Stockholms stad

Verksamhetsplan 2026

Bilaga 1 c
Informationssäkerhet – Ledningens genomgång

Ledningens genomgång år 2025

Exploateringskontoret

Kontaktperson: Johan Furugren

Sammanfattning

Ledningens genomgång är ett begrepp inom tillämpad informationssäkerhet som syftar till att de som ansvarar för informationssäkerheten inom en organisation, minst årligen ska informera sig om hur arbetet går. Krav på att genomföra momentet Ledningens genomgång ställs i Anvisningar för nämndernas arbete med verksamhetsplan 2026 och i Tillämpningsanvisningar till stadens riktlinje för informationssäkerhet, senast revidering per 2024-11-13.

Momentet finns även beskrivet i standarden för informationssäkerhet ISO-27000.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef inhämta en rapport, dvs Ledningens genomgång från informationssäkerhetssamordnaren.

Rapporten ska ge grundinformation, omvärldsanalyser och beslutsunderlag till förvaltningschefens uppgift att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

Ledningens genomgång innebär en redovisande genomlysning av befintliga komponenter av ett ledningssystem för informationssäkerhet och förbättringsförslag med åtgärder att införa eller genomföra i verksamheten. Ledningens genomgång utgör ett styrande dokument som ska biläggas nämndens verksamhetsplan.

Föreslagna och planerade aktiviteter beskrivs i detta dokument. Arbetssättet är krav- och riskbaserat med ett treårigt perspektiv och ska medföra en serie av årliga och återkommande åtgärder.

Arbete med informationssäkerhet inom exploateringskontoret kommer att för perioden 2026 - 2028 främst vara fokuserat på inventeringar, informationsklassningar och registerförteckning. Även aktiviteter som stödprocesser, rutiner, utbildningar och kompetensfördjupningar kommer att ingå.

Innehållsförteckning

1 Faktorer som styr och påverkar verksamheten 5

2 Omvärldsbevakning 7

2.1 Yttre händelser utanför staden – legal påverkan, hot och trender .. 7

2.1.1 Lagstiftning 7

2.1.2 Hot 8

2.1.3 Trender 9

2.2 Yttre händelser inom staden – förutsättningar, förändringar, inriktningar eller resurser 10

3 Risker och incidenter 12

3.1 Vad har verksamheten identifierat i RSA-arbetet 12

3.2 Resultatet från egen uppföljning (VoR och IKP) 12

3.3 Resultatet från revisioner 13

3.4 Risker som identifierats i GDPR-årsrapport 13

3.5 Risker i stadens outsourcade IT-leveranser (GSIT- och STA-avtalen) 13

3.6 Information om avvikelser (incidenter och andra händelser) 14

3.6.1 Personuppgiftsincident vid Miljödata 14

4 Verksamhetens arbete med informationssäkerhet 16

4.1 Arbete och aktiviteter under innevarande period 16

4.2 Planerat och prioriterat arbete samt aktiviteter under kommande perioder 17

4.2.1 Verksamhetsår 2026 17

4.2.2 Verksamhetsår 2027 - 2028 19

1 Faktorer som styr och påverkar verksamheten

Stockholms stads arbete med informationssäkerhet ansluter till en global ISO-standard, ISO/IEC 27001, för informationssäkerhet som systematiserar roller, processer och uppgifter med att skydda organisationers känsliga information från hot och risker. Standarden är ett ramverk, bland annat för hur ett *ledningssystem för informationssäkerhet (LIS)* implementeras för att skydda informationstillgångar och skapa processtöd som underlättar att planera, hantera, mäta och förbättra arbetet.

Stockholms stads informationssäkerhetsarbete regleras i ett antal styrdokument, bland annat i en övergripande *Riktlinje för informationssäkerhet* med en tillhörande bilaga av *Tillämpningsanvisningar*. Båda dokumenten utgör bilagor till stadens *Kvalitetsprogram*. Tillämpningsanvisningarna fastställer krav och reglerar ansvar eller roller kopplat till Stockholms stads övergripande systematiska informationssäkerhetsarbete och strukturerade metodstöd.

