Stockholms stad

Informationssäkerhet Ledningens rapport 2023

Ledningens genomgång av informationssäkerhet 2023

Inledning

Ledningens genomgång är en del i ett systematiskt informationssäkerhetsarbete. Ledningen ska hålla sig informerad om informationssäkerheten i sin verksamhet. Informationsägare och Personuppgiftsansvarig är nämnden. Operativt ansvarig är förvaltningschefen som ska se till att resurser finns och medarbetare har utbildning och information som krävs för uppdraget. Övergripande informationssäkerhetsansvarig finns på stadsledningskontoret. Lokalt på alla nämnder och bolag finns informationssäkerhetssamordnare (ISAM). Informationssäkerhetens ansvar ska följa linjeorganisationen, nämnderna arbetar utifrån stadens riktlinjer och tillämpningsanvisningar och ska anta egna lokala anvisningar.

Denna ledningens genomgång är byggd enligt uppdelning och principer från MSBs metodstöd för informationssäkerhet. Staden arbetar fortfarande med att ta fram en gemensam mall för ledningens genomgång, vilket kommer användas vid framtida genomgångar.
Tidigare genomgång gjordes i december 2022. I årshjulet har ledningens genomgång flyttats till augusti. Detta för att kunna planera och ta tillvara de slutsatser och analyser som kommer fram till arbetet med verksamhetsplan 2024. Nytt för i år är en bilaga med GAP-analys utifrån ISO 27001 med nulägesanalys och kommentar om förslag på handlingsplan.

I denna genomgång presenteras status på olika aktiviteter och krav. Grönt indikerar att aktiviteter genomförts och/eller att inga stora avvikelser noterats. Gult indikerar att det finns fortsatta brister, fler åtgärder behöver vidtas eller att arbete pågår.
Under sista delen presenteras förslag till åtgärder. Flertalet av åtgärderna kommer att presenteras i framtida lokala tillämpningsanvisningar. Andra föreslås lösas på annat sätt.

Årets rapport borde överlämnats i November, men tidigareläggs. Dels som en del i rekommendationer för att bättre vara i fas med verksamhetsplansarbetet, men också för att detta år minimera kunskapstapp i samband med personalbyte.

Sammanfattning

Årets rapport har tidigarelagts till Augusti, dels som en del av framtida rekommendation och dels för att förbättra kunskapsöverlämning i samband med personalbyte.
Rapporten går igenom analyser av nuläget och kommer med rekommendationer för fortsatta arbetet vad gäller informationssäkerhet. Rapporten går även igenom årets informationssäkerhetsincidenter samt gör en analys utifrån ISO 27001 för att kunna visa hur förvaltningens arbete med informationssäkerhet fortgår.
Under året har en ökad medvetenhet inom informationssäkerhet skett inom förvaltningen och ett mer systematiskt informationssäkerhetsarbete finns. Flera av tidigare brister har klarmarkerats och förbättringar har skett främst utifrån den nya organisationen för objekt enligt PM3, samt de tillämpningsanvisningar som antagits.
För att motverka konstaterade brister föreslås ett antal åtgärder:

- Ledningens rapport ska i fortsättningen lämnas redan i september månad.
- Förvaltningen verkar för att stadsgemensamt delegerat ansvar på tjänstemannanivå tas för centrala system för att hantera beslut rörande informationssäkerhet och att objektnära organisation förvaltas gemensamt på uppdrag från förvaltningar för dessa system.
- Förvaltningen tar fram en lista på kompetensbehov för förvaltningen vad gäller informationssäkerhet som kan användas vid rekrytering och för att se över behovet av kompetensutveckling.
- En lista på intressenter tas fram i workshop
- Inspirerande utbildningar i incidentrapportering och utredning tas fram för chefer, för att öka engagemanget för incidenthantering inom organisationen och förbättra dokumentationen
- Förändrad delegationsordning där ansvar för inköp av digitala system tas på högre nivå.
- Utbildningar för dataskyddshandläggare och objektledare under 2024
- Enklare lathund för incidenthantering i IA tas fram.
- Förvaltningen engagerar sig i utvecklandet av nytt incidenthanteringssystem som tas fram av staden.

