Ledningens genomgång 2025

Förskolenämnden

Bilaga till verksamhetsplan 2026

Ledningens genomgång

Dnr: FÖF 2025/371

Kontaktperson: Sanna Bjälevik Chronan

Sammanfattning

Förskolenämnden arbetar med ständiga förbättringar och har utvecklat arbetet med informationssäkerhet genom att fördela ansvar över fler befintliga resurser. Det främjar utvecklingen av det löpande arbetet så att nämndens kärnuppdrag vilar på en rättsäker och robust grund. En väl förankrad bas för informationssäkerhet gör det möjligt att tidigt upptäcka hot, begränsa deras spridning och därmed minska risken för allvarliga konsekvenser. Detta är särskilt viktigt i den tid vi lever i nu relaterat till omvärlden och ökning av cyberangrepp.

Förskolenämnden har förmåga att bygga upp den nödvändiga kompetensen och fortsatt införa strukturerade rutiner som stödjer rättslig efterlevnad. Regelbundna granskningar är en central faktor i detta arbete. Det påbörjade arbetet med att periodiskt utvärdera efterlevnaden av gällande lagstiftning får nämnden möjlighet att identifiera eventuella brister i tid och vidta korrigerande åtgärder innan de leder till incidenter. Genom att fortsatt etablera tydliga rutiner samt säkerställa att alla medarbetare går regelbundet utbildningar i både dataskydd som informationssäkerhet kan nämnden skapa en kultur där säkerhet är en naturlig del av det dagliga arbetet.

Organisatoriskt har nämnden utvecklat arbetet med informationssäkerhet med ett delat ansvar på befintliga resurser. Arbetet omfattar att skapa en hållbar utveckling och agera klokt och med tydliga prioriteringar. En hållbar och stabil utveckling med rätt prioriteringar i det löpande arbetet är målsättningen. En sådant arbetssätt underlättar tidig hotdetektion, minskar sannolikheten för allvarliga incidenter och säkerställer att både fysiska och digitala tillgångar hanteras i enlighet med lag, stadens policys och direktiv. Detta är en nödvändig förutsättning för att möta de ökande cyberhoten i dagens omvärld och för att upprätthålla förtroendet.

Innehållsförteckning

1. Vad är Ledningens genomgång

Ledningens genomgång är ett underlag som tas fram årligen av förskolenämndens Informationssäkerhetssamordnare. Syftet är att informera och uppdatera ledning och beslutande nämnd avseende risker, efterlevnad utifrån lagstiftning och stadens riktlinjer samt ge förslag till prioriteringar för förbättringar.

Underlaget utgår från en standard, ISO 27001 som är en del av ett övergripande ledningssystem med ingående faktorer som att övervaka, granska, underhålla samt förbättra informationssäkerheten.

Ledningens genomgång ska följa med nämndens verksamhetsplan som bilaga i enlighet med stadens rekommendation. Med detta dokument är en målsättning att ledning och beslutande nämnd på strategisk nivå ska erhålla övergripande kunskap om nuläge, ta del av bedömningar och rekommendationer för åtgärder som bidrar till hög kvalité av informationssäkerhet.

1.2 Faktorer som påverkar verksamhetens LIS

Ledningssystem för informationssäkerhet (LIS) är grunden till den process som krävs för att identifiera risker och förslag till förbättringar.

Ett flertal områden granskas, och beaktas till en helhetsbild. Dessa områden berör bland annat informationstillgångar, fysiska som digitala, incidenthantering, kompetens och omvärldsbevakning.

1.2.1 Omvärldsbevakning – ny lagstiftning och direktiv

Under 2025-2026 skärps lagstiftningen på flera fronter som NIS2-direktivet införlivas i svensk lag och utvidgar ansvarsområdet till fler sektorer och med högre krav på riskhantering, incidentrapportering och ansvar.

CER-direktivet (Critical Entities Resilience) träder likväl i kraft och omfattar regelbundna risk- och beredskapsbedömningar för samhällskritiska funktioner.

