Stockholms stad

Bilaga 6
Ledningens genomgång 2023

FÖF 2023/409

Sammanfattning

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska varje förvaltning ha ett riskbaserat förhållningssätt i informationssäkerhetsarbetet. Det innebär att arbetet baseras på att identifiera, bedöma och följa upp de risker som kan uppstå i verksamhetens informationshantering. Den sammantagna bedömningen för förskoleförvaltningen är att det saknas ett övergripande helhetsgrepp för informationssäkerhetsarbetet på förvaltningen som beror på att förskoleförvaltningen är en ny förvaltning från 1 juli 2023. Organisationen för förskolefrågor ingick tidigare i utbildningsförvaltningen, då som förskoleavdelningen.

Mitt fokus som informationssäkerhetssamordnare har varit att påbörja arbetet med att ta fram de styrdokument som är obligatoriska enligt stadens övergripande riktlinje för informationssäkerhet. Genom att formalisera och tydliggöra många gånger befintliga rutiner samt ansvarsfördelningen kan förvaltningen komma längre i arbetet med det övergripande helhetsgreppet framgent.

Arbetet med följande styrdokument har påbörjats under året;

- Lokal anvisning för informationssäkerhet
- Anvisning för hantering av informationssäkerhetsincidenter (omfattar även personuppgiftsincidenter)

En analys av utvecklingsområden har inte kunnat genomföras i enlighet med stadens ledningssystem ISO 27001:2022.

Innehållsförteckning

1 Bakgrund

Stadens inriktning är att informationssäkerhetsarbetet inom nämnder och styrelser ska utgå från den internationella standarden SS-ISO/IEC 27001/2. Informationssäkerhetsarbetet ska samtidigt alltid utföras med hänsyn tagen till stadens övergripande mål samt till nämnders och styrelsers egna verksamhetsuppdrag. Detta innebär att stadens arbete med informationssäkerhet behöver ske på flera nivåer för att vara heltäckande. Ledningssystemet för informationssäkerhet består därför av flera delar, dels av styrdokument som är stadsövergripande och gäller för samtliga verksamheter, dels av lokalt framtagna styrdokument som enbart gäller för den egna verksamheten.

Den stadsövergripande riktlinjen för informationssäkerhet består av övergripande mål och principer för informationssäkerhetsarbetet och av ett antal fördjupade tillämpningsanvisningar inom särskilda områden. Ansvaret för att inkorporera de stadsövergripande målen och principerna samt fördjupade tillämpningsanvisningarna är, likt ansvaret att skydda information i staden, decentraliserat och följer linjeansvaret. Det innebär att förvaltningschefer har ansvar för att styra och följa upp det lokala arbetet med informationssäkerhet för den egna nämnden så att riktlinjer för informationssäkerhet efterlevs.

Ett sätt för förvaltningschefen att följa upp informationssäkerhetsarbetet är att i enlighet med de stadsövergripande tillämpningsanvisningarna årligen inhämta denna rapport, ”Ledningens genomgång”, från informationssäkerhetssamordnaren. Rapporten innehåller information om det förvaltningsövergripande arbetet med informationssäkerhet på både strategisk och operativ nivå. Rapporten består även av eventuella identifierade utvecklingsområden och uppföljning av dessa i tidigare rapportering. Detta bidrar sammantaget till att ge förvaltningschefen en god bild av informationssäkerheten på förvaltningen.

2 Informationssäkerhetsincidenter

En viktig förutsättning för att lyckas med informationssäkerhetsarbetet är att det finns tydliga och kommunicerade rutiner för incidenthantering av informationssäkerhetsincidenter.

Med informationssäkerhetsincident, vilken även omfattar personuppgiftsincident, avses allmänt en oönskad eller oplanerad händelse som leder till röjande, bortfall eller felaktig ändring av information och/eller personuppgift. Det kan exempelvis vara obehörig åtkomst i ett system, misstänkt röjande av information, information som har förändrats obehörigen eller omfattande virusspridning i en digital tjänst.

