desinformation vävs samman.

Statliga aktörer fortsätter kartlägga och testa kommunala system, medan organiserad brottslighet blivit mer tekniskt avancerad och riktar sig mot både data och välfärdstjänster. Leverantörsberoenden och molntjänster skapar nya angreppsvägar som ofta ligger utanför kommunens direkta kontroll. Informationspåverkan riktad mot skola, socialtjänst och migration driver polarisering och kan snabbt övergå i hot mot personal.

Driftstörningar i el, tele och nätverk framstår som kritiska då de omedelbart påverkar trygghetslarm, hemtjänst och skolor. Samtidigt ökar insiderhotet genom felaktiga behörigheter och infiltration i entreprenörsled. Hybridattacker mot VA-verk och fastighetssystem pekar mot ett skarpare samhällshot.

Sammantaget har hotbilden under 2025 blivit bredare, snabbare och mer systemisk — och kräver att kommuner arbetar integrerat med cyber, säkerhetsskydd och kontinuitet som en sammanhållen helhet.

Externa krav på åtgärder för att möta hoten (enligt samma myndigheter som ovan)
Kommunerna behöver under 2025 förstärka sin motståndskraft genom att kombinera tekniska, organisatoriska och sociala skydd. Grundsäkerhet måste säkras genom härdning, MFA (Multi Factor Authentication), segmentering och kontinuerlig patchning, samtidigt som identitets- och behörighetsstyrning blir en kommunövergripande kärnprocess.

Leverantörskedjor och molntjänster kräver skärpta avtal, tydliga kontinuitetskrav och regelbundna kontroller. Kommuner behöver också förbereda sig för längre störningar i el, tele och nätverk och därmed stärka reservrutiner och manuella arbetssätt. Insiderhot och organiserad brottslighet måste mötas med systematisk loggning, säkerhetsprövning och tät samverkan med polis och region.

Informationspåverkan mot exempelvis skola och socialtjänst kräver snabb kommunikation, lokala lägesbilder och förmåga att korrigera falska narrativ.

Slutligen behöver kommunerna integrera cyber, krisberedskap och säkerhetsskydd i ett sammanhållet arbetssätt där ledningen tar ett aktivt ansvar och där övning, lärande och robusthet återkommer som en naturlig del av styrningen.

Vid MSBs cybersäkerhetskonferens 2025 gav företrädare från regeringen följande budskap:

- *Vänta inte med att adressera lågt hängande frukter*, dvs inför omgående (närmaste månader/närmaste halvår) enkla åtgärder som bidrar till ökad motståndskraft*
  *lågt hängande frukter = exempelvis att dokumentera behörigheter, att skydda VPN-accesser med tvåfaktorsautentisering

Hotbild – trafikkontoret

Ovan beskriven hotbild, generell och för svenska kommuner, bedöms till stora delar även gälla för trafikkontoret.

Transportsektorn är den sektorn som senare år drabbats mest av cybersäkerhetsattacker (ENISAs rapport *Threat Landscape 2024).* Trafikverkets rapport 2024, *Öppen antagonistisk hotbild mot transportsektorn,* understryker ett allvarligt läge där statsaktörer pekas ut (Ryssland, Kina och Iran). I rapporten anges t ex följande: ”*Olika typer av inhämtnings- och påverkansoperationer pågår här och nu. De syftar till att kunna påverka svenskt beslutsfattande och begränsa Sveriges politiska handlingsutrymme. Exempelvis kan ett cyberintrång användas för att hämta ut specifik information, eller för att skapa en möjlighet att i ett senare skede störa ett viktigt svenskt tekniskt system. En lyckad sådan åtgärd innebär ett allvarligt och konkret hot mot Försvarsmakten och mot Sverige som helhet. Skyddet av kritisk infrastruktur, såväl fysisk som digital, är därför av stor betydelse*”.

Inom arbetet med trafikkontorets ledningssystem för informationssäkerhet så kommer kontoret att behöva besluta om en relevant hotbild inför det återkommande riskanalysarbetet årligen.

3 Kontorets informationssäkerhetsstatus

En översikt över hur Trafikkontoret presterar inom informationssäkerhet. Syftet är att ledningen ska kunna bedöma om åtgärder fungerar och om LIS är effektivt.

