Informationssäkerhet

- Ledningens genomgång år 2026

Servicenämnden

Ledningens genomgång
Bilaga till Servicenämndens Verksamhetsplan 2026
Dnr:
Kontaktperson: Vendela Engblom

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.[1]

I *Anvisningar för nämndernas arbete med verksamhetsplan 2026* 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 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden. För 2026 driver arbetet med NIS2 prioriteringar, i synnerhet arbetet med säkerhet i leveranskedjan samt risker och utbildning av ledning och verksamhet.

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

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 riktlinje som är en bilaga till stadens Kvalitetsprogram[2]. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För servicenämnden räkning har förvaltningschef fastställt en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom serviceförvaltningen.

1.1 Vad påverkar servicenämndens informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska serviceförvaltningen 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. Detta blir extra prioriterat i och med införandet av NIS2 som träder i kraft 16 januari 2026, vilket tydliggör kravet på riskbaserat arbetssätt i alla verksamheter som omfattas. Serviceförvaltningen har också en särskild ställning i stadens informationssäkerhetsarbete i och med förvaltningens roll i det centrala upphandlingsuppdraget genom omhändertagandet av stadens kravställning i informationssäkerhet samt i andra uppdrag där förvaltningen hanterar stora mängder av information åt andra verksamheter i staden. Förvaltningens informationshantering inkluderar känsliga personuppgifter för medborgare och anställda och i vissa fall även känslig infrastrukturinformation.

[2] Stockholms stads kvalitetsprogram (start.stockholm)

1.1.1 Finansborgarrådets förslag till budget 2026

Budgetuppdrag
Servicenämnden ska inom ramen för sitt uppdrag arbeta med att effektivisera stadens administrativa funktioner. Servicenämnden ska säkerställa en ändamålsenlig balans mellan kostnadseffektivitet, kvalitet och service. Finansiering och prissättning av servicenämndens tjänster ska utvecklas för att möjliggöra fortsatta effektiviseringsvinster med bibehållen kvalitet. Servicenämndens kärnverksamhet är i huvudsak administrativa tjänster. Inom ramen för befintliga verksamhetsområden ska servicenämnden förbättra kvaliteten, utveckla tjänsterna och bredda nyttjandet. På uppdrag av kommunstyrelsen och andra nämnder eller bolag ska servicenämnden svara för genomförandet av gemensamma administrativa processer för att möjliggöra stordriftsfördelar, kvalitetssäkring av stadsgemensamma processer samt för minskad sårbarhet, något som ger värde för hela kommunkoncernen. Ett nytt exempel här är att serviceförvaltningen har anställt dataskyddsombud och kan därigenom erbjuda den tjänsten till andra förvaltningar och bolag.

Servicenämnden ska prioritera upphandlingsarbete för stadens nämnder och bolag samt tillhandahålla utbildning, support och stöd inom upphandling och inköp. Det finns risker för att offentligt upphandlad verksamhet nyttjas i brottsliga syften. Nämnden ska fortsatt rikta särskild uppmärksamhet på att motverka brottslig verksamhet. Servicenämnden ska stärka det stöd som ges till nämnder och bolag vad avser avtalsuppföljning vid identifierade avvikelser gällande leveranser och utförande av tjänster. Nämnden ska även utföra systematiska och kontinuerliga kontroller av leverantörers skyldigheter rörande skatter och avgifter. Servicenämnden ska skapa förutsättningar och erbjuda stöd för ökad samverkan mellan stadsdelsnämndernas inköpsverksamheter avseende upphandling och avtalsuppföljning. Servicenämnden ska aktivt söka samordningsmöjligheter och stödja nämnder och bolag där gemensamt upphandlingsbehov identifieras, inklusive gemensam avtalsförvaltning, avtalsuppföljning och metodstöd. I samråd med kommunstyrelsen ska servicenämnden utveckla tjänster för avtalsuppföljning inom nämnder och bolag.

I årets budget höjs ambitionerna för arbetet med informationssäkerhet ytterligare. Det omfattande dataläckage som drabbat stora delar av det offentliga Sverige under året visar på ett behov av att göra mer för att öka säkerheten.