Att ha så mycket kunskap som möjligt om de incidenter som inträffar i organisationen utgör en viktig grund för det systematiska arbetet med informationssäkerhet och dataskydd. Jag bedömer att det finns en viss medvetenhet om detta men då förvaltningen saknar en anvisning för informationssäkerhetsincidenter har det inte gått att följa upp. Inga informationssäkerhetsincidenter eller personuppgiftsincidenter har anmälts från det att förskoleförvaltningen tog över förskolefrågorna som utbildningsförvaltningen ansvarat för tidigare.

Sett till att inga incidenter rapporterats finns inget underlag för att dra några slutsatser. Det går inte heller att ta fram någon aggregerad statistik från tidigare år, i syfte att göra jämförelser då förvaltningen etablerades 1 juli 2023.

3 Pågående arbete

Det som beskrivs i detta avsnitt utgör en ögonblicksbild av de större strategiska insatserna som pågår inom informationssäkerhet och dataskydd.

3.1 Informationsklassificiering

En central aktivitet i informationssäkerhetsarbetet är att klassificera nämndens informationstillgångar. Det görs för att kunna bedöma behovet av lämpligt skydd samt säkerställa att varje informationstillgång omges med lämpligt skydd i förhållande till den skada som drabbar den enskilda individen, verksamheten, ekonomi eller samhället vid förlorad informationssäkerhet. Detta ska ske oberoende av om informationen hanteras digitalt eller analogt, i ett it-system eller på ett skrivbord.

Jag som ISAM arbetar för närvarande med att förbättra och tydliggöra informationsklassificeringsprocessen på förvaltningen. Åtgärderna består i stora drag av framtagandet av ett nytt förenklat och renodlat informationsklassificeringsprotokoll som ska kunna användas av samtliga på förvaltningen. Jag arbetar även med att ta fram ett tillhörande metodstöd med stegvisa förklaringar som följer protokollet samt matriser över skadebedömningar. Förbättringsarbetet syftar till att underlätta och harmonisera bedömningarna som görs vid klassningen samt bidra till ett enhetligt och mer kvalitativt informationssäkerhetsarbete i förvaltningen.

Arbetet med detta är särskilt viktigt då informationsklassningen i stora delar sätter grunden för informationssäkerhetsarbetet och ligger till grund för det fortlöpande arbetet med informationssäkerhet i förvaltningen.

3.2 Riskanalys

Förbättringsarbetet som pågår avseende informationsklassificering, påverkar även arbetet med riskanalys och riskhantering då dessa är tätt sammankopplade.

I samband med varje klassning ska det genomföras en riskanalys om inte det med hänsyn till klassningsvärdet eller riskerna är uppenbart obehövligt. Riskanalysen behöver genomföras eftersom de åtgärder som genereras via stadens metodstöd för informationsklassificering är en uppsättning standardåtgärder som

är lika för alla, medan it-tjänster och verksamheter i verkligheten skiljer sig åt.

Förbättringsarbetet gällande riskanalys och riskhantering omfattar framtagande av nya mallar, matriser samt annan vägledande dokumentation. Då riskhanteringsarbetet är en naturlig del av informationsklassningar så syftar även detta arbete till att tydliggöra riskhanteringsprocessen på förvaltningen. Åtgärderna består i stora drag av framtagandet av ett nytt förenklat och renodlat riskhanteringsprotokoll som ska kunna användas av samtliga på förvaltningen. Detta arbete ingår också som en del i det tillhörande metodstöd med stegvisa förklaringar som följer protokollet samt matriser över skadebedömningar som genomförs i arbetet med informationsklassningar.

Förbättringsarbetet syftar till att underlätta och harmonisera bedömningarna som görs vid riskanalyser samt bidra till ett enhetligt och mer kvalitativt informationssäkerhetsarbete på förvaltningen.

3.3 Utbildningsmaterial

I relation till det utvecklingsarbete som löpande pågår och som redovisas i detta och föregående avsnitt, behöver förvaltningen framgent även påbörja utformning av riktade utbildningsinsatser kopplade till de olika områdena. Utöver utbildning i informationssäkerhetsincidenter är det prioriterat att ta fram utbildningsmaterial avseende informationsklassificering samt riskanalys och riskhantering. Utbildningsinsatserna ska i första hand riktas till de nyckelpersoner som arbetar eller kommer att arbeta med informationsklassningar och riskhantering.

