Ledningens genomgång 2024

Förskolenämnden

Beslutad 2025-08-26

Ledningens genomgång 2024

Dnr: 2025/189

Kontaktperson: Mårten Nilsson Nyberg, Sanna Bjälevik-Chronan

1. Sammanfattning

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 förvaltningschefen inhämta en rapport, så kallad ”Ledningens genomgång” från Informationssäkerhetssamordnare (ISAM).

Denna rapportering ska ge information och underlag till förvaltningschefen att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltningschefen ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.

I rapporten lyfts vikten av att på ett mer systematiskt sätt arbeta med informationssäkerhet kopplat till väsentlighets- och riskanalys (VoR).

Särskilt prioriterade områden som föreslås under 2025 är hantering och uppföljning av behörigheter samt vikten av att nämndens information kartläggs och klassificeras. Även riskhantering och informationssäkerhet i upphandlingar lyfts som särskilt prioriterat under året.

Rapporten redovisar även olika faktorer som påverkar eller kan komma att påverka verksamhetens ledningssystem för informationssäkerhet (LIS) under året, exempelvis NIS2-direktivet och AI.

Innehållsförteckning

1.2 Vad är Ledningens genomgång

Stockholms stads arbete med informationssäkerhet utgår från en 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 genom riktlinjer för informationssäkerhet samt tillämpningsanvisningar, som är en bilaga till stadens kvalitetsprogram. Tillämpningsanvisningarna reglerar ansvar och roller för Stockholms stads systematiska informationssäkerhetsarbete.

För förskolenämndens räkning har förvaltningschefen fastställt en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom förskolenämnden.

1.3 Faktorer som påverkar verksamhetens LIS

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

Det riskbaserade förhållningssättet har sin grund i både interna samt externa hot vilket innebär att nämnden bland annat behöver hålla sig informerad med vad som händer i vår omvärld – likväl som att hålla sig uppdaterad med vad som händer internt inom staden.

1.3.1 Omvärldsbevakning – hot, trender och ny lagstiftning

1.3.1.1 NIS2-direktivet (cybersäkerhetslagstiftningen)

I slutet av 2022 beslutade EU om ett nytt direktiv som ska ersätta nuvarande NIS-direktivet. Det nya direktivet har fått namnet NIS2.

I Sverige kommer NIS2-direktivet att införas genom en ny lag, cybersäkerhetslagen, som först väntades träda i kraft sommaren 2025 men är justerad till 15 januari 2026. Under hösten 2025 pågår arbete med att behandla lagförslaget hos regeringen.

Syftet med NIS2-direktivet är att öka motståndskraften mot cybersäkerhetsrisker genom att ställa krav på en hög gemensam cybersäkerhetsnivå för nätverks- och informationssystem inom hela EU. Det handlar om att verksamheter som ansvarar för viktiga samhällsfunktioner ska ha ett systematiskt informationssäkerhetsarbete som leder fram till att lämpliga riskhanteringsåtgärder vidtas.

När Cybersäkerhetslagen trätt i kraft väntas arbete för utsedda myndigheter att ta fram föreskrifter. Det är därmed idag inte klarlagt vilket inverkan lagen kommer att ha inom förskolenämndens område och uppdrag. Det finns dock starka indikationer att förvaltningens verksamhet i sin helhet kommer att omfattas av lagstiftningen.

1.3.1.2 Oroligt omvärldsläge och krig i Europa

Omvärldsläget är oroligt, inte minst med tanke på Rysslands invasion av Ukraina samt Sveriges inträde i NATO. Detta är faktorer som påverkar hotbilden mot Sverige och svenska intressen. Dessa typer av hot syftar bland annat till att underminera förtroendet för det svenska samhället. Något som i allra högsta grad även omfattar offentlig verksamhet.

Givet detta är det viktigt att förvaltningen har en väl etablerad omvärldsbevakning och håller sig uppdaterad med de hot som direkt eller indirekt kan komma att påverka nämnden.