Servicenämnden ska delta i arbetet inom stadens sektorsorganisation för civil beredskap och i samråd med kommunstyrelsen förvalta och bygga upp ytterligare förmåga genom centralt beredskapslager.

Servicenämnden ska även delta i arbetet inom stadens sektorsorganisation för civil beredskap.
Serviceförvaltningen är utsedd sektorsansvarig för *Livsmedelsförsörjning och dricksvatten*. Som sektorsansvarig ska förvaltningen hålla samman beredskapsutvecklingen och få till stånd samverkan inom sektorn. I takt med utvecklingen av strukturen och sektorsorganisationen kan det bli aktuellt att ta fram och löpande uppdatera sektorsspecifika risk- och sårbarhetsanalyser. Förvaltningen har även ansvaret att hålla ihop sektorns samverkan och samordning med statliga myndigheter och näringsliv.

Intern kontroll

Syftet med intern kontroll är att skapa förutsättningar för en ändamålsenlig och effektiv användning av skattemedel samt för att upprätthålla service med hög kvalitet till kommuninvånarna.

Genom en tillräcklig intern kontroll skapas förutsättningar att förebygga, upptäcka och åtgärda oönskade händelser och därmed minimera risker i verksamheten samt säkra tillgångar och förhindra förluster och oegentligheter som skadar stadens anseende. Arbetet med intern kontroll är en del av stadens kvalitetsarbete.

Utöver nämndens egna identifierade processer ska nämnden, enligt stadens anvisning, ha med den obligatoriska stadsövergripande processen *Systematiskt informationssäkerhetsarbete* i sin väsentlighets- och riskanalys och bedöma om de ska med i internkontrollplanen.

Serviceförvaltningen gör varje år en bedömning av de fem obligatoriska arbetssätten, *behörighetshantering, implementering av lokal anvisning, incidenthantering, informationsklassning* och *informationssäkerhet inom upphandlingsförfarandet*, i väsentlighets- och riskanalysen. Därefter beslutar förvaltningsledningen om vilka av arbetssätten som ska ingå i intern kontrollplanen kommande år.

1.1.2 Risk och sårbarhetsanalys

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleds under 2026.
Serviceförvaltningen har i risk- och sårbarhetsarbetet 2024 identifierat ett antal processer som kan ha risker inom informationssäkerhet och har åtgärdsplaner och kontinuitetsplaner för de delar som förvaltningen har rådighet över. Förvaltningen följer stadens risk- och sårbarhetscykel och instruktioner. Under 2025 har prioriteringen varit att säkerställa kontinuitetsplaner.

- Det har konstaterats att förvaltningens processer delar risker för system, el- och personalbortfall. Kontinuitetshantering för dessa risker bör därmed kunna hanteras lika över hela förvaltningen. Principer har formas och beslutas av förvaltningsledningen i november 2025.
- Övningar är planerade på flera avdelningar och chefsgruppen krisövar i december.
- De två objekt som förvaltas på SRV: Artvise har kontinuitetsplan, kontaktcenterplattformen har tagit fram åtgärder samt säkerställt fallbackhantering under 2025, plan sammanställs i Q1 2026.

Utöver förvaltningens egna risk- och sårbarhetsarbete kommer förvaltningen att arbeta med dessa frågor inom sektorsorganisationen, både för den sektor som förvaltningen ansvarar för, samt för de tre som serviceförvaltningen deltar i. Dessa frågor kommer också att tas upp i riskinventeringen för NIS2.

1.1.3 Resultatet från egen uppföljning (IKP)

I Servicenämndens tertialrapport 2 2025 rapporterades följande; Intern kontroll har till största delen skett enligt plan utan att några väsentliga avvikelser har identifierats. Förvaltningen har under året stärkt arbetet med systematiska behörighetskontroller, det har exempelvis inneburit att samtliga medarbetares tillgång till gruppdiskar, funktionsbrevlådor och sändlistor och liknande under perioden har kontrollerats. Arbetet är en systematisk kontroll i förvaltningens internkontrollplan och kommer att kontrolleras två gånger per år.