Uppföljning av tidigare beslut

Beslut om informationssäkerhet har tagits för förvaltningen genom de lokala tillämpningsanvisningarna fastställda av direktör 2022-02-08.
I den beskrivs förvaltningsspecifik organisation, årshjul och rutiner för verksamheten som rör informationssäkerhet.

Uppföljning av de lokala tillämpningsanvisningarna.

Organisation

Funktion i organisation	Roll enligt anvisning	Status
Ledning	Utse nödvändiga roller inom organisationen samt anta de lokala tillämpningsanvisningar. Tillse att resurser finns och medarbetare har den utbildning och information som krävs för uppdraget	Nödvändiga roller har tillsatt till viss del, PM3-arbetets implementering fortgår.
Chefer	Utreda incidenter, säkerställa registervård, att göra inköp i enlighet med gällande lagar och styrdokument, att ha klassat viktiga tillgångar, ta fram lokala rutiner för egna verksamheten utifrån behov.	Brister har skett vid inköp av digitala system eller vid ändringar av digitala system. Konsekvensbedömningar har inte alltid gjorts. Incidentrapporter hanteras inte inom tidsspann. Inventering och registervård finns en handlingsplan och arbetas med under året med stöd från ISAM.
Processägare	Äger processer inom verksamhetsområde inom klassificeringsstruktur. Fattar beslut när osäkerhet uppstår vid hantering av information.	Rollen utsedd och prövad i praktiken.
Objektägare	Ansvarar för informationstillgången (objekt) och utser objektledare	Roller utsedda för objekt hitintills, arbete fortgår men inte klart. Plan finns för fortsatt arbete.
ISAM	Att vara kontaktpunkt, rådgöra, samverka och stödja, omvärldsbevaka och följa upp	Bedöms av ledningen

DSO	Vägleda, informera, självständigt bevaka de registrerades intressen.	Bedöms av ledningen
ILS-samordnare, Arkivansvarig och stadsdelsarkivarier	Stödjande inom sina respektive områden	Inga noteringar.
Objektledare	Ansvarar för informationssäkerhet i objekt genom att se till att dokumentation finns på plats och att rutiner finns och följs.	Där objektledare har utsetts har dessa delar fungerat. Ett större ansvar för att se till dessa delar behöver flyttas från ISAM till objektledare.
Dataskyddshandläggare	Ansvarar för praktiska arbetet med registervården på respektive chefs uppdrag.	Har inte startat ännu, personer utsedda. Start under hösten 2023.
Övriga roller, medarbetare, objektspecialister, IT-funktioner	Beskrivande roll för funktionen. Bedöms av respektive chef.	Utbildningar har genomförts med vissa nyckelfunktioner. Inköp av digitalt system (digitala körjournaler) och personuppgiftsbehandling har ändå skett utan att nödvändig dokumentation och kontroll har gjorts. Implementering därför inte fullständig.
Samverkan med andra förvaltningar	Avdelningschef deltar i styrgruppsmöte med stadsdelsnämnderna i västerort. ISAM deltar på möten och får information från stadens informationssäkerhetsavdelning.	Genomförts. Utökat samarbete med ISAM i stadsdelsnämnderna i västerort.

Klassning och riskbedömning

Aktivitet	**Status**
Alla system är informationsklassade enligt årshjul	Uppföljning av verksamhetens informationsanvändning pågår under 2022-2023 enligt anvisningarna
Inköp av nya system och utveckling ska vara informationsklassade.	Avvikelse noterad – inköpt system för digitala körjournaler var inte klassade.

Årshjul

Månad och aktivitet	Status
Januari Utvärdering av samtliga rutiner utifrån genomförda riskanalyser och tidigare års incidenter.	Genomförd (fanns även med 2022-års anvisningar)
Februari Uppföljning av digitala inköp Planering av utbildningar för verksamhet Uppföljning av revisionsrapporter och DSO-rapport Fastställande av rutindokument	Genomförd – dock inte uppföljning av digitala inköp som tidigare fanns i verksamhetsplan. Februari månad följdes 2022-års anvisningar.
Mars Fastställande av nyckelpersoner för utbildning	Genomförd
April Uppföljning med dataskyddshandläggare	Dataskyddshandläggare ännu inte utsedda
Övrigt	Ledningens rapport tidigareläggs för att utgöra underlag för verksamhetsplan. GAP-analys (som ska göras i september) finns med i ledningens rapport