DORA-förordningen är inte förskolenämnden primär målgrupp men kanske kan komma att påverkas. Den är mer riktad mot finanssektorn och konkretiserar ett IKT-riskramverk med tekniska standarder.

SIS (Svenska institutet för standarder) utvecklar en svensk version av NIST Cybersecurity Framework. Detta är ett verktyg för att möta nationella och EU-krav.

AI-Act är framtaget av EU som i sin form blir helt tillämpbar under 2026. Denna som namnet antyder är riktat mot AI och en indelning av AI-system i fyra risknivåer som i sig skapar en kravlista på lämpliga åtgärder.

CRA (Cyber Resilience Act) som från 2026 kommer att kravställa tillverkare och leverantörer att bygga in kontinuerlig säkerhetsuppdateringar i sina produkter och lösningar.

Gemensamt för dessa innebär förändringar som påverkar offentlig sektor i olika stor omfattning, varav en del kan vara primär likväl som sekundära påverkansfaktorer. Det som framkommer tydligt är behovet av strukturerat arbete, tydliga rutiner, regelbundna granskningar och kompetensutveckling för att både följa lagar och direktiv för ett robust, förtroendefullt digitalt samhälle. För nämndens del omfattar detta till aktivt bevaka stadens information, anvisningar och uppdateringar av policys.

Sammanfattningsvis resulterar de skärpta kraven inom området att nämnden i större utsträckning behöver införliva efterlevnad av både direktiv som lagstiftning utifrån stadens anvisningar. Kraven omfattar hela leverantörskedjan från inför ett inköp och upphandling till införande, drift och förvaltning.

1.2.2 Omvärldsbevakning – hot och trender

Det är att konstatera att världen vi lever i och samhället nationellt som internationellt utsätts dagligen för digitala angrepp i olika former. Den omfattande incidenten som är knuten till angreppet på Miljödata AB är ett tydligt exempel. Det finns en trend av fortsatt ökning av riktade angrepp mot kommunala verksamheter.

Former av angrepp varierar som att stjäla data för att begära lösensumma och om inte så publiceras datan, detta benämns som double-extortion. Det finns även supply-chain attacker vilket betyder att angriparen attackerar tredje part, exempelvis kan

nämnden ha ett avtal kopplat till ett system, leverantören i sin tur kan i delar av sin tjänst använda tredje part för utförande av uppgifter. Detta ställer höga krav innan inköp och upphandlingar att både dataskydd som informationssäkerhet granskas.

Det som även ökar är användning av artificiell intelligens (AI) och syntetisk media som i takt med teknik-utvecklingen blir svårare och svårare att detektera. För kommunal verksamhet kan det förekomma i form av phising-attacker (nätfiske). Detta ställer krav på kontinuerlig kompetensutveckling hos enskilda medarbetare och chefer likväl att lokala anvisningar är implementerade.

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

För budget 2026 framgår det tydligt att det finns en prioritering att öka säkerhet och kunskap genom riktat uppdrag till stadens alla förvaltningar och bolag. Uppdraget belyser att undersöka AI och syntetisk media. Nationellt talar även budget för en förstärkning av arbetet med cybersäkerheten.

Med digitalisering och en ökning av användning av AI behöver nämnden fortsatt utveckla men även stärka arbetet inom informationssäkerhet. Ett ändamålsenligt arbetssätt som främjar hållbar utveckling och resiliens mot angrepp behöver fortsatt utvecklas. Dataskydd och informationssäkerhet är två områden som är en del av nämndens kärnuppdrag vars samverkan är en nyckelfaktor för en robust och trygg grund.

1.2.4 Vad har verksamheten identifierat i RSA-arbetet

Inom förskolenämnden finns behov att fånga in området informationssäkerhet och bygga samverkan med området beredskap. Inom nämndens RSA-arbete betonas krisledningsförmåga, beredskapsövningar samt stärka förskoleverksamhetens motståndskraft. Det saknas stärkt gemensam planering som även inkluderar kritiska tillgångar inom våra digitala tjänster och system. Hot och konsekvenser mot nämndens digitala informationstillgångar bör beaktas som en del av helhetsbilden för beredskap.