1.3.1.3 Ökade cyberattacker mot kommuner

Under 2023 ökade antalet försök till cyberangrepp kraftigt mot statliga myndigheter och leverantörer av samhällsviktiga tjänster. Förutom att andelen cyberangreppsförsök ökat visar även statistiken på att närmare hälften av alla IT-incidenter har sitt ursprung hos leverantörer.

MSB har i tidigare rapporter påvisat att störningar i digitala leveranskedjor är de incidenter som riskerar att få störst samhällskonsekvenser eftersom en mängd organisationer och dess tjänster kan påverkas samtidigt. I början på året 2024 utgjorde Tieto Evry-incidenten ett väldokumenterat typexempel på just denna problematik.

1.3.1.4 AI

Utvecklingen av artificiell intelligens (AI) går fort och det finns en stor efterfrågan på att använda ny teknik. Med det så finns det också stora risker med användandet av AI som exempelvis personlig integritet och hantering av stora mängder data. Det kommer ställa höga krav på arbetet med informationssäkerhet och dataskydd.

1.3.1.5 Adekvansbeslut om tredjelandsöverföring

I juli 2023 fattade EU-kommissionen ett nytt adekvansbeslut om tredjelandsöverföring till USA.

EU-kommissionens beslut innebär att överföringar som sker till amerikanska organisationer och företag som omfattas av ”EU-US Data Privacy Framework” nu kan ske utan att lämpliga skyddsåtgärder, såsom standardavtalsklausuler, behöver vidtas enligt artikel 46 i dataskyddsförordningen.

1.3.2 Vad händer inom staden – budget, inriktningar, lokala förändringar eller satsningar

Cybersäkerhetslagstiftningen kommer att påverka förvaltningar och bolags arbete med informationssäkerhet. Särskilt fokus i arbetet kopplat till detta bedöms vara att generellt applicera och fortsätta utveckla ett riskbaserat arbetssätt för informationssystem, incidenthantering, kontinuitetshantering, säkerhet i leveranskedjan, säkerhet vid upphandling eller utveckling samt generellt högre ställda krav på informationssäkerhet och tekniska säkerhetsåtgärder.

1.3.3 Resultatet från egen uppföljning (VoR och IKP) 2024

I väsentlighet- och riskanalysen (VoR) för 2024 fanns nedanstående oönskade händelser inom området informationssäkerhet.

- Medarbetare har behörighet till information som den inte ska ha tillgång till.
- Lokala anvisningen för informationssäkerhet följs inte.
- Anvisningen för hantering av informationssäkerhetsincidenter följs inte.
- Åtgärderna från informationsklassningar efterlevs inte.
- Informationssäkerhetsarbetet är inte inkluderat från start i en upphandling.

I internkontrollplanen (IKP) för 2024 fanns inga kontroller med som rör informationssäkerhet.

Uppföljning av de oönskade händelserna som lyftes i väsentlighet- och riskanalysen för 2024 har följts upp genom stickprover och observationer under året.

Nedan följer den uppföljning och bedömning som gjorts för respektive oönskad händelse i VoR:en. Identifierade risker i rapporten har sin utgångspunkt från granskning 2024.

Medarbetare har behörighet till information som den inte ska ha tillgång till
Genom observationer och stickprovskontroller har det konstaterats att det i vissa system bland annat inte är möjligt att begränsa behörigheter till användare på det sätt som framkommer av kraven från informationsklassningar som gjorts på utbildningsförvaltningen. Stickprover har även visat på brister i uppföljning av behörigheter.

ISAM:s rekommendation till åtgärd
ISAM föreslår att en förvaltningsövergripande rutin tas fram för granskning av användares behörigheter.

Om inte annat framkommer av kraven från klassningen bör respektive verksamhet, minst årligen, granska sina behörigheter. Chef över respektive verksamhet är ansvarig för att behörigheterna hålls uppdaterade och aktuella och att behörighetsstyrningen ligger i linje med kraven som framkommer av klassningen.