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. Integritetsrisker behöver hanteras i enligt med dataskyddslagstiftningen.

3.1 Status för genomförda åtgärder och kontroller

Informationsklassning och kompletterande riskanalys

Trafikkontoret nyttjar ett stort antal applikationer vilka tillhör objekt i Vintergatan och av dessa förvaltas en del av dem huvudsakligen av SLK (eller St:Erik försäkring/Stadsarkivet). Informationsklassning av applikationerna pågår.

Behov av den kompletterade riskanalysen, enligt stadens handbok för informationsklassning, har identifierats vid de informationsklassningar som genomförts under 2025 och när det har bedömts att riskanalyser är nödvändig har dessa genomförts.

Det finns ett stort behov av effektivare arbetssätt vid informationsklassning då dessa under tidigare år varit mycket resurskrävande. Under 2025 har en effektivisering skett inklusive kvalitetshöjande åtgärder och ytterligare effektivisering med hjälp av förbättrade verktyg är planerad att implementeras vid årsskiftet 2025/ 2026. Idag genomförs informationsklassningar med förstärkt fokus på det värdeskapande och utpekad åtgärdsansvarig roll är involverad i formulering av säkerhetsåtgärd.

Projektet Cybertrygg

Projektet Cybertrygg ska öka säkerheten för trafikkontorets samtliga IT-system i enlighet med NIS lagen (lagen om

informationssäkerhet för samhällsviktiga och digitala tjänster 2018:1174), samt stötta kontorets efterlevnad till kommande lagstiftning NIS2 (benämnd cybersäkerhetslagen). Projektet ska bidra förebyggande kring tekniska och administrativa säkerhetsåtgärder för att minska sårbarheten och öka förmågan att hantera cyberangrepp. Se projektets projektdirektiv för mer detaljerade effektmål och projektmål.

Projektet som är indelat i två block (A och B) beräknas pågå till slutet av 2028. Nedan beskrivs genomförda och pågående aktiviteter, samt övergripande plan för 2026:

- **Block A** arbetar med cyberfysiska system och IT-infrastruktur som används för övervakning och styrning av stadens trafikanläggningar. Under hösten 2025 har projektet arbetat förberedande inför upphandling av ny hård- och mjukvara, samt utlokalisering av driftsåtagande. Just nu inväntas upphandlingsbeslut via trafiknämnden för att komma vidare. När väl upphandlingar är genomförda kommer samtliga IT-infrastruktur att ersättas och byggas enligt ny säkerhetsmodell och alla system flyttas över från befintlig till ny IT-infrastruktur.
- **Block B** har två spår:
    - **B1** hanterar åtgärdsplan kopplad till Transportstyrelsen tillsynsärende (Tjänsteutlåtande Dnr T2024-00412), där redovisning för trafiknämnden sker årligen. Arbetet innebär att släcka de brister som Transportstyrelsen identifierat, vilket ger en bättre grund för ökad säkerhet. Bland annat kommer kontoret under 2026 att börja använda stadens centrala funktion för omvärldsbevakning, CERT Stockholm. Där kommer kontorets informations-tillgångar att löpande mappas mot nyupptäckta sårbarheter, t.ex. säkerhetsluckor i operativsystem, så att säkerhetsuppdateringar kan installeras skyndsamt.
    - **B2** ska bidra med initiativ som stöder kontorets utveckling så att hela kontoret, inklusive alla system, når efterlevnad till den nya cybersäkerhetslagen (NIS2). Cybertrygg, trafikkontorets överordnade systematiska informationssäkerhetsarbete och Vintergatan behöver vara synkroniserade, vilket innebär att alla initiativ och aktiviteter behöver planeras gemensamt. Detta för att säkerställa att övergången till den nya cybersäkerhetslagen sker på ett målinriktat och effektivt sätt där implementeringen med ändrade arbetssätt sker på hela trafikkontoret.

I skrivande stund så är inriktningen att projekt cybertrygg ska kunna stödja framtagande av mer generella arbetssätt som möter NIS2 när det gäller exempelvis verksamhetsövergripande riskanalys med allriskperspektiv, incidenthantering och kontinuitetshantering

Inga andra kontroller har genomförts under 2025.