En väsentlig avvikelse har dock uppkommit, vilket avser objektförvaltning av stadens kontaktcenterplattform Telia Ace. Förvaltningen har vidtagit åtgärder, bland annat genom att systemförvaltningen av plattformen under perioden har präglats av förstärkt avtalsuppföljning, registervård och behörighetskontroller i syfte att säkerställa att leverantören lever upp till de krav som har

avtalats. Förvaltningen har en nära dialog med leverantören i syfte att säkra leverans och funktionalitet. Serviceförvaltningen har under perioden fått i uppdrag från kommunfullmäktige att genomföra en ny central upphandling och implementering av kontaktcenterplattform (KCP). Detta till följd av att betydande brister upptäckts i nuvarande plattform samt att samarbete och dialog med nuvarande leverantör varit utmanande sedan avtalets start.

För att ytterligare förstärka arbetet med informationshantering har systemstödet VisAlfa upphandlats, och införandeprocessen pågår för att säkerställa att verktyget kan hantera både förvaltningens omfattande personuppgiftsbehandlingar samt informationssäkerhetsarbete.

1.1.4 Risker som identifierats i GDPR-årsrapport

Förvaltningen har under de senaste åren bytt dataskyddsombud tre gånger, och har nu anställt dataskyddsombud i egen regi som även (genom konsultrollen via DIT) hanterar fem andra förvaltningar.

GDPR-årsrapporten från 2024 innehöll följande avvikelser som bedömdes av dåvarande DSO som allvarliga:

- Tröskelanalyser och konsekvensbedömningar behöver genomföras strukturerat
- Uppdatera lokal anvisning för informationssäkerhet
- Utbilda ledningen i personuppgiftsansvar
- Information till registrerade internt behöver förtydligas
- Instruktion till personuppgiftsansvariga behöver skickas ut och fastställas
- Få bättre kontroll över processer där ni hanterar känslig information

Följande åtgärder har genomförts:

- **Konsekvensbedömningar.**
    - Kartläggning + prioritering av de känsligaste processerna som bör konsekvensbedömas är gjord
    - Konsekvensbedömning av majoriteten av SF:s känsliga processer görs i samband med upphandling av nytt ärendehanteringssystem (Q4 2025-Q1 2026)
    - Tröskelanalys + konsekvensbedömning görs numera strukturerat i centrala + lokala upphandlingar, vilket har påverkan på även

andra förvaltningar och bolags strukturerade hantering av personuppgifter.

- **Information till registrerade internt**
  - Förvaltningen bedömer att stadens centrala information till anställda (nyligen uppdaterad) täcker även förvaltningens informationsbehov.
- **Information till kandidater om personuppgifts-registrering**
  - Stadens rekryteringsprocess har uppdaterats med information till registrerade i varje del av processen för att minimera risken av att en kandidat upplever att de inte fick tillräckligt med information om hur deras personuppgifter hanteras.

- **Instruktion till SF:s kunder (PUB)**
  - Beslut fattades av förvaltningschef Charlotte Goliath i samband med presentation av Ledningens genomgång 4 november att den version av instruktionen som skickats ut till kunder får fortsätta gälla.

- **Uppdatera lokal anvisning**
  - Förvaltningen genomför årlig uppdatering av den lokala anvisningen för informationssäkerhet i december 2025.

- **Förstärk kunskap och hantering av processer där förvaltningen hanterar känslig information**
  - Stora delar av förvaltningens känsliga processer har informationsklassats i samband med processen för upphandling av nytt ärendehanteringssystem. Detta för att tydligt identifiera för ansvarig ledning vilka processer där de hanterar känslig information, inklusive sekretess, känsliga personuppgifter, med mera. Detta kommer att leda till arbete på avdelningsnivå med identifierade risker, och i stort förstärka SRV:s hantering av känslig information (och därmed även Stockholm stads informationssäkerhet).

GDPR-årsrapporten från 2025 innehåller följande prioriteringar:

- Serviceförvaltningen får beröm för sitt arbete
- Översynen av incidenthanteringen – det rekommenderas att det påbörjade arbetet med en översyn av incidenthanteringsprocessen slutförs (se 1.1.7)
- Personuppgiftsincidenter – serviceförvaltningens personuppgiftsincidenter är i regel alltid av ringa karaktär och orsakas av enkla misstag i hanteringen. Det rekommenderas att undersöka huruvida det kan finnas tekniska lösningar för att undvika vissa av dessa.
- Översyn av personuppgiftsansvarsfrågan – serviceförvaltningens personuppgiftsbiträdesansvar samt personuppgiftsansvar för interna processer som görs i centrala system bör ses över. Ibland kan det vara fråga om gemensamt personuppgiftsansvar snarare än en biträdesroll.
- Tredjelandsöverföring. Kontroll och mitigering av risker kopplat till detta.
    - Rekommenderas att verksamheten granskar befintliga system och processer löpande för att identifiera tredjelandsöverföring och risker kopplat till detta. Både central och lokal risk, samt relevant för centrala upphandlingsuppdraget. Delaktighet i referensinformation, dela information, etc.

1.1.5 Utbildning av förvaltningsledningen samt enhetschefer och vissa avdelningar

Utifrån kunskap om kommande lagstiftning och ledningens ansvar, för att lägga bottenplattan för NIS2**,** har följande utbildningar genomförts:

- Utbildning om riskbaserat arbetssätt samt AI-relaterade risker för förvaltningsledningen
- Genomgång av ISAM:s analys utifrån mognadsdialogen (MSB:s arbetssätt) för incidenthantering och riskhantering med förvaltningsledningen
- Utbildning om riskbaserat arbetssätt samt AI-relaterade risker på chefsforum och för lokalplanering
- Workshop för att genomföra mognadsdialogen (MSB:s arbetssätt) för riskhantering med förvaltningsledningen
- Genomgång av NIS2 för Kontaktcenter Stockholms ledningsgrupp

- Genomgång av NIS2 med funktionen för informationssäkerhet
- Utbildning i vikten av korrekt behörighetshantering med ekonomiavdelningens processledare

1.1.6 Informationsklassning – utveckling och åtgärder

Före, *nulägesbeskrivning från VP 2024*:

- Informationsklassningar i olika faser av upphandlings- och avtalsprocessen behöver struktureras och stärkas.
- Normerande klassningar görs oftast inte i upphandlingar hos serviceförvaltningen om inte tydlig IT-tjänst (detta var allmän praxis i staden).

Genomförda aktiviteter under året:

- Ny förenklad blankett inför klassning samt förklarande presentationsmaterial publicerat på intranätet
- Ny roll införd: klassningsledare som ansvarar för dokumentation och guidning i klassningsprocessen
- Förbättrad klassningsprocess presenterades för förvaltningsledningen i februari, där ingick en ny processkarta och en tydligare beskrivning av roller som kunde behövas
- Inventering av klassningar på serviceförvaltningen är genomförd
    - Genomfört/pågående omkring 40 klassningar
- Pågående förbättringsarbete kring pedagogik, förutsägbarhet och struktur för alla involverade
- Informationsklassning sker för alla centrala upphandlingar
- Informationsklassning sker för interna upphandlingar, även ibland för justering av system
- Informationsklassning av förvaltningens processer skedde i Q4 2025 i samband med upphandling av nytt ärendehanteringssystem.

1.1.7 Incidenthanteringsprocess – utveckling och åtgärder

Incidenthantering på serviceförvaltning upplevs som en tungrodd och svår process. Detta beror delvis på en upplevelse av att systemstödet inte matchar behovet och delvis på att den stora volymen personuppgiftshantering med många manuella steg (både i system och i t.ex. brevhantering) gör att det sker ett flertal incidenter av ringa karaktär som genererar mycket arbete för anställda. Det är tydligt att antalet incidenter ökar under 2025; detta beror i stort sett enbart på att verksamheter har blivit mycket bättre

på att urskilja när incidenter sker och när de ska rapporteras. Omkring 100 incidenter har skett under året, den stora majoriteten är personuppgiftincidenter varav endast en bedömts vara av sådan karaktär att den behövs rapporteras till IMY (Miljödata).