Lokala anvisningen för informationssäkerhet följs inte
Genom en översyn av det systematiska informationssäkerhetsarbetet har det identifierats att det finns brister i efterlevnad av den lokala anvisningen för informationssäkerhet. Det innefattar framför allt det ansvar som åligger de roller som pekas ut i anvisningen.

ISAM:s rekommendation till åtgärd
ISAM föreslår att den lokala anvisningen uppdateras i syfte att tydliggöra roller och ansvar för informationssäkerhetsarbetet på förvaltningen. Utöver detta föreslås fortsatt arbete med att implementera anvisningen på förvaltningen.

Anvisningen för hantering av informationssäkerhetsincidenter följs inte
Genom de under året inrapporterade incidenterna bedöms anvisningen för hantering av informationssäkerhetsincidenter inte följas i den utsträckning som förväntas.

ISAM:s rekommendation till åtgärd
ISAM föreslår att anvisningen för hantering av informationssäkerhetsincidenter ses över och uppdateras, inte minst med beaktande av den nya cybersäkerhetslagstiftningen. Utöver detta föreslås fortsatt arbete med att implementera anvisningen i nämndens verksamhet.

Åtgärderna från informationsklassningar efterlevs inte
Nämndens IT-system och tjänster förvaltas främst av utbildningsförvaltningen inom ramen för portföljstyrningen av stadens pedagogiska verksamheter. Dessa IT-system och tjänster har informationsklassats, dock är flera av dessa inte uppdaterade. I nuläget har information som tillhör förskolenämnden inte identifierats därmed är det oklart om all information tillhörande nämnden har informationsklassats.

Informationsklassning är dock enbart första steget i att kunna genomföra tekniska och organisatoriska åtgärder. När informationens skyddsvärda är känd, ska åtgärder vidtas för att skydda informationen.

ISAM:s rekommendation till åtgärd
ISAM föreslår i samsyn med DSO att nämndens information kartläggs och klassificeras utifrån informationsmängd i enlighet med stadens riktlinjer för informationssäkerhet. Ytterligare är att identifiera och tydliggöra gränsdragningar mellan nämndernas verksamheter och utveckla samverkan inom ramen för objektstyrning i relation till informationssäkerhet.

Informationssäkerhetsarbetet är inte inkluderat från start i en upphandling
Genom observationer och aktivt deltagande i arbete med upphandling av nya system har det identifierats att informationssäkerhet inte är tillräckligt inkluderat från start. Detta bedöms vara en stor risk för nämnden då det får till följdeffekt att informationssäkerheten, i ett för sent skede, hanteras inom upphandlingsprocessen samt i projekt. Detta resulterar i att det blir svårt att på ett tillfredsställande sätt uppfylla kraven på informationssäkerhet, både på systemteknisk nivå och kopplat till de aktuella leverantörernas systematiska informationssäkerhetsarbete.

ISAM:s rekommendation till åtgärd
ISAM föreslår att förvaltningen följer samtliga steg och delmoment i stadens metodstöd för informationsklassning.

ISAM rekommenderar även att en lokal rutin, som kompletterar stadens riktlinje för informationssäkerhet med tillhörande tillämpningsanvisningar, tas fram i syfte att tydliggöra och synliggöra vad som behöver omhändertas och beaktas vid upphandling, anskaffning och utveckling av varor och tjänster samt när insatser behöver göras i upphandlingsförfarande och projekt.

1.3.4 Resultatet från revisioner

Inga tredjeparts eller interna revisioner av nämndens arbete med informationssäkerhet har gjorts under året. Nämnden rekommenderas dock arbeta för att säkerställa ett systematiskt och riskbaserat informationssäkerhetsarbete i enlighet med stadens riktlinjer och kommande cybersäkerhetslagstiftning.

1.3.5 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudet (DSO) lämnar årligen in en årsrapport (GDPR-årsrapport) till nämnden i samband med verksamhetsberättelsen. DSO:n har till uppgift att övervaka verksamhetens dataskyddsregelefterlevnad samt att ge råd och rapportera direkt till högsta förvaltningsnivå. Årsrapporten följer upp nämndens efterlevnad inom dataskyddsområdet. Förutom krav som berör informationssäkerhet inkluderas en rapportering av nämndens efterlevnad av exempelvis registrerades rättigheter och konsekvensbedömningar.