3.4 Registerförteckning

I enlighet med dataskyddsförordning (GDPR) behöver förskolenämnden upprätta en registerförteckning vars syfte är att säkerställa förenlighet med dataskyddsförordningen samt för att framgent tillse att förteckningen och aktiviteter kopplade till den omhändertas. Detta är ett arbete som behöver påbörjas snarast men någon vidare fördjupning av detta görs inte i dagsläget.

4 GAP-analys

Jag bedömer att en GAP-analys i enlighet med stadens ledningssystem ISO 27001:2022 behöver göras på förvaltningen. En GAP-analys är ett sätt att analysera och förstå hur en organisations situation i nuläget ser ut i förhållande till önskat framtidsläge samt hur organisationen ska nå dit.

GAP-analysen bör initialt göras på en övergripande nivå i enlighet med uppdelningen av säkerhetsåtgärderna inom kategorierna organisatoriska-, personrelaterade-, fysiska- samt tekniska säkerhetsåtgärder. De fyra kategorierna syftar främst till att tydliggöra ansvarsfördelningen inom organisationen.

Vid analysen av respektive säkerhetsåtgärd föreslås en bristvärderingsskala *(allvarlig – betydande – måttlig – försumbar) samt* prioriteringsskala *(hög – medel – låg)*. Dessa ger sammantaget en indikation på vilken åtgärd som är viktig och hur brådskande arbetet med åtgärden är. I många fall innebär det inte nödvändigtvis ett större arbete med mycket resurser, ibland räcker validering av befintliga rutiner eller framtagande av en ämnesspecifik riktlinje som omfattar flera säkerhetsåtgärder.

Då detta är ett arbete som ligger i framtiden går det inte att göra en bedömning av organisationens mognadsgrad när det kommer till respektive säkerhetsåtgärd. Det finns dock, genom stadsövergripande riktlinjer och annan dokumentation, en grund att stå på för förvaltningen. För utvalda delar av det materialet pågår ett arbete idag på förvaltningen med upprättande av styrdokumenten;

- Lokal anvisning för informationssäkerhet
- Anvisning för hantering av informationssäkerhetsincidenter (omfattar även personuppgiftsincidenter)

Dessa aktiviteter är också sådant som omfattas av specifika säkerhetsåtgärder som följer av stadens ledningssystem för informationssäkerhet.

4.1 Organisatoriska säkerhetsåtgärder

Policy för informationssäkerhet

Förskoleförvaltningen saknar i dagsläget en verksamhetsanpassad informationssäkerhetspolicy och tillhörande ämnesspecifika policyer som beskriver organisationens tillvägagångssätt för att hantera informationssäkerhet. Arbetet med den lokala anvisningen för informationssäkerhet syftar till att peka ut ansvar och mandat kopplat till övergripande aktiviteter. Den omfattar dock inte en generell informationssäkerhetspolicy som bör innehålla uttalanden avseende definitionen av informationssäkerhet samt förvaltningens strategiska informationssäkerhetsmål. Informationssäkerhetspolicyn bör även ta hänsyn till krav som härrör från verksamhetskrav, föreskrifter, lagstiftning och avtal, aktuella och förväntade risker och hot mot informationssäkerheten.

På lägre nivå bör informationssäkerhetspolicyn vid behov stödjas av ämnesspecifika policyer för att ge ytterligare stöd för genomförandet av informationssäkerhetsåtgärder. En första åtgärd är att ta fram ämnesspecifika informationssäkerhetspolicy om de i stadsövergripande tillämpningsanvisningar prioriterade områden. De nedan uppräknade stadsövergripande tillämpningsanvisningarna ger viss vägledning, men behöver ytterligare anpassas till förskoleförvaltningens verksamhet.

- Ansvar och roller inom informationssäkerhet
- Kartläggning och klassning av information
- Identitet och åtkomst
- Anskaffning och utveckling av varor och tjänster
- Drift och förvaltning av it-tjänster
- Incidenthantering och kontinuitetshantering
- Loggning och spårbarhet

Förteckning över information och andra relaterade tillgångar

En förteckning över information och andra relaterade tillgångar, inklusive informationsägare, behöver utarbetas och upprätthållas för att bevara informationssäkerheten. Detta kan med fördel dels göras genom arbetet med framtagande av en registerförteckning enligt dataskyddsförordningen, det är dock något som endast rör personuppgifter. Övrig information som inte utgör personuppgifter, och som i dagsläget finns i diverse informationsklassificeringsprotokoll, behöver sammanställas och finnas tillgänglig på en och samma plats. Exempel på sådan information är kartor.

