Stockholms stad

Ledningens genomgång av informationssäkerhet 2023

UTBF 2023/4473

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 utbildningsförvaltningen är att riskarbetet sker löpande och i många fall är välfungerande i praktiken. Det har däremot saknats ett övergripande helhetsgrepp för informationssäkerhetsarbetet på förvaltningen vilket i vissa fall kan ha orsakat viss otydlighet eller skapat en informell ad hoc-hantering.

Frånvaron av ett övergripande helhetsgrepp ledde till att arbetet med förvaltningsövergripande styrdokument och anvisningar har varit prioriterat under året. Mitt fokus som informationssäkerhets-samordnare har därför varit att ta fram de styrdokument som är obligatoriska enligt stadens övergripande riktlinje för informationssäkerhet samt att åtgärda det som har lyfts som en brist i dataskyddsombudets årsrapport och i revisionsrapporten för 2022. Genom att formalisera och tydliggöra många gånger befintliga rutiner samt ansvarsfördelningen har förvaltningen nu kommit längre i arbetet med det övergripande helhetsgreppet.

Följande styrdokument har tagits fram under året;

- Lokal anvisning för informationssäkerhet
- Anvisning för hantering av informationssäkerhetsincidenter (omfattar även personuppgiftsincidenter)
- Processbeskrivning avseende rätten till tillgång (registerutdrag) enligt dataskyddsförordningen
- Processbeskrivning avseende rätten till rättelse och radering enligt dataskyddsförordningen

Under arbetet med styrdokumenten och anvisningarna har jag identifierat ett antal utvecklingsområden som behöver hanteras. För att identifiera och analysera dessa utvecklingsområden på ett systematiskt sätt har jag tillsammans med andra på förvaltningen sammanställt ett GAP i enlighet med stadens ledningssystem ISO 27001:2022. Detta redogörs för i avsnitt 4.

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 Informationssäkerhets-incidenter

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 genom att skicka en utredning till fel elev och vårdnadshavare, 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. Trots att förvaltningen tidigare under året saknat en anvisning för informationssäkerhetsincidenter har det funnits en viss medvetenhet och fram till 31 augusti 2023 har 11 informationssäkerhetsincidenter anmälts till informationssäkerhetssamordnaren (ISAM).[1] Av dessa informationssäkerhetsincidenter utgör nio personuppgiftsincidenter, varav sju anmälts till Integritetsskyddsmyndigheten (IMY).

Sett till antalet incidenter, utgör dessa inte ett tillräckligt underlag för att dra långtgående slutsatser. Då vi saknar aggregerad statistik från tidigare år, är det heller inte möjligt att göra jämförelser. Det som däremot kan konstateras utifrån samtal med anmälare av incidenter, personuppgiftskoordinatorerna på avdelningarna och på skolorna är att det finns ett mörkertal av incidenter som inte anmäls sett till förvaltningens storlek samt att många incidenter beror på den mänskliga faktorn. Detta stämmer även överens med de slutsatser IMY kommer fram till rapporten ”Anmälda personuppgiftsincidenter 2022”. [2] Detta bedöms kunna avhjälpas till övervägande del genom den nyligen beslutade anvisningen för informationssäkerhetsincidenter samt utbildningar som kommer att genomföras med nyckelpersoner, som till exempel personuppgiftskoordinatorerna. Längre fram kommer enklare stödmaterial riktat till förvaltningens skolor presenteras. För att fånga behovet och säkerställa att det är målgruppsanpassat kommer framtagandet av stödmaterialet ske i nära samarbete med avdelningarnas personuppgiftskoordinatorer.

[1] Antalet omfattar inte de potentiella informationssäkerhetsincidenter som anmäls till servicedesk och som av leverantörens säkerhetsansvarig rapporteras till mig månadsvis.
[2] https://www.imy.se/globalassets/dokument/rapporter/anmalda-personuppgiftsincidenter-2022.pdf.

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.