Inom informationssäkerhetsområdet och utifrån de avvikelser som DSO identifierat gentemot dataskyddsförordningens krav, ger DSO följande rekommendationer:

- Nämndens information bör kartläggas och klassificeras utifrån informationsmängd i enlighet med stadens riktlinjer för informationssäkerhet för att kunna skydda information (inklusive personuppgifter) med rätt slags skydd.

Utöver rekommendationerna ovan som berör informationssäkerhet har DSO granskat och gett rekommendationer inom andra områden som berör efterlevnaden av dataskyddslagstiftning. Dessa krav och rekommendationer tas inte upp särskilt i denna rapport. I förslagen till förbättringar, i avsnitt 1.5 nedan, tas dock hänsyn till DSO:s samtliga rekommendationer.

1.3.6 Information om avvikelser (incidenter och andra händelser)

Under året har 2 incidenter rapporterats in. Båda incidenterna har även anmälts vidare som anmälningspliktiga personuppgiftsincidenter till Integritetsmyndigheten (IMY).

1.4 Sammanställning av 2025 års VoR

Följande avsnitt redovisar en sammanställning av de oönskade händelser som tagits upp i väsentlighets- och riskanalysen (VoR) för 2025 års arbete.

1.4.1 Sammanställning av oönskade händelser i VoR för 2025

Behörigheter

- Medarbetare har behörighet till information som de inte ska/bör ha tillgång till.

Behörighetshantering

- Anställda, konsulter och leverantörer har åtkomst till information som de inte ska ha tillgång till.

Implementering av lokal anvisning

- Felaktig hantering av personuppgifter samt att nämnden inte följer gällande lagstiftning kring GDPR och informationssäkerhet.

Incidenthantering

- Incidenter rapporteras inte samt att åtgärder från incidenthanteringen inte följs upp eller implementeras.

Informationsklassning

- Åtgärder från informationsklassning följs inte upp eller efterlevs inte.

Informationssäkerhet inom upphandlingsförfarande

- Informationssäkerhetsarbetet inkluderas inte från start i en upphandling.

Informationssäkerhet och dataskydd vid anskaffning eller Utveckling

- Informationssäkerhet inkluderas inte från start vid anskaffning eller utveckling av varor och tjänster

Riskhantering

- Åtgärder från riskanalys tas inte omhand eller efterlevs inte.

Roller och ansvar

- Ansvar för informationssäkerhet och dataskydd efterlevs inte samt att roller är inte utpekade.

Utbildning inom informationssäkerhet och dataskydd

- Anställda och konsulter genomför inte de obligatoriska utbildningarna.

1.5 Förbättringar som föreslås för nämnden

Nedan följer förslag på förbättringsaktiviteter under åren 2025, 2026 och 2027. Förbättringarna baseras på de risker och oönskade händelser som lyfts i verksamhetens väsentlighets- och riskanalys för 2024.

Utöver detta föreslås även aktiviteterna med hänsyn till rekommendationer från GDPR-årsrapport som DSO ansåg vara prioriterade utifrån risker för enskildas fri- och rättigheter.

1.5.1 Aktiviteter under år 2025

Översyn av lokal anvisning för informationssäkerhet
Årlig översyn och vid behov uppdatering görs av den lokala anvisningen. Under 2025 föreslås en uppdatering göras i syfte att tydliggöra roller och ansvar samt fortsatt implementeringsarbete av anvisningen på förvaltningen.

ISAM ansvarar för översyn och uppdatering.

Översyn av anvisning för hantering av informationssäkerhetsincidenter
Under 2025 föreslås en uppdatering av anvisning för hantering av informationsincidenter göras i syfte att tydliggöra processen samt anpassa anvisningen till krav som följer av den nya cybersäkerhetslagstiftningen som väntas träda i kraft under sommaren 2025.

ISAM ansvarar för översyn och uppdatering.