Exploateringskontorets framtagna *Lokal anvisning för informationssäkerhet* specificerar hur stadens övergripande krav och tillämpningsanvisningar för informationssäkerhetsarbetet ansluter till förvaltningens aktiviteter.

För att exploateringskontoret ska nå målet att säkerställa en tillfredsställande operativ skyddsnivå för befintliga informationstillgångar måste arbetssätten kring området informationssäkerhet och dataskydd bli mer transparenta och utformas systematiskt, krav- och riskbaserat.

Framtagningen av ett lokalt LIS som stöd för att verksamhetens interna aktiviteter och samlade stöddokument, kontrollrutiner och andra typer av styrmedel för informationshantering fortlöper. Ledningssystemet ska dels utgöra en samlad process och kunskapskälla för planering, genomförande och kontroll/uppföljning och dels för att kunna såväl förebygga, identifiera, analysera och följa upp förekomsten av olika brister eller avvikelser som påverkar informationssäkerheten. En viktig aktivitet som utförs i det systematiska informationssäkerhetsarbetet är att kartlägga befintliga system och infrastrukturella relationer, applikationer, objekttillhörighet och status avseende

informationsklassning, riskanalys, m.m. vilket kan bidra en aktuell överblicksbild och bas för uppföljning.

En central del i styrmodellen är också *Ledningens genomgång*, en årlig och övergripande redovisning av informationssäkerhetsarbetet. Syftet är att förvaltningschef ska försäkra sig om att arbetet bedrivs ändamålsenligt, följer stadens riktlinjer och ger avsedd effekt. Ledningens genomgång ska resultera i ett samlat beslutsunderlag inför kommande år, inklusive vilka förslag till förbättringar som behöver genomföras.

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

2 Omvärldsbevakning

2.1 Yttre händelser utanför staden – legal påverkan, hot och trender

2.1.1 Lagstiftning

Generellt uppstår kontinuerligt fler hotbilder med olika typer av hotmedel och tekniker. Myndigheter tenderar att vara särskilt utsatta för oönskade aktiviteter.

En utökad lagstiftning, t ex en uppdatering av Säkerhetsskydds-förordningen har aktualiserats i slutet av 2021. Likaså har en omfattande rad initiativ och insatser från skyddsopererande myndigheter som MSB och SÄPO genomförts.

NIS2-direktivet (Network and Information Systems Directive 2) syftar till att uppnå och upprätthålla en hög säkerhetsnivå i nätverk och informationssystem, och flera av områden berör offentlig verksamhet som kommuner. NIS2-direktivet beslutades av EU i december 2022 och ersätter det NIS-direktiv som började gälla 2018 genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS). NIS2 medför tydligare krav på riskanalyser och säkerhetsåtgärder.

NIS2-direktivet ska införas fullt ut i svensk lagstiftning genom tillkomsten av en ny cybersäkerhetslag. Regeringen har lagt fram en proposition till riksdagen och beslut väntas i december 2025. Lagen förväntas träda i kraft den 15 januari 2026.

Ett nytt överbryggningsavtal för personuppgiftsbehandlingar mellan amerikanska och europeiska organisationer och aktörer har godkänts av Europeiska dataskyddsmyndigheten (EDPB) och benämns *EU US Data Privacy Framework*, Hur Stockholms stad agerar på detta ramverk analyseras på central nivå.

AI-förordningen eller AI act är det legala ramverk som ska reglera utveckling, användning och tillämpning av artificiell intelligens inom EU. Fokus ligger på de AI-system som klassificeras med högre risk. Syftet är att AI-system i Europa ska vara säkra och respektera mänskliga rättigheter. AI-förordningen gäller för samtliga leverantörer, importörer, distributörer och användare av AI-system som används eller tas i bruk inom EU:s

marknadsområde, oavsett om de är etablerade inom eller utanför EU. Därmed påverkar förordningen aktörer som

- utvecklare och leverantörer av AI-system, inklusive mjukvaruföretag och teknikleverantörer
- importörer och distributörer som inför AI-system på EU-marknaden
- användare av AI-system (både privatpersoner, företag och offentliga myndigheter)

AI förordningen trädde i kraft 2024 och dessa lagkrav ska självfallet uppfyllas och appliceras inom verksamheters användning av AI. Den började gälla stegvis från 2024 och ska vara fullt införd 2027.

2.1.2 Hot

Från ansvariga cybersäkerhetsmyndigheter och deras publicerade årsrapporter från 2024 och 2025 finns en generell och sammanvägd hotbild. Myndigheterna är ENISA (Den Europeiska Cybersäkerhetsbyrån), MSB, Säpo, MUST och FMV. Hoten och rekommendationerna är analyserade utifrån en allmän, generisk verksamhet (t ex en kommun).

Identifierade förändringar i hotbilden sammanfattas nedan:

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 penetrering av kommunala system. 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.

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

Hotbilden har under 2025 blivit bredare, snabbare och mer systematisk och kräver att kommuner arbetar integrerat med cyber, säkerhetsskydd och kontinuitet som en sammanhållen helhet.

Kommuner behöver förstärka sin motståndskraft genom att kombinera tekniska, organisatoriska och sociala skydd. Grundsäkerhet måste säkras genom s k 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.

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.

2.1.3 Trender

AI är fortsatt ett omoget område, juridisk, tekniskt och affärsmässigt men utvecklingen går snabbt.

Exploateringskontoret är ansvarig för sin informationsbehandling, oavsett om det sker med traditionell IT eller med hjälp av AI. Informationssäkerhetsaspekterna gäller oavsett teknik och behöver därmed beaktas och kontrolleras. Flera initiativ har tagits för att sprida information samt bredda kompetens och förståelse kring AI. Några intressanta projektidéer med AI-stöd har identifierats under året.

Från ett informationssäkerhetsperspektiv är det av stor vikt att en policy för allmänt tillgänglig generativ AI tas fram och beslutas för kontoret och vilken AI som är tillåten inom staden.

Myndigheten för digital förvaltning (DIGG) har publicerat en vägledning om hur förberedelser och arbetet med att implementera AI bör ske: Riktlinjer för generativ AI inom offentlig förvaltning Syftet med riktlinjerna är att ge regioner, myndigheter och kommuner vägledning och skapa trygghet i användningen av generativ AI samt underlätta användningen av den för att möta verksamhetens behov.

Övriga tydliga trender är generell samverkan hos olika aktörer – såväl inom som staden – och aktiviteter för att öka robusthet och motståndskraft genom att stärka skyddsmekanismer för informationssäkerhet/cybersäkerhet, it-säkerhet och dataskydd.

2.2 Yttre händelser inom staden – förutsättningar, förändringar, inriktningar eller resurser

Kvalitetsprogrammet betonar vikten av utökade krav och insatser för att säkerställa en god informationshantering. Uppdaterade tillämpningsanvisningar till riktlinjer för informationssäkerhet har publicerats.

Stadens funktion för övergripande informationssäkerhet har 2025 organiserats under stadens Säkerhetsavdelning och informationssäkerhetsansvarig (CISO) har erhållit en expanderad uppdragsbeskrivning.

Staden har infört en central s k *CERT-funktion* (Computer Emergency Response Team) som ansvarar för det dagliga arbetet med att förebygga, upptäcka och hantera cybersäkerhetsrelaterade händelser inom stadens it-miljö. CERT Stockholm fungerar som en gemensam resurs för hela staden ett komplement till det it-säkerhetsrelaterade arbete som bedrivs inom varje förvaltning och bolag. Detta kan vara avgörande för att kunna respondera korrekt och skyndsamt i lägen av allvarliga incidenter.

Ett *Informationssäkerhetsråd* finns etablerat inom staden. Rådets representanter besitter olika specialistinriktningar och kompetensfält och kan kontaktas vid frågeställningar och rådgivning kring åtgärder.

Staden anmodar användning av stödsystemet ***KLASSA*** för informationsklassificering. Systemet har uppdaterats till ny version 4 vilken innefattar en tydligare kravställning och mer anpassade frågor rörande dataskydd. En ny version 5 av systemet är under lansering 2026.

Nya digitala applikationer har införts för att öka säkerheten och kvalitet i distansarbete och kommunikation (t ex *Nordic for Zoom*, *Säkra meddelanden*).