Informationsklassificering

För att säkerställa förståelse för och identifiering av skyddsbehovet av information, behöver informationen klassas i enlighet med organisationens informationssäkerhetsbehov och baserat på konfidentialitet, riktighet samt tillgänglighet. Detta sker i dagsläget inte och förbättringsarbete pågår (se avsnitt 3.1).

Integritet och skydd av personuppgifter

Förvaltningen behöver arbeta med att identifiera kraven för upprätthållande av personlig integritet och skydd av personuppgifter enligt tillämpliga lagar och andra författningar samt avtalskrav.

4.2 Personrelaterade säkerhetsåtgärder

Medvetenhet och utbildning om informationssäkerhet

Jag ser att uppföljning av genomförande för e-utbildningen om informationssäkerhet och dataskydd behöver göras för förvaltningens medarbetare. Därtill behöver behov av fördjupade utbildningar i särskilt utvalda processer inom informationssäkerhet som till exempel informationsklassificering utredas ytterligare. Detta beskrivs även i avsnitt 3.3.

4.3 Tekniska säkerhetsåtgärder

Användarklienter

För att skydda information som lagras på, behandlas av eller är tillgänglig via förvaltningens datorer, telefoner och surfplattor bedömer jag att förvaltningen behöver ta fram rekommendationer för användningen. I dagsläget saknas en sådan rekommendation eller checklista vilket gör att förvaltningen inte har någon kontroll över eventuell privat användning av stadens användarklienter och eventuella överföringar av personuppgifter samt annan information.

4.4 Sammantagen bedömning

Den sammantagna bedömningen är att förskoleförvaltningen behöver börja med att sätta en grund det görs lämpligen initialt genom det arbete som pågår med den lokala anvisningen för informationssäkerhet. Förvaltningen behöver vidare identifiera bristande eller ej existerande säkerhetsåtgärder i enlighet med stadens ledningssystem för informationssäkerhet. Detta behöver genomföras för att förvaltningen ska kunna bilda en uppfattning om mognadsgrad och prioriteringsområden framgent. Detta redogörs för i avsnitt 5.

5 Plan för arbetet framåt

Planen för arbetet framåt bygger i stora delar på de slutsatser som har dragits utifrån behovet av en GAP-analys och arbetet som pågår. Planen baseras därför på de säkerhetsåtgärder som redovisats i föregående avsnitt och som efter egen uppskattning delats in i följande tre delar.

Del 1: Fortsätta sätta grunden för informationssäkerhet på förskoleförvaltningen genom att

- ta fram en övergripande informationssäkerhetspolicy samt ämnesspecifika riktlinjer utifrån prioriterade områden i de stadsövergripande tillämpningsanvisningarna,
- ta fram en hanteringsanvisning för informationssäkerhetsincidenter.

Del 2: Identifiera nuläge och önskat läge, inventering och slutföra förbättringsarbete genom att

- genomföra en GAP-analys
- inventering av information och informationstillgångar
- påbörja arbete med att sammanställa en förteckning över nämndens information, inkluderat personuppgifter
- slutföra förbättringsarbetet med informationsklassificering
- slutföra förbättringsarbetet med riskhantering

Del 3: Utöver löpande arbete med inventering, klassning och riskhantering fokusera på övriga högt prioriterade säkerhetsåtgärder från resultatet av GAP-analysen i del 2.

Arbetet inom ramen för det som benämns som del 1 är redan initierad och kommer fortsatt att prioriteras under slutet på 2023 samt början på 2024. När säkerhetsåtgärderna i del 1 är genomförda kan åtgärderna i del 2 och därefter del 3 initieras och genomföras. Säkerhetsåtgärderna samt eventuell tidplan kommer att följas upp i nästa rapport om ledningens genomgång som lämnas september-oktober 2024.

Mårten Nilsson Nyberg
Informationssäkerhetssamordnare
Förskoleförvaltningen