Uppföljning av behörigheter
ISAM föreslår att en förvaltningsövergripande rutin tas fram för granskning av användares behörigheter.

ISAM ansvarar för att aktiviteten genomförs.

Uppföljning av utbildningsinsatser
Årlig översyn och uppföljning av genomförandegrad för de obligatoriska e-utbildningarna inom informationssäkerhet och dataskydd.

ISAM ansvarar för att aktiviteten genomförs.

Inventering och klassificering

Inventering och översyn av it-komponenter, informationsmängder samt tillhörande verksamhetsprocesser. Översyn och uppdatering av befintliga som nya klassningar i enlighet med processen för informationsklassning i staden, vilka också inkluderar en självvärdering, handlingsplan och konsekvensbedömningar avseende dataskydd för verksamheten samt aktiviteter för riskhantering med tillhörande säkerhetsåtgärder.

ISAM ansvarar för att aktiviteten initieras.

Översyn av informationssäkerhet vid anskaffning och utveckling
En översyn av processer och rutiner för informationssäkerhet och dataskydd vid upphandling, anskaffning och utveckling av varor och tjänster föreslås göras under 2025 i syfte att verksamheten på ett tydligare sätt och i rätt tid får med informationssäkerhet på ett fullgott sätt.

ISAM ansvarar för att aktiviteten genomförs.

Övriga prioriterade aktiviteter från GDPR-årsrapport
- Rutiner för att hantera individers rättigheter.
- Säkerställa att konsekvensbedömningar och informationsklassningar genomförts.

Övriga risker som bedömts som låga med tillhörande rekommenderade åtgärder i GDPR-årsrapport föreslår ISAM tillsammans med DSO hanteras under 2026.

ISAM ansvarar för att aktiviteterna initieras med stöd av DSO på förvaltningen.

1.5.2 Aktiviteter under år 2026 samt 2027

Översyn av lokal anvisning för informationssäkerhet
Årlig översyn och vid behov uppdatering görs av den lokala anvisningen.

ISAM ansvarar för översyn och uppdatering.

Översyn av anvisning för hantering av informationssäkerhetsincidenter
Årlig översyn och vid behov uppdatering görs av anvisningen för hantering av informationssäkerhetsincidenter.

ISAM ansvarar för att aktiviteten genomförs.

Uppföljning av utbildningsinsatser
Årlig översyn och uppföljning av genomförandegrad för de obligatoriska e-utbildningarna inom informationssäkerhet och dataskydd.

ISAM ansvarar för att aktiviteten genomförs.

Särskild utbildning för chefer och ledning i enlighet med krav från cybersäkerhetslagstiftningen
Utöver de obligatoriska e-utbildningarna inom informationssäkerhet och dataskydd föreslås det från och med 2026 en gång per år hållas en särskild obligatorisk utbildning för chefer och ledning som ett led av kraven på utbildning i den kommande cybersäkerhetslagstiftningen.

Inventering och klassificering
Inventering och översyn av it-komponenter, informationsmängder samt tillhörande verksamhetsprocesser.

Översyn och uppdatering av befintliga som nya klassningar i enlighet med processen för informationsklassning i staden, vilka också inkluderar en självvärdering och handlingsplan för verksamheten samt riskanalys med tillhörande säkerhetsåtgärder.

Särskilt fokus bör läggas på att inventera och klassificera kritiska verksamhetsprocesser med tillhörande informationsbärare (informationssystem) som ett led i kraven från cybersäkerhetslagstiftningen.

ISAM ansvarar för att aktiviteten initieras och genomförs.

Kontinuitetshantering och katastrofåterhämtning
Framtagande av förvaltningsövergripande kontinuitetsplan för hantering av störning och/eller förlust av kritisk aktivitet eller resurs. Bedöms som särskilt prioriterat, bland annat utifrån kommande lagstiftning inom området. I detta föreslås det även tas fram en komplett lista över prioritetsordning för system och tjänster i syfte att kunna prioritera återställning vid katastrofåterhämtning (disaster recovery).

ISAM ansvarar för att aktiviteten initieras.