Resultat från tidigare revisioner

Dataskyddsombudets årsrapport

Rapporterad brist	Status – ISAM.
Bristande uppdatering och brister i omfattning av registret. Information och implementering av rutin behöver bli bättre.	Fortsatta brister. Systematik skapades för årshjulet men 2-årsperiod sattes för inledande informationssamling. Revidering behövs.
Brister i styrdokument på central nivå (SLK)	Brister åtgärdat på central nivå, dokument för systematik framtagna på förvaltningsnivå.
Information är inte klassad. Rekommendation att öka samarbete inom stadsdelsförvaltningarna i västerort för att klassa information.	Klassningar genomförda på flertalet system, verksamheten har förbättrat sin informationsvärdering. Det har skett ett ökat samarbete inom stadsdelsnämnderna i västerort för att gemensamt klassa information. Vissa system är ännu inte klassade.
Konsekvensbedömningar inte identifierade. Rekommendation att öka kunskap om behovet.	Påbörjat arbete med tröskelanalyser för att identifiera klassningar, dock enbart konsekvensbedömning gjord vid ett tillfälle (Nyckelfri hemtjänst), och en rekommendation om att genomföra konsekvensbedömning där sådan ännu inte är genomförd (öppen kalenderlösning). Utbildningar genomförda med nyckelpersoner.
Personuppgiftsincidenter och begäran om registerutdrag. Inga avvikelser konstaterades.	Viss försening i att besvara registerutdrag och begäran om radering har kunnat ses på grund av personalsituation.
Kunskap om dataskydd har inte nått hela organisationen. De digitala utbildningarna måste nå samtliga medarbetare.	Information och påminnelser om dataskyddsutbildningar har gått ut till hela organisationen. Trots detta kan det finnas brister i att viss personal inte genomfört utbildningen. Genomförande är svår att följa upp på central nivå.

Revisionsrapport från stadsrevisionen

Bedömd brist	Status enligt ISAM
Implementering av dataskyddsförordningen Nämnden bör utveckla sin styrning och uppföljning av arbetet med att efterleva dataskyddsförordningen. Vidare bör nämnden informationsklassa sina informationstillgångar samt regelbundet och systematiskt inventerar sina personuppgiftsbehandlingar. Rekommendationerna bedöms kvarstå.	Åtgärder bedöms kunna vara klara under hösten 2023. Registerförteckningen anpassas efter klassificeringsstrukturen och en systemförteckning/objektförteckning har skapats

Tidigare rekommendationer från ISAM (Ledningens rapport 2023)

Rekommendation	Status
ISAM presenterar nya lokala tillämpningsanvisningar där organisationen definieras. Ledningsgruppen ges en lista på system med förslag på objektägare som sedan beslutas av ledningen.	Genomförd
Rollen dataskyddshandläggare införs	Genomförd
Grundstruktur för registerförteckningen tas fram som överensstämmer med klassificeringsstrukturen	Viss försening men bedöms kunna vara genomförd under året
Vid införande av digitala lösningar tas höjd för det extra arbete införande kräver, och att hela livscykeln beaktas	I stort sett följs denna. Enskilda avvikelser förekommer.
Rekommenderas att ansvariga ägare av processernas information enligt stadsdelens klassificeringsstruktur tillsätts på avdelningschefer i förvaltningens lokala tillämpningsanvisningar.	Genomförd
RSA-arbetet aktivt tar höjd för informationssäkerhetshändelser där ISAM involveras för att få med analyser av omvärldshändelser och incidenter/risker.	Inväntar årets RSA och VOR-arbete
Införa dataskyddsutbildning och informationssäkerhetsutbildning som återkommande del i årshjul för enheterna med återrapporteringsskyldighet för chefer	Staden har tagit fram ny utbildning. Ny rutin behövs. Är ännu inte med i VP för samtliga enheter. Rekommendationen kvarstår för nästa VOR- för att få ner på varje enhet.

om att samtliga medarbetare genomgått utbildning.	
Införa dataskyddsutbildning och informationssäkerhetsutbildning som standardaktivitet vid nyanställning och vid vikarieanställning/konsultanställning och konsultanställning.	Genomfört i checklistan för nyanställda
Införa rutin om kontroll av genomgången dataskydd och informationssäkerhetsutbildning genomgåtts vid behörighetstilldelning i viktigare system.	Hanteras inom varje objekt. Har ännu inte implementerats på hela förvaltning – kontrollen tar tid och skulle i sådana fall behöva förenklas.
Införa obligatorisk utbildning av informationssäkerhet för chefer.	Inte kunnat kontrolleras då staden bytt utbildning, och kontroll inte genomförts. Rekommendationen kvarstår och bör skrivas in i tillämpningsanvisningarna.
Förbereda rutiner för att snabbt kunna hantera information enligt säkerhetsskyddslagen om sådan identifieras eller nya uppdrag ges av kommunfullmäktige.	Rekommendationen kvarstår.
Ett integrerat arbetssätt med avvikelser och incidenter.	Rekommendationen kvarstår. I arbetet med stadens genomlysning av incidenthanteringssystem är det viktigt att rekommendationerna även skickas till ansvariga centralt.

Status gällande förebyggande åtgärder

ISAM-gruppen har kontinuerligt värderat risker och incidenter som skett under året och vidtagit åtgärder, såsom upplysningar om risker vid bluffmail. Konsekvenser av incidenter har också visat sig kunna minimerats på grund av tidigare genomförda riskanalyser.
Riskerna har identifierats och lagts in i arbetet för VOR och internkontrollplan, status och åtgärder presenteras i ILS-systemet.
För enskilda objekt ska uppföljningar ska göras när nya riskanalyser ska tas fram. Bedöms behövas under hösten, främst för NIS-system. Då ny organisation med objektledare enligt PM3 innebär ökat ansvar på objektledare för att ta fram dessa.

Systemförteckning har 72 poster för identifierade IT-tjänster som förvaltningen använder sig av. Av dessa anses 23 poster röra eget upphandlade/avropade system. Dessa anses ha högre informationssäkerhetsrisker då inga normerande klassningar gjorts och då nämnden på egen hand måste ta fram säkerhetskrav. Av dessa har förklassning gjorts för 13 av systemen och ytterligare tre är planerade med datum. Handlingsplaner är upprättade på 11 av systemen och

bedömts inte behövas på tre av systemen. Riskanalyser är gjord på fem system notering om att riskanalys inte behövs på tre system.
Dokumentation och analyser har även gjorts på centrala system, då staden i sina nuvarande anvisningar uppdrar åt varje förvaltning att göra självständiga analyser. Främst har detta gällt arbete med införande av nya system för säkra meddelanden och för videokonferanser.
Staden menar att förvaltningarna själva ansvarar för att kontrollera och göra klassificeringar och analyser av alla system (informationssystemsobjekt). Det bedöms i nuläget svårt att förvaltningen har personalresurser att kunna genomföra detta.

Informationssäkerhetsincidenter

En uppföljning av incidenter sker i bilaga 1.

Inkomna reaktioner från kunder och intressenter (inklusive klagomål)

Två klagomål rörande personuppgiftsbehandling har kommit in under perioden november till juni.
Ena klagomålet rör hantering av personuppgifter inom socialtjänst från en enskild och att uppgifter ska ha kommit ut. Kontroll har gjorts i socialtjänstens system för loggning, för att kunna se vilka personer som haft tillgång till systemet. Förvaltningen kan inte se att sekretessesbrytandet skett på den här myndigheten.
Ett annat klagomål rör hur socialtjänst tar emot orosanmälningar och hänvisar enskilda och skolor till bland annat epost. Den som lämnar klagomålet hänvisar till att inlämnande via epost inte är säkert på öppet nät och frågar varför staden uppmanar till inlämnande av orosanmälningar så. Något alternativ sågs inte i dagsläget, en ny metod tas fram av staden centralt. Som förvaltning hanterar vi all inkommande information på det sätt det lämnas, och vi kan inte förbjuda andra att hantera personuppgifter på ett osäkert sätt. Alternativa sätt att lämna in uppgifter är via telefon, fax (fax2mail), post eller personligt lämna över informationen.

Resultat av mätningar inklusive process- och miljöprestanda

Indikatorer rörande informationssäkerhet redovisas inom ILS-systemet och kommer inte att redovisas här. Inga övriga mätningar görs för närvarande. Mätningar för att uppnå mål som föreslås under åtgärder

Överrensstämmelse med krav och mål

Verksamhetsplan

Text i VP	Status
Systematiskt informationssäkerhetsarbete Det systematiska informationssäkerhetsarbetet ska stärkas under året, vilket bland annat kommer att innebära intensifierat arbete med att definiera och arbeta in nya lokala tillämpningsanvisningar för förvaltningen. Informationsinventering och informationsklassning av nämndens informationstillgångar ska fortsätta, roller och ansvar ska förtydligas och implementeras inom organisationen i enlighet med stadens riktlinjer och metodstöd. Informationssäkerhetsarbetet ska verka för öppenhet och säkerhet där organisationens brister identifieras, rapporteras och åtgärdas. Arkiv och informationssäkerhet ska tillvarata varandras kunskap och färdiga strukturer ska användas inom båda områdena för att förbättra informationssäkerhetsarbetet och översikten över personuppgiftsbehandlingen. Utbildning av medarbetare ska systematiseras och genomföras repetitivt	Verksamhetsplanens mål bedöms kunna komma uppfyllas, men extra fokus behöver göras på den nya utbildningen som tas fram av staden och kontroll för att utbildningarna ingår som obligatorisk del för nyanställda. Nya lokala tillämpningsanvisningar har antagits, roller har tilldelats och strukturen för förteckningen över hantering av personuppgifter uppdateras och bedöms kunna vara klart under året.

Slutlig redovisning kommer att göras i verksamhetsplan.

Grundläggande krav från staden

Fråga	Status
Förvaltningschef/bolagschef har inrättat en *ändamålsenlig organisation* med tillräckliga resurser för att hantera verksamhetens aktiviteter för informationssäkerhet inklusive dataskydd samt övriga områden.	Förvaltningen har tillsatt en ny organisation, implementering pågår – samtliga ansvarsroller är satta.
Förvaltningschef/Bolagschef har fastställt en *lokal anvisning* som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas i den egna verksamheten.	Lokal anvisning har antagits.

Förvaltningschef/bolagetschef har tillsett att dataskyddsombudet har en *självständig och oberoende ställning* och rapporterar till nämnd/styrelse.	Dataskyddsombudet har en självständig och oberoende ställning med möjlighet att rapportera till nämnd, GDPR-rapporten är årlig rapport som lämnas till nämnd.
Förvaltningschef/bolagschef har tillsett a) att verksamhetens informationsmängder har kartlagts samt b) att de viktigaste informationsmängderna även har klassat och riskbedömts.	Förvaltningens informationsmängder har kartlagts med stadens hanteringsanvisningar och kompletterats med särskild systemförteckning. Egna upphandlade informationsmängder har klassats, men fortsatt arbete behöver göras även med obligatoriska IT-tjänster som staden tillhandahåller. En prioriteringslista har gjorts.
Förvaltningschef/bolagschef har tillsett att verksamheten, utifrån riskprioritering, har följt upp implementeringen av skyddsåtgärder för de viktigaste informationsmängderna. Skyddsåtgärderna berör både den egna verksamheten samt leverantörer/biträden.	Förvaltningschefen har delegerat till chefer att riskbedöma enligt lokala tillämpningsanvisningar. Då staden menar att det ska göras för varje verksamhet finns fortsatt behov på vissa områden. Vissa inköp och sedan tidigare inköp har upptäckts inte gjorts enligt rutin och uppföljning krävs.
Förvaltningschef/bolagschef har säkerställt att registerförteckningen ger en rättvisande bild av verksamhetens personuppgiftsbehandlingar och hålls uppdaterad.	Registerförteckningen kan fortfarande sakna information. Registerförteckningen anpassas till nämndens klassificeringsstruktur för att kunna hålla kontinuitet och ta tillvara processkartläggning som redan är gjord. Beräknas vara klar under året.
Förvaltningschef/bolagschef har informerat sig om att verksamhetens informationssäkerhetsrisker hanteras i en handlingsplan, samt beslutat om vilka av dessa som tas om hand i verksamhetsplanen för nästkommande år.	Informationssäkerhetsrisker dokumenteras för enskilda system, incidentrapportering tas om hand och analyseras av informationssäkerhetgruppen. Viktiga åtgärder har lagts in i verksamhetsplan och i VOR. T.ex. frågan om registerförteckning.

Enligt ISO-standard 27001

Se bilaga 2

Utvärdering av lagefterlevnad

Lagar har identifierats av förvaltningen och ansvariga avdelningschefer har satts för kontroll av lagefterlevnad på förvaltningen.
Följande av dessa är relevanta för informationssäkerhet:

Lag	Information	Status
Tryckfrihetsförordningen (1949:105) med offentlighetsprincipen (som är en del av tryckfrihetsförordningen)	Rätt att uttrycka sig fritt i skrift men skyddar mot förtal och kränkningar av enskilda eller grupper. Offentlighetsprincipen reglerar rätt att ta del av allmänna handlingar som inte omfattas av sekretess utan att behöva berätta vad handlingen ska användas till.	Noteringar i journal kan ha förekommit inom socialtjänst vid utlämnande av allmän handling. Det kan innebära att enskild i onödan fått röjt att de begärt ta del av allmän handling i enskilds akt och att man utan skäl registrerat begäran trots att det inte behövs.
GDPR- EU:s dataskyddsförordning (2016/679) Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning,	Europaparlamentets och rådets förordning (EU) om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter samt lag som kompletterar Europaparlamentets och rådets (EU om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.	Ingår i DSOs rapport. Se för avvikelser. Främst rörande möjlighet till ett säkert system för direktmeddelanden som innehåller känsliga personuppgifter och sekretess. Incident där stadens arbetsmarknadsförvaltning har gett instruktioner om att ta in och förvara material som inte bedöms som tillåtet enligt dataskyddsförordningen har förekommit men har hanterats.

Offentlighets- och sekretesslag (2009:400) med kompletterande offentlighets- och sekretessförordning (2009:641)	Bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar. Bestämmelserna innebär begränsningar i yttrandefriheten enligt regeringsformen, begränsningar i den rätt att ta del av allmänna handlingar som följer av tryckfrihetsförordningen samt, i vissa särskilt angivna fall, även begränsningar i den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Sekretess gäller mot allmänheten, mellan olika myndigheter och mellan olika verksamhetsgrenar inom samma myndighet.	Rutiner och arbetssätt är inarbetade, incidenter rapporteras i IA-systemet. Förvarande och bevarande av information ska innebära viss förutsägbarhet. Sekretessmaterial som inte är ringa och inte omfattas av undantag i sekretessförordningen ska diarieföras. Avvikelser i detta finns inom personalområdet vilket beror på krav från staden där uppgifter som möjliggör lokalisering av det dokument som registreras inte tillåts.
Lag (2001:454) om behandling av personuppgifter inom socialtjänsten med kompletterande förordning (2001:637)	Behandling av personuppgifter inom socialtjänsten, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt ett eller flera särskilda kriterier.	Inga noterade avvikelser.
Patientdatalag (2008:355) med tillhörande förordning (2008:360)	All legitimerad personal och den personal som har särskilt förordnande att utöva visst yrke har skyldighet att föra journalanteckningar för varje patient och vid varje kontakt som gäller vård, både avseende utredning och behandling.	Inga noterade avvikelser.

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)	Syftet med denna lag är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för samhällsviktiga tjänster inom sektor hälso- och sjukvård och digitala tjänster.	Rutiner är upprättade och utbildningar har skett. Nödvändig dokumentation har skett för egna system, men det har inte kunnat göras för centrala system. Dels då material inte lämnas till förvaltningar för att kunna göra en bedömning. Staden centralt planerar att göra en gemensam informationsvärdering och klassning för NIS-systemen och ett projekt pågår.
Brottsdatalag (2018:1177)	Ska skydda personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.	Inga noterade avvikelser.
Säkerhetsskyddslag (2018:585)	Det återupptagna arbetet med civilt försvar innebär att kommuner och regioner får ett ökat behov av att arbeta med säkerhetsskydd dvs att skydda verksamheter och information.	Informationsanalys har sedan tidigare inte visat att information som omfattas av denna lag behandlas på förvaltningen. Ingen information har markerats som hemlig. Det saknas lokala rutiner för att hantera den typen av information.
Arkivlag (1990:782)	Anger de grundläggande bestämmelserna för hur de svenska myndigheterna och andra statliga och kommunala beslutande församlingar ska sköta sina arkiv. Arkiven ska bevaras, hållas ordnade och vårdas så att de tillgodoser: rätten att ta del av allmänna handlingar	Rör främst arkivområdet. Vissa handlingsplaner visar att tidigare upphandlingar inte hanterat dessa frågor. Viss eftersläpning finns inom förtecknande.