Det har på olika håll i förvaltningen efterfrågats ett bättre stöd vid informationsklassificering. Processen har upplevts som snårig och skadebedömningarna ibland som skönsmässiga. Därför arbetar jag som ISAM för närvarande med att förbättra och tydliggöra informationsklassificeringsprocessen. Arbetet sker tillsammans med informationssäkerhetshandläggarna på IKT-enheten som är särskilt sakkunniga. Åtgärderna består i stora drag av framtagandet av ett nytt förenklat och renodlat informationsklassificeringsprotokoll som ska kunna användas av samtliga avdelningar på förvaltningen. Vi 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 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 uppdatering av befintliga dokument samt framtagande av nya mallar, matriser samt annan vägledande dokumentation.

3.3 Utbildningsmaterial

I relation till det utvecklingsarbetet som löpande pågår och som redovisas i detta och föregående avsnitt, har förvaltningen påbörjat utformning av riktade utbildningsinsatser kopplade till de olika områdena. Utöver utbildning i informationssäkerhetsincidenter, som det redogörs för i avsnitt 2, 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, som till exempel objektspecialister, projektledare samt upphandlare.

3.4 Registerförteckning

Jag har som informationssäkerhetssamordnare i stor utsträckning varit involverad i utbildningsförvaltningens projekt kring nämndens registerförteckning. Projektets syfte är att utveckla förteckningen för att säkerställa förenlighet med dataskyddsförordningen samt för att fortsatt tillse att förteckningen och aktiviteter kopplade till denna omhändertas framgent. Samarbetet mellan projektet och informationssäkerhetsfunktionen har varit lyckat och gynnsamt sett till de synergier som finns kopplat till förvaltningsövergripande informationssäkerhetsarbete. Arbetet med projektet pågår löpande och projektet beräknas avslutas sommaren 2024.

4 GAP-analys

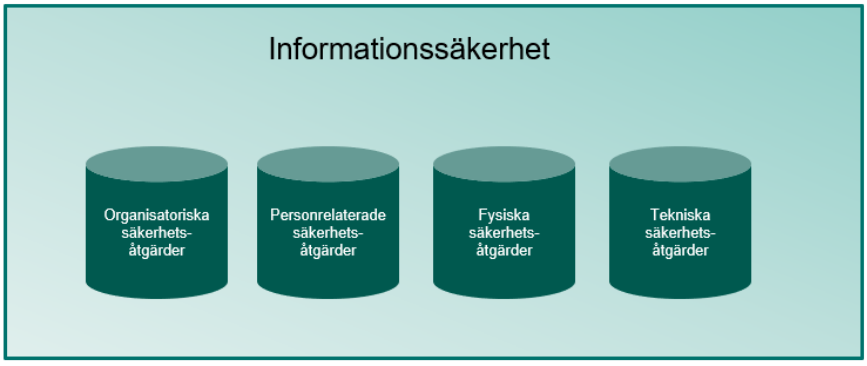
Jag har tillsammans med informationssäkerhetshandläggare på IKT-enheten genomfört en GAP-analys i enlighet med stadens ledningssystem ISO 27001:2022. En GAP-analys är ett sätt att

analysera och förstå hur en organisations situation i nuläget ser ut i förhållande till önskat framtidsläge samt hur organisationen ska nå dit.

GAP-analysen är gjord 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.

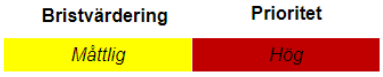
Vid analysen av respektive säkerhetsåtgärd har vi gjort en bristvärdering *(allvarlig – betydande – måttlig – försumbar) samt* prioritering *(hög – medel – låg)*. Dessa ger sammantaget en indikation på vilken åtgärd som är viktig och hur brådskande arbetet med åtgärden är. I många fall innebär det inte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

I denna rapport och i arbetet framåt har vi valt att fokusera på de säkerhetsåtgärder som vi uppskattat till högprioriterade. Genom prioriteringsordningen har vi även tagit fram en plan för arbetet framåt, denna presenteras i avsnitt 5.