3.2 Resultat från interna och externa revisioner

Resultatet från uppföljning via VoR och intern kontrollplan
Trafikkontoret hade inför år 2025 i väsentlighets- och riskanalys, VoR, identifierat risker kopplade till nedan delprocesser:

- Fastställa krav genom informationsklassning
- Fastställa lokal anvisning för informationssäkerhet
- Informationssäkerhet i upphandlingsförfarande
- Kontinuitetsplanering IT-system
- Lokal rutin behörighetshantering
- Rutin för incidenthantering

De risker med tillhörande åtgärder som pekats ut via VoR har fokus på ett etablerat och systematiskt sätt att arbeta i respektive delprocess. Vid uppföljning så kan det konstateras att det är enbart i delprocess ”Informationssäkerhet i upphandlingsförfarande” som en tydlig progress skett. En huvudorsak till bristande progress avseende övriga delprocesser ovan är att processerna med att åtgärda riskerna har inte skett samordnat inom kontoret och därmed har andra aktiviteter prioriterats.

Inga externa revisioner har genomförts under 2025

3.3 Mätningar och KPI:er för informationssäkerhet

Inga mätningar har genomförts under 2025. Trafikkontoret överväger deltagande i MSB:s cybersäkerhetskoll och i nuläget prioriteras det egna arbetet men möjligheten kvarstår.

4 Risker och incidenter

Syftet är att ledningen ska få en tydlig bild av aktuella risker och inträffade incidenter, samt vilka lärdomar som dragits. Detta ger underlag för prioritering av resurser och åtgärder.

4.1 Det systematiska arbetet

Det systematiska arbetet på kontoret kan förbättras och Transportstyrelsens tillsyn av NIS1 renderade i sanktioner samt i ett antal åtgärder som fått stort fokus under året.

Under hösten 2025 har alltfler tagit del av relevanta utbildningar och seminarier kring den kommande cybersäkerhetslagen, vilket bidragit till en alltmer gemensam syn. Under 2026 kommer utbildningsinsatserna att fortsätta.

En viktig aktivitet som har utförs i det systematiska informationssäkerhetsarbetet har varit att upprätta en lista avseende kontorets applikationer, objekttillhörighet och status avseende informationsklassning, riskanalys m.m. Här är en systematik etablerad vilket ger en överblick som kan bibehållas över tid med små medel samt ger en bas för uppföljning.

4.2 Identifierade risker och deras status

För kommande år är ambitionen att komplettera kontorets risk- och sårbarhetsanalys, RSA med det systematiska informationssäkerhetsarbetet.

4.3 Risker i stadens outsourcade IT-leveranser (GSIT & STA - avtalen)

ISIL (Stadens interna forum för styrning av informationssäkerhetsrisker i leveranskedjan för stadens grundläggande IT-leverans) har analyserat sårbarheter och hot som är avstämt med stadens outsourcingleverantörer (för GSIT och STA), säkerhetsavdelningen vid SLK och stadens IT-direktör. Kommunicerat till ISAM samt kommuniceras till IT-chefer vid respektive förvaltning och bolag.

Tre huvudrisker är definierade:

- Ransomware (R1)
- Interna hot (R2)
- Överbelastningsattacker (R3)

Konsekvens	4. Allvarlig		*R1*		*R2*
	3. Betydande				
	2. Måttlig				*R3*
	1. Försumbar				
Sannolikhet		1. Låg/ Osannolik	2. Medel-hög/Möjlig	3. Hög/ Sannolik	4. Mycket hög

Ovan matris visar hur dessa risker bedömts, R1-R3. En bedömning som delas av både SLK och av stadens outsourcingleverantörer (för GSIT och STA). Riskerna är omfattande/höga och kräver relativt omfattande åtgärder för att nå acceptabla risknivåer. Åtgärder finns specificerade på övergripande nivå, varav flertalet behöver implementeras lokalt vid respektive förvaltning och bolag (t ex genom deltagande i SLKs projekt *Långsikt* som berör alla förvaltningar och bolag)

4.4 Rapport om inträffade incidenter och konsekvenser

Den incident som fått fokus under året är incidenten vid Miljödata, en incident som drabbade flertalet kommuner och där personuppgifter för ett stort antal personer läckt ut och även lagts ut på darknet. Trafikkontorets informationssäkerhetssamordnare och dataskyddsombud har följt incidenten och delgetts detaljer kring det inträffade. Trafikkontorets dataskyddsombud har varit mycket engagerad i ärendet då läckan inkluderade personuppgifter för medarbetare vid trafikkontoret.

Trafikkontorets dataskyddsombud har även delgetts ett mindre antal personuppgiftsincidenter av ringa allvarlighetsgrad

Staden och trafikkontoret saknar effektiva verktyg, processer och kultur för incidentrapportering och på trafikkontoret kan rutinerna för när och hur rapportering ska ske förbättras. Inga rapporter avseende incidenter har nått kontorets informationssäkerhetssamordnare.

4.5 Lärdomar och förbättringsåtgärder efter incidenter

Vid incidenter ska även tidsram beaktas och anmälningsskyldighet till respektive tillsynsmyndighet. Trafikkontoret har en beslutad lokal rutin för hantering av incidenter, den behöver dock förankras och övas. I objekten går det även att förtydliga vem som kan ta rollen som incidentledare.

Dagens lagstiftning, inklusive kommande cybersäkerhetslag, kräver att incidenter ska kunna upptäckas, identifieras, hanteras och förebyggas. Vid incidenter ska även tidsram beaktas och anmälningsskyldighet till respektive tillsynsmyndighet. Anmälningsplikt inom 24 timmar (och då ska en del förarbete genomförts) ställer stora krav på bemanning, beredskap och att rutinen är övad.

Den lokal rutinen för hantering av incidenter innehåller bilaga personuppgiftsincidenter som kan nyttjas fristående från den övergripande incidenthanteringsrutinen eller som del av rutinen (personuppgiftsincidenter är här en delmängd och ingår i begreppet incidenter).

Notera att även bilaga personuppgiftsincidentsrutin kan ha behov av att skärpas, förtydligas och förankras i verksamheten. Att de som förväntas vara incidentledare eller leda utredningen av personuppgiftsincidenter utses i förväg och uppdateras om sitt ansvar och vad de förväntas göra vid en personuppgiftsincident. Det gäller i objekten, i linjen och i projekten.

5 Efterlevnad av kommunens riktlinjer

Syftet är att ledningen ska få en bedömning av hur väl kontoret följer stadens policy och styrdokument. Detta så att ledningen ska kunna agera vid avvikelser.

Ledningssystemet för informationssäkerhet är stadens strukturerade ramverk för att säkerställa att information hanteras säkert och i enlighet med lagar och interna krav. Det omfattar styrning, roller och processer för riskhantering, kontinuitet och incidenthantering, och ger kontoret verktyg för att skydda informationens konfidentialitet, riktighet och tillgänglighet.

Stockholms stads informationssäkerhetsarbete regleras i en riktlinje för informationssäkerhet som är en bilaga till stadens Kvalitetsprogram. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.
Respektive förvaltning ska ha en lokal anvisning, fastställd av

förvaltningschef, som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas vid trafikkontoret. Det innebär att definiera ansvar och roller, genomföra riskanalyser och klassning av information samt införa rutiner för incidenthantering och kontinuitet.
Arbetet ska dokumenteras, följas upp och integreras i ordinarie styrning för att säkerställa efterlevnad och förbättring.

Inom trafikkontoret så finns det en lokal anvisning som bygger på stadens riktlinjer och tillämpningsanvisningar som beslutades av förvaltningsdirektören 2025-04-25.

5.1 Identifierade avvikelser och orsaker

Se avsnitt *4.1 Det systematiska arbetet*.

5.2 Planerade eller pågående korrigerande åtgärder

Trafikkontorets lokala anvisning för informationssäkerhet har uppdaterats under 2025, men kommer att revideras ytterligare under 2026 för att säkerställa att den är synkroniserad med förvaltningsmodellen Vintergatan. Stor vikt behöver därefter läggas på förankring och kommunikation av den lokala anvisningen för samtliga anställda på trafikkontoret.

6 Återkoppling från intressenter

Syftet är att ledningen ska förstå hur LIS upplevs av verksamheten och externa parter. Detta ger insikt i behov av stöd eller förändringar.

6.1 Synpunkter från interna verksamheter

Arbetet med att stärka systematiken inom informationssäkerhet pågår och därför finns ännu inga dokumenterade synpunkter i organisationen.

6.2 Feedback från externa parter eller leverantörer

Erfarenheter från MSB:s cybersäkerhetskonferens och AI-seminarier har tagits tillvara.
Ingen annan feedback har dokumenterats.

6.3 Sammanställning av behov och förväntningar

Inga behov eller förväntningar från externa parter har dokumenterats.

7 Resurser och kompetens

Syftet är att ledningen ska få en bedömning av om resurser och kompetens är tillräckliga för att nå målen. Detta så att ledningen ska kunna besluta om förstärkningar.

7.1 Kompetensnivå och utbildningsbehov

Det finns en grundläggande kunskap på kontoret avseende informationssäkerhet inklusive dataskydd, på övergripande nivå. Objekten behöver dock ha en något djupare och mer sammanhållen kompetens.
Utbildningsinsatser inför cybersäkerhetslagen och kring AI har genomförts sporadiskt.

7.2 Behov av stöd från centrala funktioner eller externa aktörer

Behov av externt stöd finns för nedan områden/mål, se kapitel 9:

- Effektivisera informationsklassningsarbetet med hjälp av anpassade kravmallar och förifyllda svar anpassade till dels outsourcad it (STA-avtalet), cyberfysiska system samt avseende molntjänster
- Etablera ett kartotek med kontorets ”*best practice*” avseende tekniska och organisatoriska säkerhetsåtgärder (dvs konkreta rutiner, instruktioner mm avseende respektive säkerhetsområde såsom loggning, behörighetshantering, säkerhetskopiering etc)
- Behörighetshantering dokumenterat för respektive system (teknik, process, rutin)
- Bredda kontorets kunskap angående informationssäkerhet med fokus på nya cybersäkerhetslagens föreskrifter (utbildningsinsatser)
- Genomföra fler informationsklassningar med tillhörande riskanalys
- Genomföra fler sårbarhetsgranskningar av IT-system
- Genomföra riktade revisioner avseende de IT-system som klassats ge allvarliga konsekvenser vid bortfall, tex angående säkerhetskopiering och förmåga för återställande
- Genomföra block A i projekt Cybertrygg avseende cyberfysiska system och IT-infrastruktur som används för övervakning och styrning av stadens trafikanläggningar.

Befintliga avropsavtal finns att nyttja för att försörja ovan externa behov.

8 Förbättringsområden

Omfattar identifierade områden där informationssäkerheten kan stärkas. Syftet är att ledningen får underlag för strategiska beslut.

8.1 Identifierade svagheter i processer eller teknik

Det finns goda möjligheter att ytterligare stärka och effektivisera arbetssätten för informationsklassning då de tidigare har varit resursintensiva. Det finns även potential att utveckla hanteringen av resultaten från informationsklassningarna, såsom handlingsplaner och säkerhetsåtgärder för att underlätta ett mer samlat genomförande. Genom att tydliggöra roller och ansvar skapas förutsättningar för att säkerhetsåtgärderna ska kunna implementeras mer konsekvent och bidra till att informationsklassning och riskanalyser upplevs som ännu mer värdeskapande i organisationen.

8.2 Förslag på förbättringsåtgärder

Effektivisering och kvalitetshöjande åtgärder kring informationsklassningar har införts. Fler steg är adresserade för att nå ytterligare effektivisering och högre kvalitet, steg som har initierats både vid trafikkontoret och även centralt i staden.

8.3 Möjligheter till innovation och effektivisering

Från och med december 2025, i samband med release av KLASSA version 5, erbjuder KLASSA-verktyget stöd för verksamhetsanpassade kravlistor och trafikkontoret planerar att ta fram specifika kravkataloger med förifyllda svar – dels för outsourcad it utgående från systemtjänsteavtalet, dels för cyberfysiska system och för molntjänster, något som bedöms underlätta för klassningarna markant samt öka kvalitén och nyttan.

Centralt i staden, vid SLK, så sker en översyn av verktygstöd för informationsklassning. Ambitionen är att från och med 2027 närmare kunna knyta samman verksamhetsövergripande riskbild,

RSA, VoR, krav på säkerhetsåtgärder och uppföljning av dessa krav. Ovan arbete med specifika kravkataloger bedöms kunna återanvändas och bidra i utvecklingen.

9 Fastställande av mål

Syftet är att ledningen ska säkerställa att avdelningens mål är i linje med stadens övergripande mål och att de är realistiska och mätbara.

9.1 Anpassning av mål till kommunens strategi

Kontoret prioriterar och adresserar åtgärder utifrån ledningens genomgång (del av ledningssystemet för informationssäkerhet, krav enligt stadens riktlinje).

Prioriterade områden:

- Roller och ansvar kring informationssäkerhet är tydliggjorda och förankrade i verksamheten.
- Kontorets rutin för incidenthantering är förankrad och övad (vilket inkluderar att incidentledare finns tillgänglig vid en incident).
- Behörighetshantering dokumenterad för respektive system (teknik, process, rutin).

9.2 Prioriterade mål för kommande period

Mål för informationssäkerhetsarbetet vid Trafikkontoret för 2026 föreslås till följande:

- Effektivisera informationsklassningsarbetet med hjälp av anpassade kravmallar och förifyllda svar anpassade till dels outsourcad it (STA-avtalet), cyberfysiska system samt avseende molntjänster
- Etablera ett kartotek med kontorets ”*best practice*” avseende tekniska och organisatoriska säkerhetsåtgärder (dvs konkreta rutiner, instruktioner mm avseende respektive säkerhetsområde såsom loggning, behörighetshantering, säkerhetskopiering etc.)
- Bredda kontorets kunskap angående informationssäkerhet med fokus på nya cybersäkerhetslagens föreskrifter
- Fastställande av kontorets förvaltningsmodell Vintergatan samt säkerställa att den lokala anvisningen för informationssäkerhet utgår från samma roller och ansvar som fastställts i kontorets förvaltningsmodell
- Ökad integration i informationssäkerhetsarbetet, RSA och VoR
- Genomföra en för kontoret verksamhetsövergripande riskanalys

- Genomföra Block A i projekt Cybertrygg avseende cyberfysiska system och IT-infrastruktur som används för övervakning och styrning av stadens trafikanläggningar.

10 Beslut och uppföljning

Syftet är att ledningen ska besluta en tydlig plan för vilka beslut som fattats, vem som ansvarar och hur uppföljning ska ske. Detta är avgörande för styrning och ansvar.

10.1 Beslutade åtgärder och ansvariga personer

Förvaltningen ska under 2026 följa upp att stadens riktlinje och tillämpningsanvisning för informationssäkerhet efterlevs.

Vidare att den lokala anvisningen följs, främst med fokus på att;

1. Fortsatt effektivisering, avseende arbetet med säkerhets-åtgärder, primärt med hjälp av informationsklassningar.
2. Revidering och förankring av lokal anvisning
3. Tillse att prioriterade informationstillgångar är klassade och att handlingsplaner tas fram med tekniska och organisatoriska åtgärder och implementeras
4. Genomföra fler sårbarhetsgranskningar av IT-system
5. Genomföra riktade revisioner avseende de IT-system som klassats ge allvarliga konsekvenser vid bortfall, tex angående säkerhetskopiering och förmåga för återställande
6. Kravställa för respektive IT-system inom systemtjänsteavtalet.

10.2 Tidsplan för genomförande och uppföljning

Genomförandet ska följas upp under sena våren och avrapporteras med hjälp av ISAM inför planeringen av 2027.

10.3 Datum och agenda för nästa ledningens genomgång

Nästa ledningens genomgång ska genomföras senast i oktober 2026. Agendan ska vara liknande denna, med kompletteringar från Cybersäkerhetslagen och eventuella förtydliganden i stadens ledningssystem.