Det finns därmed ett behov av att tydliggöra processen, hjälpa verksamheten förenkla hanteringen, och undersöka om förebyggande arbete är möjligt.

Under 2025 har ett flertal verksamhetsområden tagit fram rutiner eller påbörjat arbetet för att förenkla hantering.

Serviceförvaltningens ISAM har tillsammans med förvaltningens dataskyddsombud tagit fram en plan för en användarresekartläggning av incidenthanteringen, och genomför omkring 12-14 intervjuer under november och december månad. Utkomsten av denna kommer att vara en kartläggning över incidenthanteringsprocessen och detta kommer i sin tur möjliggöra ett antal åtgärdsförslag samt en ny incidenthanteringsrutin.

2.1 Serviceförvaltningens informationssäkerhetsarbete under 2026

2.1.1 Serviceförvaltningens lokala anvisning för informationssäkerhet

Förvaltningen har en lokal anvisning för informationssäkerhet. Anvisningen är presenterad i sin helhet för förvaltningens samtliga chefer och finns tillgänglig för alla medarbetare på förvaltningens samarbetsyta.

Enligt anvisningen har serviceförvaltningen inte ett fastställt årshjul för arbetet med informationssäkerhet, utan planerar arbetet utifrån väsentlighets- och riskanalysen som genomförs i samband med verksamhetsplaneringen och framtagande av intern kontrollplan.

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

Under fjärde kvartalet 2025 kommer anvisningen att uppdateras för att reflektera förändringar i informationssäkerhetsarbetet, inklusive rekryteringen av dataskyddsombud samt introduktionen av

klassningsledare och breddningen av informationsklassningar i det centrala upphandlingsarbetet.

2.1.2 *NIS2 – prioriterade områden*

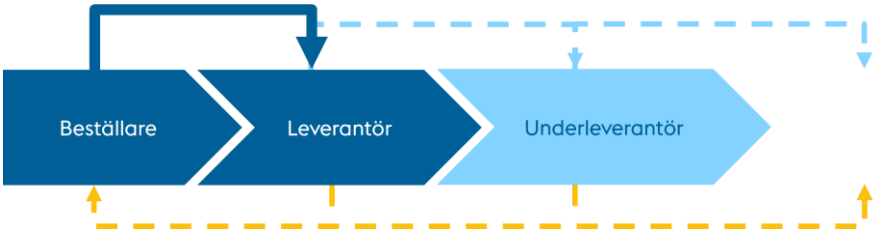
NIS2 specificerar 10 åtgärdsområden för verksamheter. För 2026 har serviceförvaltningen valt att fokusera på:

- **Riskhantering**
  Serviceförvaltningens särskilda ställning i stadens informationssäkerhetsarbete eftersom förvaltningen hanterar stora mängder information, inklusive känslig information, åt stadens förvaltningar och bolag gör att ett riskområde som tydligt behöver arbetas med är informationssäkerhetsrisker. Arbetet med riskhantering inkluderar en riskinventering av förvaltningens ISAM samt säkerhetsansvarig som delvis kommer att utgå ifrån väsentlighet och riskanalysen, riskerna som identifierats i serviceförvaltningens riskanalys inför upphandling av ärendehanteringssystem och riskprocesser identifierade i processklassning för den upphandling. Utöver det kommer varje avdelning ges tillfälle att arbeta med sina informationssäkerhetsrisker med stöd av förvaltningens ISAM, samt andra aktiviteter som kommer ur riskinventeringen.

- **Incidenthantering**
  Incidenthantering i NIS2 kräver att det grundläggande incidenthanteringsarbetet är välfungerande och lätthanterligt. Därför har serviceförvaltningen valt att lägga extra vikt vid att utveckla förvaltningens arbete på detta område. Se 1.1.7 för vidare beskrivning av arbetet.

- **Säkerhet i leveranskedjan**
  Förvaltningens jurist har utrett NIS2:s troliga påverkan på förvaltningens verksamhet och konstaterat att serviceförvaltningen omfattas, och kan omfattas på flera sätt. Säkerhet i leveranskedjan kommer att bli extra viktig för serviceförvaltningen utifrån det centrala upphandlingsuppdraget. En viktig risk här att ta hänsyn till för serviceförvaltningen är att även om det juridiska ansvaret för underleverantörer endast omfattar den direkta leverantören så kommer det med största sannolikhet bli så att förvaltningen måste ta hand om indirekta risker, vilket innebär underleverantörer och

eventuellt i vissa fall underleverantörer där inget avtal existerar.



- **Utbildning av ledning och anställda**
  Utbildning är utpekat som en viktig säkerhetsåtgärd i NIS2, och serviceförvaltningen bedömer att det behöver prioriteras och planerar för en utbildning i olika områden i informationshantering under 2026. Målet för utbildningen är att den enskilde anställda känner en trygghet i det hen behöver hantera, och att chefer och experter har tydlig kunskap och ett ansvarskännande över sitt verksamhetsområde.

2.1.3 Skyddade personuppgifter

Miljödata-incidenten tydliggjorde att staden som helhet behöver få bättre kontroll över hur skyddade personuppgifter hanteras. Serviceförvaltningen har ett särskilt ansvar för detta i och med verksamhetsområde Lön och Pension. En stor förändring sker under första halvan av 2026 genom automatisering av hanteringen av skyddad folkbokföring, vilket kommer att innebära en rutinförändring. Dagens rutin och tillhörande internkontroll hanteras med största noggrannhet.

I övrigt arbetar serviceförvaltningen med:

- Ett förbättrat chefsstöd för att stötta förvaltningens chefer i hantering av anställda med skyddad folkbokföring
- En inventering av riskprocesser där förvaltningen hanterar personuppgifter i stora volymer och det inte flaggas om en person har skyddad folkbokföring men adresser eller andra känsliga uppgifter ingår. De flesta av dessa processer hanteras via centrala system där serviceförvaltningen inte har rådighet över kravställningen, men förvaltningen ska upphandla nytt ärendehanteringssystem under 2026 och där kan det bli aktuellt med relaterad kravställning.

3 Prioritering av åtgärder

3.1 Under 2026 ska serviceförvaltningen

- chefer;
  - årligen ser till att samtliga medarbetare och konsulter genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
  - genomföra de utbildningsinsatser och riskrelaterade åtgärder som förvaltningen pekar ut för deras avdelningar och enheter
  - 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.

Förvaltningen har informationssäkerhet som återkommande tema på chefsforum för att upprätthålla kompetens och rutiner. Den lokala anvisningen ska även revideras i avsnitt 4 om befintliga rutiner, eftersom nya rutiner har framkommit sen anvisningen fastställdes.

Under 2026 ska serviceförvaltningen prioritera;
- fortsätta utveckla rutiner för att tydliggöra informationssäkerhet i inköpsprocessen kopplat till säkerhet i leveranskedjan (NIS2)
- utveckla hanteringsanvisningarna
- Revidering av lokal anvisning för informationssäkerhet
- att 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 (NIS2)
- Öva enligt kontinuitetsplaner
- Genomföra utbildningsinsats inom informationshantering, fokusområde incidenthantering, riskarbete samt personuppgifter, m.fl. (NIS2)
- Överväga skapandet av centralt riskregister på förvaltningen.
- Säkra kompetens och resurser i enlighet med definierat uppdrag och ansvar avseende hantering av informationssäkerhet i centrala upphandlingar.

3.2 Under 2027 ska serviceförvaltningen
- Granska hur väl lokal rutin för regelbundna informationsklassningar följs
- Identifiera och genomföra ytterligare åtgärder som krävs för NIS2

- Säkra kompetens och resurser i enlighet med definierat uppdrag och ansvar avseende hantering av informationssäkerhet i centrala upphandlingar.
- Revidera lokal anvisning
- Öva enligt kontinuitetsplaner.

3.3 Under 2028 ska serviceförvaltningen

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