Förändrade förhållanden som kan påverka ledningssystemet

I stort sett är läget densamma som föregående års rapport. Omvärldsläget visar på fortsatt arbete med systematiskt informationssäkerhetsarbete. Ökad risk för terrohot och sämre säkerhetsläge gör även sannolikheten för attacker mot informationssystem större. Det är därför fortsatt av vikt att värdera informationen och skapa lämpliga säkerhetsåtgärder för dessa där det behövs. Ökade krav och förändrade riktlinjer från staden innebär ett fortsatt intensifierat arbete med informationssäkerhet på förvaltningsnivå. Det kommer innebära att mer resurser måste läggas på förbättring av informationssäkerhet både på strategisk central nivå och operativ nivå bland medarbetare. Staden uppmanar till ökad digitalisering vilket innebär ytterligare behov av arbete med att säkra de digitala tillgångarna.
Pågående arbete med NIS-direktivet som idag för förvaltningen rör hälso- och sjukvård kan innebära att begreppet vidgas och fler verksamheter kan ingå. Förändrad lagstiftning vad gäller hälso- och sjukvård inom kommunala verksamheter (ny äldreomsorgslag) kan innebära ökat behov för arbete med NIS.
Den lag där kommuner får ökat ansvar för civilt försvar kan innebära behov av att arbeta med information som omfattas av säkerhetslagen. Uppdrag kan ges till nämnden eller information omvärderas vilket kan innebära att informationstillgångar anses omfattas av säkerhetsskyddslagen.

Rekommendation till förbättringar

- För att förbättra hur åtgärder hinner analyseras och hanteras i verksamhetsplanen föreslås att ledningens rapport lämnas senast under septembermånad.
  Hur: Förändring av tillämpningsanvisningarna vid nästa revision
  Vem: Isam tar fram förslag, beslutas av ledningen
  Prioritet: Låg

- Resurser för att hantera varje system kan inte ligga på varje förvaltning, när arbetet med och förvaltandet av systemen finns centralt. Staden centralt borde mer aktivt arbeta med PM3-modellen för gemensamma IT-system.
  Förvaltningarna saknar idag resurser för att kunna bedriva informationssäkerhet för alla centrala objekt enligt det ansvar staden lägger på varje förvaltning. Samtidigt som möjligheten till påverkan är mindre när bestämmandet av utveckling och åtgärder sker centralt. För att effektivisera resurshantering borde staden se över sin PM3-modell avseende den förvaltningsnära objektledningen, och lägga den tydligare på förvaltningsnivå. Det innebär också att förvaltningarna gemensamt bör bli tydligare beställare och arbeta gemensamt med staden för att utveckla systemet. Den verksamhetsnära objektledningen bör då också få tydligare instruktion om att de arbetar på förvaltningarnas och bolagens uppdrag. En sådan verksamhetsnära objektorganisation under PM3-modellen kan skapas gemensamt hos förvaltningarna och bolag. Det innebär att de genomför de resurskrävande riskanalyserna och klassningarna tillsammans med varje berörd förvaltning, och representanter därifrån. Staden har hitintills menat att ansvaret inte kan tas över från annan nämnd. Dock bör det inte finnas ett hinder i kommunallagen att respektive nämnd delegerar ansvar till