4.1 Organisatoriska säkerhetsåtgärder

Policy för informationssäkerhet



Utbildningsförvaltningen saknar i dagsläget en verksamhetsanpassad informationssäkerhetspolicy och tillhörande ämnesspecifika policyer som beskriver organisationens tillvägagångssätt för att hantera informationssäkerhet. Den beslutade lokala anvisningen för informationssäkerhet pekar 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 utbildningsförvaltningens verksamhet (det kursiverade existerar redan).

- *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. För utbildningsförvaltningens del finns en registerförteckning enligt dataskyddsförordningen som hanterar 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 på ett fungerande sätt och förbättringsarbete pågår (se avsnitt 3.1).

Åtkomstkontroll, autentiseringsinformation och åtkomsträttigheter

För att säkerställa behörig åtkomst och förhindra obehörig åtkomst till information, behöver en ämnesspecifik policy tas fram för åtkomsthantering. I dagsläget sker ingen uppföljning eller stickprov av behörigheter, vilket innebär att vi förlitar oss på att chefer och medarbetare ser till att tilldela och avsluta behörigheter för rätt personer i rätt tid under medarbetarens hela anställningsperiod. Detta gäller även anställda som byter tjänst men som är kvar på förvaltningen. Arbetet med detta avser dock inte att ifrågasätta validiteten av tilldelade behörigheter, utan snarare att ha livscykelhantering avseende behörigheter i stort.

Säkerhetsåtgärden har samband med säkerhetsåtgärden ”Priviligierade åtkomsträttigheter och användning av priviligierade åtkomsträttigheter” som beskrivs i avsnitt 4.3 och bör hanteras tillsammans.

Övervakning, granskning och ändringshantering av leverantörstjänster

För att upprätthålla en överenskommen nivå för informationssäkerhet och tjänsteleveranser i enlighet med leverantörsavtalen behöver förvaltningen regelbundet övervaka, granska, utvärdera och hantera ändringar i leverantörers informationssäkerhetspraxis och tjänsteleveranser. Detta sker i dagsläget av it-avtalsansvariga. Det finns dock ett behov att kontrollera ändamålsenligheten i förvaltningens riktlinje för leverantörsstyrning inom it-avtal.

Insamling av bevis

Utbildningsförvaltningen behöver fastställa och införa rutiner för identifiering, insamling, anskaffande och bevarande av bevis som rör informationssäkerhetsincidenter. Även om detta berörs kort i anvisningen för hantering av informationssäkerhetsincidenter, behöver det tas fram en ämnesspecifik policy (även kopplat till loggning, se avsnitt 4.3). En sådan policy syftar till att säkerställa att bevis som rör informationssäkerhetsincidenter hanteras på ett konsekvent och verkningsfullt sätt. Dessa rutiner för hantering av bevis bör generellt sett inkludera instruktioner för identifiering, insamling, anskaffande och bevarande av bevis för olika typer av lagringsmedier, enheter och status för enheter.

Informationssäkerhet vid störning samt kontinuitetsberedskap inom informations- och kommunikationsteknik

Utbildningsförvaltningen saknar en övergripande plan för hur informationssäkerheten och informations- och kommunikationsteknik ska upprätthållas och underhållas på lämplig nivå vid störning med hänsyn tagen till att detta många gånger omfattas av avtal med leverantörer. Förvaltningen behöver dock, oberoende av avtalsrelationer, ha en egen strategisk plan för hur tillgången till förvaltningens information ska säkerställas under störning. Denna kan inkluderas i informationssäkerhetspolicyn som nämns ovan.