Projektet för generativ AI inom Stockholm stad m fl kommuner, SveaGPT, fortlöper under 2026. Då det är av strategisk väsentlighet att stadens medarbetare bygger erfarenhet av AI-användning tillhandhåller SLK plattformen (ett utvecklingsprojekt med RISE) i syfte att stärka förståelse och förmåga att i tre aspekter:

- Kompetensutveckling, dvs att förstå teknikens möjligheter och begränsningar i det dagliga arbetet
- Verktyg, att verksamheten kan skapa och testa olika användningsfall
- Insikt om drift, förvaltningsmodell och utveckling av generativ AI

Under 2026 utvärderas (centralt) hantering av känslig information, behov av konsekvensutredningar (s k DPIA i GDPR), uppfyllnad av AI-förordningen och NIS2.
Informationsklassning kan behöva göras beroende på vad SveaGPT används till. Användare och ytterst nämnden är ansvarig för hur resultat från AI-tjänster används.

3 Risker och incidenter

3.1 Vad har verksamheten identifierat i RSA-arbetet

Arbetet med risk- och sårbarhetsanalys (RSA) bedrivs i tvåårscykler och en ny cykel inleds under 2026.

RSA-arbetet 2024–2025 fokuserade på hur samhällsviktig verksamhet påverkas av extraordinära händelser i fredstid och höjd beredskap. RSA-processen ska säkerställa att samhällsviktig verksamhet alltid kan fortgå. Endast ett område av exploaterings-nämndens verksamhet har bedömts som samhällsviktig – fakturering av markupplåtelser. Arbetet har under 2025 fokuserat på kontinuitetsplanering.

3.2 Resultatet från egen uppföljning (VoR och IKP)

I nämndens Väsentlighets- och Riskanalys (VoR) för 2025 har under verksamhetsområdesmål 3.5 ”Hög beredskap och stark rådighet ska råda i alla verksamhetsområden” under processen ”Systematiskt informationssäkerhetsarbete” identifierats sex oönskade händelser:

- Behörighetshantering - felaktig åtkomst till information (RV 9)
- Behörighetstilldelning Agresso (ekonomisystemet) – personer som inte ska ha behörighet till Agresso har behörighet eller för hög behörighet (RV 8)
- Implementering av lokal anvisning – medarbetarna tar inte del av lokal anvisning och riskerar därför att inte hantera information på korrekt sätt (RV 6)
- Incidenthantering - incidentrapportering görs inte enligt lagstiftning och övriga regler och rutiner (RV 9)
- Informationsklassning - avvikelser i informations-hanteringen jämfört med informationsklassning. (RV 8)
- Informationssäkerhet inom upphandlingsförfarande – Nödvändiga krav ställs inte (RV 6)

Ingen av dessa punkter överfördes till internkontrollplanen (IKP) för 2025.

3.3 Resultatet från revisioner

Under år 2025 har hittills inte någon rekommendation från revisionen lämnats om informationssäkerhet. Tidigare rekommendation från revisionsrapport nr 5/2019 *Implementering av dataskyddsförordningen*, bedöms vara åtgärdad.

3.4 Risker som identifierats i GDPR-årsrapport

I den årsrapport som Dataskyddsombudet (DSO) lämnade i samband med verksamhetsberättelsen, fanns ”brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga” för ett av de sex obligatoriska rapporteringsområdena.

Styrdokument
Fler rutiner för dataskyddsarbetet bör utarbetas och de som finns, bör uppdateras. Det gäller registerföring, incidenthantering, konsekvensbedömning och de registrerades rättigheter.

3.5 Risker i stadens outsourcade IT-leveranser (GSIT- och 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:

- Utpressningsattacker av stulen information (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

Matrisen visar hur dessa risker R1-R3 har bedömts av såväl 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, bl a genom deltagande i SLKs projekt *LångSIKT* som berör och föranleder insatser för efterlevnad från samtliga förvaltningar och bolag.

3.6 Information om avvikelser (incidenter och andra händelser)

Inga incidenter har hittills under året rapporterats i IA för exploateringskontoret.

3.6.1 Personuppgiftsincident vid Miljödata

Den 25 augusti fick Stockholms stad information från system-leverantören Miljödata om att deras it-miljöer utsatts för ett dataintrång. Den 14 september publicerade hotaktören de stulna personuppgifterna på Darknet, däribland personuppgifterna från Stockholms stad. Darknet är en krypterad del av internet som nås med specialprogram.