enskild tjänsteperson på annan förvaltning. Kommunallagen kräver inte att delegerad tjänsteman arbetar på förvaltning direkt knuten till nämnden. Det bör därför inte heller vara något hinder att ge annan tjänsteperson att utföra analyser och uppgifter åt förvaltningarna. För arkivering av handlingarna på respektive förvaltning bör den Verksamhetsnära objektförvaltningen ansvara för att dessa registreras/förvaras korrekt på varje berörd förvaltning och ge information som är nödvändig åt respektive förvaltningens systemförteckning. Staden bör kunna bidra med resurser för att göra denna form av organisation möjlig. Klassning av samtliga objekt som staden uppdrar åt förvaltningarna att använda sig av kommer inte att uppfyllas om inte denna förändring görs. För kommunen som helhet skulle detta innebära maximal nytta för informationssäkerhet, med tillgängliga resurser och besparingar för att kunna uppnå de krav staden ställer enligt sina regler.
Hur: Förvaltningsledning tar aktiv ställning i frågan och hanterar den tillsammans med övriga förvaltningar och bolag gentemot stadens ledning.
Vem: Förvaltningsledning och ISAM
Prioritet: Hög

- Förvaltningen ser över kompetensbehovet för informationssäkerhet. Kompetenskrav/behovsanalys ska ses som grund och hjälp vid rekryteringar och vidareutbildningar och inte som ett absolut kravdokument.
  Hur: Förslag tas fram av ISAM och presenteras sedan för informationssäkerhetsgrupp och antas av ledningen.
  Vem: ISAM, Infosäkgrupp och förvaltningsledning.
  Prioritet: Låg

- En lista på intressenter tas fram (se GAP-analys)
  Hur: Förslag tas fram genom workshops under 2024 och ingår i VP
  Vem: Som uppdrag i VP
  Prioritet: Låg

- Utbildningar i riskhantering ges på en högre nivå. Grundläggande kunskap har nåtts i organisationen att använda IA som verktyg för att rapportera brister. En utbildning som kan verka inspirerande och förbättra kvalitén skulle förbättra IA-arbetet och det systematiska kvalitétsarbetet.
  Hur: Kvalitetsförbättrande utbildning för chefer
  Vem: Som aktivitet i VP och budgeterat.
  Prioritet: Medel

- Revidering av delegationsbeslut för inköp av digitala stödsystem flyttas från som lägst biträdande enhetschef, till avdelningschef. Det inkluderar beställningar av ramavtal. Detta för att förhindra nya incidenter rörande inköp, tydliggöra processägarrollen och minska risk för kunskapsbrist vid inköp.
  Hur: Förändring av delegationsordning
  Prioritet: Låg

- Kunskapsnivåer för objektledare och dataskyddshandläggare behöver stärkas under året och ingå i verksamhetsplan 2024
  Hur: Som uppdrag i VP
  Vem: Som aktivitet i VP
  Prioritet: Medel

- Enkel lathund för riskbedömning inom IA-systemet tas fram med mallar för när utredningar måste påbörjats, eller när/hur utredningar inte behöver inledas alls då risken/konsekvenserna är för små.
  Hur: Som uppdrag i VP
  Vem: Bör göras gemensamt för de som är stödfunktioner för säkerhetsfrågor och andra frågor som berörs av IA.
  Prioritet: Medel

- Ett nytt riskanalysverktyg håller på att tas fram av staden centralt. Förvaltningen bör aktivt engagera sig i det framtagandet och rikta uppmärksamhet på de brister man sett i nuvarande.
  Hur: ISAM skickar en lista på uppmärksammade brister till informationssäkerhetsavdelningen i staden. (se bilaga 1 Sammanfattning av informationssäkerhetsincidenter 2023 Januari till Juli 2023)
  Vem: ISAM
  Prioritet: Hög

- Upprättas enkel rutin för vid behov snabbt kunna hantera säkerhetsklassad material om det skulle uppstå. Vem som hanterar materialet, var det förvaras och hur det diariförs
  Hur: Enklare rutin
  Vem: Säkerhetssamordnare
  Prioritet: Låg

Bilagor

1. Sammanfattning av informationssäkerhetsincidenter 2023 Januari till Juli
2. GAP-analys enligt ISO 27001

Förkortningar

ISAM – Informationssäkerhetssamordnare
DSO – Dataskyddsombud
NIS - Rective on security of network and information systems - the NIS Directive.
VOR – Väsentlighets och riskanalys
RSA – Risk och sårbarhetsanalys

SLK – Stadsledningskontoret

Revisionshistorik

Detta dokument sammanställdes av Informationssäkerhetssamordnaren Dani Cohen 2023-08-25.
Det är den andra ledningens genomgång sedan rapporterna började ta fram 2022.