Integritet och skydd av personuppgifter

Förvaltningen har identifierat och uppfyller i stora delar kraven för upprätthållande av personlig integritet och skydd av personuppgifter enligt tillämpliga lagar och andra författningar samt avtalskrav. Förvaltningen saknar dock en övergripande policy för skyddade personuppgifter (sekretessmarkering och skyddad folkbokföring). Stora delar av området hanteras på ett välfungerande och ändamålsenligt sätt och på många av förvaltningens avdelningar och skolor finns bra rutiner. Dessa rutiner skulle dock behövas sättas ihop, sammankopplas och formaliseras i en egen ämnesspecifik policy.

Exempelvis finns ett ställningstagande som har stor bäring på informationssäkerhet och dataskydd och som tar sikte på att samtliga elever, även elever med skyddade personuppgifter, ska

inkluderas och finnas med i våra it-komponenter (som t.ex. skolplattformens delsystem, M365 och digitala lärresurser). Detta är av två anledningar, den ena är att det kan röra sig om indirekt röjande när en enskild elev på ett för andra synligt sätt hanteras annorlunda. Ett exempel på detta skulle kunna vara då samtliga elever i en klass i t.ex. Teams syns med för och efternamn förutom en som heter ”Kalle Anka1”. En annan viktig anledning är vi måste lita på att Skatteverket och Polismyndigheten fattat korrekta beslut om skyddsnivå och därmed inte i egna system skapa fingerade uppgifter.

Detta ställningstagande finns inte skriftligt och skulle behöva beslutas om. Vår rekommendation är att vi i övrigt avvaktar med framtagandet av denna ämnesspecifika policy då det pågår arbete på stadsövergripande nivå och då staden tillsammans med andra organisationer inom eSam arbetar med att ta fram stödmaterial.

Efterlevnad av policyer, regler och standarder för informationssäkerhet

Efterlevnaden av förvaltningens befintliga styrdokument inom informationssäkerhet och dataskydd bedöms vara någorlunda hög. Sett till att många av styrdokumenten som uppräknas i sammanfattningen ovan är nyligen fastställda och beslutande, finns det ett visst implementeringsarbete som behöver genomföras på respektive avdelning under personuppgiftskoordinatorernas ledning innan vi på ett systematiskt sätt kan börja följa upp och granska efterlevnaden. Hur uppföljningen och granskningen ska gå till är något som saknas rutiner kring, därför behöver detta utarbetas i den övergripande informationssäkerhetspolicyn.

4.2 Personrelaterade säkerhetsåtgärder

Medvetenhet och utbildning om informationssäkerhet

Många av förvaltningens medarbetare har gått e-utbildningen om informationssäkerhet och dataskydd. E-utbildningen utgör en bra grund, men vi har sett behov av fördjupade utbildningar i särskilt utvalda processer inom informationssäkerhet som till exempel informationsklassificering som behöver tas fram. Detta beskrivs ytterligare 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 behöver förvaltningen 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.

Priviligierade åtkomsträttigheter och användning av priviligierade åtkomsträttigheter

I samtliga it-komponenter och tjänster som förvaltningen tillhandahåller finns priviligierade åtkomsträttigheter. Det rör sig om behörigheter som vid användning kan ha förmåga att kringgå säkerhetsåtgärder och behöver begränsas, följas upp och styras för att säkerställa att rätt personer har rätt behörigheter i rätt tid. Det sker i dagsläget ingen uppföljning eller stickprovskontroll av tilldelningen och användningen vilket gör att det finns risk för att medarbetare som till exempel byter tjänst och därmed inte har behov av den typen av åtkomst fortsatt har den åtkomsten. Arbetet med detta avser inte att ifrågasätta validiteten av tilldelade behörigheter, utan snarare att ha livscykelhantering avseende behörigheter i stort.

Säkerhetsåtgärden har samband med säkerhetsåtgärden ”åtkomstkontroll, autentiseringsinformation och åtkomsträttigheter” som beskrivs i avsnitt 4.1 och bör hanteras tillsammans.

Loggning

Loggar i it-komponenter och tjänster ska registrera aktiviteter, avvikelser, fel och andra relevanta händelser. Då förvaltningen inte har egenutvecklade it-komponenter eller tjänster är förvaltningen i stor utsträckning beroende av leverantörers loggar och förvaltningens ursprungliga, samt många gånger flera år gammal kravställning avseende detta. Vid flertalet informationssäkerhetsincidenter har det uppdagats att loggarna ofta är av dålig kvalitet och inte innehåller den typen av information som hjälper oss att skapa belägg för eventuella intrång. Den dåliga kvaliteten beror på att leverantörerna själva bestämmer vad en loggfil ska innehålla och hur de ska lagras. Ett annat problem är att det saknas verktyg för att läsa, söka och presentera loggarna som gör informationen begriplig. Den dåliga kvaliteten i vissa loggar gör

också att förvaltningen behöver ifrågasätta logginformationens riktighet. Utbildningsförvaltningen behöver därför ta fram en ämnesspecifik policy som avser loggning och som baseras på den stadsövergripande tillämpningsanvisningen. På så sätt finns en vid var tid gällande policy tillgänglig för avtalsansvariga att använda vid incidenthantering, leverantörsstyrning samt vid upphandlingsprojekt.

4.4 Sammantagen bedömning

Den sammantagna bedömningen är att utbildningsförvaltningen i många avseenden ligger i framkant med informationssäkerhetsarbetet, även om arbetet inte alltid är formaliserat i befintliga styrdokument. Behovet av att formalisera och harmonisera de såväl befintliga som icke existerande säkerhetsåtgärder är dock stort. Samtliga ovan uppräknade säkerhetsåtgärder har en hög prioritering, detta innebär dock inte att samtliga säkerhetsåtgärder behöver vidtas samtidigt och på en gång. Vi ser ett behov att på ett systematiskt sätt sätta grunden för informationssäkerhetsarbetet samt vidta de bredare och generella säkerhetsåtgärderna, innan det arbetas vidare med säkerhetsåtgärder inom specifika informationssäkerhetsområden. Detta redogörs för i nästa avsnitt.

5 Plan för arbetet framåt

Planen för arbetet framåt bygger i stora delar på de slutsatser som har dragits utifrån GAP-analysen och har samband med de utvecklingsområden som i övrigt identifierats inom informationssäkerhetsområdet. Planen baseras därför på de säkerhetsåtgärder som redovisats i föregående avsnitt och som vi efter analys delat in i följande tre delar.

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

- ta fram en övergripande informationssäkerhetspolicy samt ämnesspecifika riktlinjer utifrån prioriterade områden i de stadsövergripande tillämpningsanvisningarna,
- sammanställa en förteckning över nämndens information som inte utgör personuppgifter, samt
- slutföra förbättringsarbetet med informationsklassificering.

Del 2: Fokusera på loggning, behörighetshantering och leverantörsstyrning genom att

- ta fram en ämnesspecifik riktlinje för loggning och hur förvaltningen arbetar med insamling av bevis vid informationssäkerhetsincidenter,
- ta fram en ämnesspecifik riktlinje avseende behörighetshantering inklusive privilegierade åtkomsträttigheter samt uppföljningen av dessa, samt
- validera att övervakning, granskning och ändringshantering av leverantörstjänster upptas på ett tillfredsställande sätt i förvaltningens riktlinje för leverantörsstyrning inom it-avtal, samt

Del 3: Fokusera på övriga högt prioriterade säkerhetsåtgärder genom att

- ta fram ämnesspecifik strategi för informationssäkerhet och kontinuitetsberedskap inom informations- och kommunikationsteknik vid informationssäkerhetsstörningar,
- ta fram plan för uppföljning och granskning av informationssäkerhet på förvaltningen, samt
- ta fram en förvaltningsövergripande riktlinje för hantering av skyddade personuppgifter.

Arbetet inom ramen för det som benämns som del 1 är redan initierad och kommer fortsatt att prioriteras under läsåret 23/24. 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.

Noor Mousawi
Informationssäkerhetssamordnare
Utbildningsförvaltningen