De personuppgifter som Stockholms stad hade hos Miljödata är medarbetares:
• personnummer
• förnamn och efternamn
• telefon och mobiltelefon (hem och/eller till arbete)
• e-postadress (hem och/eller till arbete)
• utdelningsadress (hem)
• organisationskopplingar (Webb-ID strukturen i LISA självservice)
• anställningsidentitet/AD-konto
• anställningsperiod

• anställningsform
• yrke/befattning (yrkeskod).

Incidenten berör personuppgifter om medarbetare som är eller har varit anställda vid stadens förvaltningar under perioden 2024 till augusti 2025.

Stockholms stad har anmält personuppgiftsincidenten till Integritetsskyddsmyndigheten (IMY) och till polisen. Även exploateringskontoret har anmält personuppgiftsincidenten till IMY.

4 Verksamhetens arbete med informationssäkerhet

4.1 Arbete och aktiviteter under innevarande period

Under 2025 har arbetet med informationssäkerhet och dataskydd fortskridit med bland annat följande aktiviteter.

- En genomgång mellan förvaltningschef och informationssäkerhetssamordnare (och del av genomgång med dataskyddsombudet) har ägt rum för att informera och belysa grunder och status inom respektive område för informationssäkerhet och dataskydd.

- I samband med verksamhetsberättelse och bokslut tar förvaltningen del av dataskyddsombudets överlämnade årsrapport och stor hänsyn tas till eventuella rekommendationer till personuppgiftsansvarig som lämnas i rapporten.

- Uppdatering pågår av *Lokal anvisning för informationssäkerhet inom exploateringskontoret*.

- Revidering av *Rutin för personuppgiftsincidenter inom exploateringskontoret*.

- Kontroll av status gällande genomgångna obligatoriska e-utbildningar hos samtliga medarbetare. Det har i denna kontroll konstaterats ett akut behov av att återkomma med en uppdaterad information till de medarbetare som inte förnyat eller genomgått de två obligatoriska e-utbildningarna.

- Initierat upphandlingar av konsult för informationsklassning av ett flertal objekt och informationstillgångar.

4.2 Planerat och prioriterat arbete samt aktiviteter under kommande perioder

4.2.1 Verksamhetsår 2026

Under 2026 förslås som prioriterade åtgärder att genomföras följande aktiviteter:

1. Att etablera en teknisk plattform för lokalt LIS (två separata samarbetsytor) och sammanställa interna underlag, rutiner och processbeskrivningar.

2. Att sammanställa personuppgiftsbiträdesavtal med bilagan instruktion för personuppgiftsbehandling.

3. Att inventera och dokumentera vilka informations-klassningar som är genomförda och lagra dokumentationen i annat system än KLASSA 4. Säkerställa att samtliga prioriterade informationstillgångar är klassade och att klassningars handlingsplanernas tekniska och organisatoriska åtgärder implementeras.

4. Att genomföra omklassningar av befintliga lokala verksamhetssystem. Övergången av server- och applikationsdriftstjänster från det nuvarande GSIT-avtalet till stadens nya Systemtjänsteavtal skedde under första halvåret 2025.

   Under 2026 bedrivs uppföljningsprojektet *LångSIKT* som kommer att innebära skärpta krav för permanent etablering av lokala verksamhetssystem till nya nätverkszoner, segmentering, integrations- och kommunikationsregelverk mellan olika system.

5. Att inventera system- och applikationsbaserade person-uppgiftsbehandlingar och uppdatera registerförteckning. Registerförteckningen ska omformas och införas i lokalt LIS. Fokus ligger på verksamhetsprocesser som kan innehålla volymer av integritetskänsliga och känsliga personuppgifter.

6. Att etablera en rutinprocess för begäran av registerutdrag. Individers rättigheter till begäran om tillgång av registrerade personuppgifter (registerutdrag) har av Europiska dataskyddsstyrelsen (EDPB) valts ut som ett fokusområde

för 2024 och det är därmed ett område som kommer att prioriterats av dataskyddsmyndigheterna.

7. Att inventera och tilldela informationsägare till respektive informationsbärande system och applikation. Roller och ansvar kring informationssäkerhet ska vara tydliggjorda och förankrade i verksamheten.

8. Att behörighetshantering ska dokumenteras (gällande teknik, process, rutin) för respektive system.

9. Att verka för etablering enligt stadens vedertagna förvaltningsmetod pm3 för de kvarvarande objekt som bör omfattas. Objektägare och objektledare ska verka som informationsägare.

10. Att fortsätta informera om förutsättningar som interna riktlinjer och lagar gällande användning av AI.

11. Att följa upp obligatoriska e-kurser gällande informationssäkerhet och dataskydd och återkoppla till verksamheten. Information ska ske vid introduktion för nyanställda och externa konsulter. Planera generellt kompetenshöjande insatser och medverka som stöd i verksamhetskopplade frågor.

    Riktade och rekommenderade fördjupande utbildningsinsatser för chefer och ansvariga informationsförvaltare bör anmodas berörda.
    Utbudet av tillgängliga e-utbildningar framgår av tabellen

Tillgängliga e-utbildningar 2025
Chefer, ledningsgrupp och medarbetare med specialistområden

Namn	Beskrivning	Krav	Typ
Informationssäkerhet för medarbetare i staden	*Grundutbildning inom informationssäkerhet.*	*Obligatorisk för samtliga*	*Certifiering*
Informationssäkerhet – Fördjupning	*Fördjupningskurs inom informationssäkerhet*		*E-lärande*
Informationssäkerhet för chefer	*Utbildning för roll som chef*		*E-lärande*

Informationssäkerhet: Ledningsgruppens ansvar	*Utbildning för förvaltningschef och ledningsgrupp*		*E-lärande*
Förberedelse inför informationsklassning	*Deltagare i klassningar*		*E-lärande*
Grundutbildning i dataskydd		*Obligatorisk för samtliga*	*Certifiering*
Fördjupning i dataskydd – överföring till tredje land		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – rättslig grund		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – personalfrågor		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – webbpublicering och e-post		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – känsliga personuppgifter		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – offentlighet och sekretess		*Obligatorisk för berörda roller*	*E-lärande*
Fördjupning i dataskydd – registerutdrag		*Obligatorisk för berörda roller*	*E-lärande*

4.2.2 Verksamhetsår 2027 - 2028

Under 2027 och 2028 förslås som prioriterade åtgärder att genomföras följande aktiviteter:

1. Fortsatt förstärkning av strukturerat och systematiskt informationssäkerhetsarbete som ska anpassas efter och uppfylla ställda centrala eller lokala krav.

2. Utvärdera om förvaltningsspecifik utbildning ska tas fram för exploateringsprojekt: Informationssäkerhet inom exploateringsprojektverksamhet.

3. Eventuellt införande av intern normerande informations-klassning för projektstödsystem. Kartläggning vilka externa normerande klassningar som finns att tillgå, t ex centrala system och plattformar.

4. Genomföra övningar av incidenter och provtryckningar av säkerhetsmekanismer i processer inom verksamhetens delar

och hos ansvariga it-leverantörer.

5. Fortsätt arbete med framtagande och förvaltning av enhetliga begrepps- och informationsmodeller som medger integrerat systemstöd i lokala verksamhetssystem för underlättande av funktioner och informationskontroll.

6. Utöka omvärldsbevakning kring identifiering av externt påverkande krav eller lagar, myndigheter, generell omvärldsbevakning och bredda/stärka förvaltningens kompetensförsörjning. Samverkan med andra förvaltningar och organisationer.

7. Utreda behov och lokalt stöd för informationssäkerhet i geodatahantering och GIS-plattformar för kartstöd.

8. Regelbunden och löpande revidering av lokala processer och styr- och stöddokumentation.

9. En cyklisk handlingsplan (årshjul) för systematiska aktiviteter vidareutvecklas. Planen ska synkroniseras med dataskyddsombudets aktiviteter.

Observera att några aktiviteter kan omformas och fler kan tillkomma.

Detta dokument är fastställt av förvaltningschef och informationssäkerhetsansvarig Thomas Andersson december 2025.