1.2.5 Resultatet från egen uppföljning (VoR och IKP)

Sammantaget ses ett identifierat behov att utveckla och implementera en tydlig rutin för behörighetstilldelningar likväl som att gallra och rensa. Vikten ligger på att regelbundet granska och

följa upp varav stickprovskontroller är att rekommendera. Även loggning av hantering kan vid behov vara nödvändigt för att skapa en trygghet i att rätt funktioner och roller har rätt nivåer av behörigheter och minska risk för missbruk.

Därutöver ska belysas inköp och upphandlingar som bör ha föregåtts av ändamålsenlig granskning från funktioner inom både dataskydd som informationssäkerhet. Nämnden har som offentlig aktör ett stort ansvar kopplat till lagen om offentlig upphandling.

Risk för bristande hantering av incidenter likväl kunskap om incidenthantering är ett område som har behov att förtydligas och följas upp för att säkerställa efterlevnad. Som en förlängning av detta finns därmed behov att ta fram en för nämnden aktuell kontinuitetsplan som syftar till att säkerställa drift vid oönskade händelser.

1.2.6 Resultatet från revisioner

Stadsarkivet har utifrån registratur, arkivering och gallring granskat nämnden. Från detta har det identifierats förslag till åtgärder. Dessa åtgärder är åtgärdade och delvis under arbete.

Avseende arbetsmiljö finns det pågående revision med fördjupad undersökning. Denna revision är fortsatt pågående utifrån staden som helhet varav förskolenämnden är en utvald verksamhet.

Baserat på GDPR årsrapport som årligen tas fram av nämndens dataskyddsombud finns ett antal risker identifierade. Ett fortsatt arbete gällande registerförteckningen, behörighetsgranskning, klassningar av både känslighet och klassningar av system och tjänster lyfts fram.

Det finns under året två incidenter anmälda till Integritetsmyndigheten (IMY). Varav den ena var i mindre omfattning och den andra avser angreppet mot Miljödata AB, som då är knutet till ett personalhanteringsverktyg vid namn Stella. Inom den incidenten har förskolenämnden följt stadens särskilda anvisningar för hantering samt under en period tillsatt en särskild arbetsgrupp som genomförde dagliga avstämningar.

1.3 Förbättringar som föreslås för verksamhetens

Nedan är behov av förbättringsaktiviteter under 2026, 2027 och 2028

2026
Implementera årshjul för informationsäkerhet och dataskydd som omfattar följande:

- Införa incidentmöten minst två gånger per år med utvalda funktioner och roller.
- Rutin för behörighetsstyrning- och delning
- Kommunikation internt samt uppföljning av genomförda e-utbildningar i dataskydd och informationssäkerhet.
- Granskning- och stickprovskontroller för efterlevnad
- Stärkt inkludering av informationssäkerhet och dataskydd vid inköp som upphandlingar
- Genomföra klassningar av digitala tjänster och system
- Uppdatera Lokala anvisningar en gång per år
- Ta fram en kontinuitetsplan för nämnden

2027
Omfattar i stort delar som presenteras under 2026 men med mer fokus på att utvärdera åtgärder, revidera där förbättringsbehov identifieras samt uppföljning av följsamhet till rutiner och lagstiftning.

Ett särskilt påpekande är att utveckla åtgärder och rutiner med utgångspunkt från lagar och direktiv i enlighet med stadens anvisningar.

Granskning och revidering av följande:

- incidenthantering
- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning

2028
Åter nämns uppföljning, revidering som prioriterat för att säkerställa en god bas att stå på med fortsatt utveckling i balans till behov. Inventering och omklassningar av digitala tjänster och system är av särskilt intresse. Därutöver är det särskilt prioriterat att granska gallring och rensning av sparat material i gemensamma mappar, funktionsbrevlådor samt medarbetares och chefers egna mejlkorgar.

Granskning och revidering av följande:

- incidenthantering

- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning.