

Informationssäkerhet

Ledningens genomgång 2024
Södermalms stadsdelsnämnd
SÖD 2025/66

Innehållsförteckning

1	Inledning	3
1.1	Informationssäkerhet	3
1.2	Informationssäkerhet i Stockholms stad	3
1.3	Internationell standard	3
1.4	Ledningens genomgång	3
2	Södermalms stadsdelsnämnds informationssäkerhetsarbete ..	4
2.1	Informationsklassning	4
2.1.1	År 2024	4
2.1.2	Behov	4
2.1.3	Utmaningar	4
2.1.4	Förslag till åtgärder	5
2.2	Förteckning av it-system och tjänster	5
2.2.1	År 2024	5
2.2.2	Behov	6
2.2.3	Utmaningar	6
2.2.4	Förslag till åtgärder	6
2.3	Lokal anvisning samt rollbesättning och ansvar	6
2.3.1	År 2024	6
2.3.2	Behov	7
2.3.3	Utmaningar	7
2.3.4	Förslag till åtgärder	7
2.4	Utbildning	7
2.4.1	År 2024	7
2.4.2	Behov	8
2.4.3	Utmaningar	8
2.4.4	Förslag till åtgärder	8
2.5	Incidenthantering	8

2.5.1	År 2024.....	8
2.5.2	Behov	9
2.5.3	Utmaningar.....	9
2.5.4	Förslag till åtgärder.....	9
2.6	Informationssäkerhet på upphandlingsområdet	9
2.6.1	År 2024.....	9
2.6.2	Behov	10
2.6.3	Utmaningar.....	10
2.6.4	Förslag till åtgärder.....	10
2.7	Nätverk och samarbeten	10
2.7.1	År 2024.....	10
2.7.2	Behov	11
2.7.3	Utmaningar.....	11
2.7.4	Förslag till åtgärder.....	11
2.8	Övrigt.....	11
4	Treårsplan	11
4.1	Omvärldsbevakning på informationssäkerhetsområdet	11
4.1.1	Ett proaktivt förhållningssätt	11
4.1.2	Nya lagar införs	12
4.1.3	Nya it-lösningar införs och existerande it-lösningar kompletteras eller byts ut.....	12
4.1.4	Antalet potentiella externa partners och leverantörer vid kommande partnerskap samt inköp och upphandling blir färre.12	
4.1.5	Ransomware och cyberattacker ökar.....	13
4.1.6	Otillbörliga påverkanskampanjer mot myndigheter ökar	13
4.2	Prioriteringar under år 2025	14
4.3	Prioriteringar under år 2026	14
4.5	Prioriteringar under år 2027	15

1 Inledning

1.1 Informationssäkerhet

Informationssäkerhet handlar om att säkerställa att information har rätt skydd. Det innebär krav på att informationen finns tillgänglig när den behövs, att informationen är korrekt samt att informationen inte kommer obehöriga till dels. Informationssäkerhetsbegreppet är teknikneutralt vilket innebär att det omfattar all information oavsett om informationen är muntlig, pappersbunden eller digital. För att säkerställa att nivån av informationssäkerhet är tillräcklig krävs att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt.

1.2 Informationssäkerhet i Stockholms stad

Informationssäkerhetsarbetet i Stockholms stad regleras i en central riktlinje med tillhörande tillämpningsanvisningar. Ansvaret för informationssäkerhetsarbetet i Stockholms stad är decentraliserat och följer linjeorganisationen. Nämnderna i Stockholms stad är informationsägare för de egna verksamheterna. Informationsägare ansvarar för att informationen är riktig samt för det sätt som informationen används på. Nämnderna ansvarar således för att det finns ett ändamålsenligt och effektivt informationssäkerhetsarbete inom den egna verksamheten samt att lagkrav och stadsövergripande riktlinjer efterlevs.

1.3 Internationell standard

ISO/IEC 27001:2023 är en internationell standard för ledningssystem på informationssäkerhetsområdet. Stockholms stads informationssäkerhetsarbete utgår från nämnda standard. ISO/IEC 27001:2023 ger organisationer ett ramverk för implementering av ett ledningssystem för informationssäkerhet där säkerhetsnivån tar sin utgångspunkt i en verksamhetsanpassad riskanalys och där informationssäkerhetsarbetet följer en tydlig process. I 9.3 i ISO/IEC 27001:2023 anges bland annat följande.

”Högsta ledningen ska, med planerade intervall, granska organisationens ledningssystem för informationssäkerhet för att säkerställa att systemet är fortsatt lämpligt, tillräckligt och verkningsfullt.”

1.4 Ledningens genomgång

Ledningens genomgång utgör en årsrapport över förvaltningens informationssäkerhetsarbete. Rapporten syftar till att ansvariga för informationssäkerheten inom organisationen informeras om hur arbetet fortgår. Rapporten utgör en del av det underlag som ligger till grund för förvaltningsledningens bedömning om det lokala informationssäkerhetsarbetet anses tillfredställande och adekvat.

2 Södermalms stadsdelsnämnds informationssäkerhetsarbete

2.1 Informationsklassning

2.1.1 År 2024

Arbetet med att informationsklassa förvaltningens informationstillgångar/informationsobjekt/informationsmängder fortgår. I förra årets rapport uppgick det totala antalet informationsklassningar, avslutade och pågående, vid förvaltningen till totalt 74 stycken. Antalet informationsklassningar, avslutade och pågående, har under året ökat med 30 stycken. Det totala antalet informationsklassningar som genomförts vid förvaltningen, avslutade och pågående, uppgår därmed till totalt 44 stycken. Den systematik för informationsklassningsarbetet som arbetats fram de senaste åren har under året förvaltats och vidareutvecklats i samarbete med berörda funktioner inom informationssäkerhet, dataskydd, IT m.fl.

Förvaltningens påbörjade arbete för att intensifiera informationsklassningsarbetet har fortsatt under 2024, bland annat genom att den under 2023 anlita konsultens uppdrag har förlängts fram till och med maj 2025. Konsultens uppdrag omfattar att leda förvaltningens informationsklassningsarbete framåt. Förvaltningen arbetar även med en översyn av tidigare genomförda informationsklassningar med eventuella uppdateringar i de fall behov identifierats. Informationssäkerhetssamordnaren och konsulten samverkar kring utveckling av processer för det framtida klassningsarbetet.

2.1.2 Behov

Arbetet med informationsklassningar behöver fortgå i ökad takt. Resultaten av informationsklassningarna behöver tas om hand, analyseras, förvaltas och åtgärdas. Arbetsprocessen för informationsklassningar behöver vidareutvecklas och alla berörda funktioner inom organisationen behöver delta i utvecklingsarbetet. Det fortsatta införandet av metoden pm3 är ett viktigt led i denna process, likaså översynen av hur förvaltningen framöver kan ha en arbetsprocess som säkerställer att klassningar genomförs i tillräcklig takt och med god kvalitet.

2.1.3 Utmaningar

Förvaltningen har inte informationsklassat samtliga relevanta informationstillgångar/informationsobjekt/informationsmängder. Det är en utmaning att information om att it-system och tjänster behöver informationsklassas inte alltid når

informationssäkerhetssamordnare. Utmaningar vad gäller ansvar och roller inför och under informationsklassningar samt vid efterföljande arbetsprocesser har även identifierats, det gäller dels behörighetshantering samt arbete med kontinuitetsplanering men det finns även en utmaning i fördelning av arbetsuppgifter till relevanta roller, fördelning av dubbla roller till it-samordnare i vissa fall samt utmaningen att få in relevanta svar från de normerande klassningar som ska genomföras för centrala system inom staden. Om tillräckligt underlag från de normerande klassningarna uteblir försvåras förutsättningarna för förvaltningen att dels införa nya system och dels fullfölja klassningsåtagandet.

2.1.4 Förslag till åtgärder

Antalet genomförda informationsklassningar ökar ytterligare under år 2025. Informationsklassningsprocessen vidareutvecklas för att möjliggöra fler genomförda informationsklassningar och underlätta vid omklassningar. Som ett led i det arbetet fortsätter förvaltningen implementeringen av Stockholms stads styr- och samverkansmodell för digitala stöd, pm3. Förvaltningen fortsätter att utse lokala objektledare för alla it-system och tjänster som förvaltningen brukar. Lokal objektledare säkerställer att informationsklassning genomförs och att resultatet av informationsklassningen tas om hand samt att behövliga åtgärder genomförs, exempelvis vad gäller eventuell behörighetshantering samt kontinuitetsplanering. Fokus under 2025 föreslås även vara att stärka objektledarna i deras roller och tydligare definiera dessa roller för att underlätta att rätt åtgärd vidtas av rätt roll i rätt tid.

2.2 Förteckning av it-system och tjänster

2.2.1 År 2024

En inventering av förvaltningens it-system och tjänster påbörjades under år 2022. En förvaltningsövergripande förteckning upprättades i samband med det. Arbetet med att färdigställa förteckningen har fortgått under år 2023 och 2024. I förra årets rapport lyftes bland annat att förteckningen avseende förvaltningens it-system och tjänster som omfattas av NIS-direktivet inte kan anses komplett. Den bedömningen kvarstår. Stockholms stads stadsledningskontor, nedan kallat Stadsledningskontoret, har inlett ett projekt för att stötta stadsdelsnämnderna i informationssäkerhetsarbetet relaterat till NIS-direktivet. Det arbetet kan komma att anpassas till införandet av NIS2. Det har under 2024 identifierats ett behov att även lokalt på förvaltningen arbeta vidare med förteckningen. I sammanhanget kan nämnas att informationssäkerhetsarbetet relaterat till NIS-direktivet kan komma att kompliceras av det nya NIS2-direktivet som trädde i kraft inom EU 18 oktober 2024 och de förändringar det kan medföra. Innan NIS2 kan implementeras i

Sverige väntas lagförslaget om ny cybersäkerhetslag. Propositionen väntas under våren 2025 och riksdagsbehandling väntas hösten 2025.

2.2.2 Behov

Förteckningen över förvaltningens it-system och tjänster behöver uppdateras kontinuerligt i takt med att nya it-system och tjänster införs och att gamla avvecklas. I avvaktan NIS2 behöver förvaltningen se över förteckningen och uppdatera den utifrån kraven i NIS1. Förvaltningen behöver utreda, analysera och klarlägga vilka förändringar NIS2-direktivets införande medför för förvaltningen.

2.2.3 Utmaningar

En förutsättning för arbetet med att hålla förteckningen uppdaterad är att information om införande respektive avveckling av it-system och tjänster når förvaltningens informationssäkerhetssamordnare. Förvaltningen konstaterar att detta informationsflöde behöver utvecklas. Vidare saknas till viss del resurser för att utreda, analysera och klarlägga vilka förändringar NIS2-direktivets införande medför för förvaltningen.

2.2.4 Förslag till åtgärder

Förvaltningen fortsätter implementeringen av Stockholms stads styr- och samverkansmodell för digitala stöd, Pm3. Förvaltningen fortsätter att utse lokala objektledare för alla it-system och tjänster som förvaltningen brukar samt stärker objektledarna i deras roller. Lokal objektledare tillser att information når förvaltningens informationssäkerhetssamordnare vid införande respektive avveckling av it-system och tjänster. Kompetens, tid och resurser avsätts/inhämtas för att utreda, analysera och klarlägga vilka förändringar NIS2-direktivets införande medför för förvaltningen. Förvaltningen bör även samverka inom samt, vid behov, utanför staden för att ytterligare nyansera effekterna av införandet av NIS2.

2.3 Lokal anvisning samt rollbesättning och ansvar

2.3.1 År 2024

En lokal anvisning för informationssäkerhet togs fram år 2022. Den lokala anvisningen revideras årligen. Arbetet med att sprida information om förvaltningens lokala anvisning har genomförts under åren 2022-2024 inom ramen för lokala utbildningar samt genom omnämnande i nyhetsbrev till förvaltningens chefer och medarbetare. Anvisningen beskriver bland annat ansvarsfördelningen och roller på informationssäkerhetsområdet. Arbetet med rollbesättning utifrån den lokala anvisningen och därmed även Stockholms stads styr- och samverkansmodell för

digitala stöd, pm3, påbörjades under år 2022 på informationssäkerhetsområdet. Arbetet har fortsatt under år 2023-2024. Under 2025 kommer arbetet växlas upp och ett projekt för införandet att startas upp.

2.3.2 Behov

Arbetet med att informera om förvaltningens lokala anvisning fortgår, bland annat informeras medarbetare fortsatt om anvisningen vid lokala utbildningstillfällen. Arbetet med rollbesättning utifrån den lokala anvisningen och Stockholms stads styr- och samverkansmodell för digitala stöd, pm3, behöver fortsätta och fler roller behöver besättas. Kunskapen inom förvaltningen kring styr- och samverkansmodellen behöver öka.

2.3.3 Utmaningar

Det är en utmaning för förvaltningen att implementera Stockholms stads styr- och samverkansmodell för digitala stöd, pm3 samt att besätta roller utifrån modellen.

2.3.4 Förslag till åtgärder

Fortsatt information om förvaltningens lokala anvisning vid lokala utbildningstillfällen. Kartläggning av nuvarande arbetsätt, arbetsfördelning och samarbete kring implementeringen av Stockholms stads styr- och samverkansmodell för digitala stöd, pm3 och hur det kan utvecklas. Förvaltningen analyserar hur kunskapen om styr- och samverkansmodellen kan utökas inom förvaltningen. Kartläggning av informationssäkerhetsprocesserna i samband med införandet av förvaltningens nya kvalitetsledningssystem väntas också kunna bidra till utvecklandet av arbetsätten.

2.4 Utbildning

2.4.1 År 2024

Stadsledningskontoret tillhandahåller en digital obligatorisk utbildning i informationssäkerhet. Under år 2023 har utbildningen gjorts om till en certifiering vilket innebär att alla medarbetare vid förvaltningen ska certifiera sig. Certifieringen är giltig ett år och ska därefter göras om. Antalet medarbetare som genomfört utbildningen år 2024 är totalt 881 personer. Det är en marginell sänkning från år 2023 då totalt 900 personer certifierades. Siffran är fortsatt klart högre än de 367 medarbetare som genomförde utbildningen år 2022. Förvaltningen har även följt upp deltagandet tertialvis under år 2024 med ansvariga chefer och fått information om att en viss andel medarbetare fortsatt genomför utbildningen i grupp. Antalet medarbetare som genomfört utbildningen kan således i praktiken vara än högre än vad statistiken visar.

2.4.2 Behov

Arbetet med att öka antalet medarbetare som genomför utbildningen/certifieringen behöver fortgå.

2.4.3 Utmaningar

Alla medarbetare vid förvaltningen har inte möjlighet att genomföra utbildningen så som exempelvis förvaltningens timanställda medarbetare. För medarbetare i vissa verksamheter där kontorsuppgifter inte är lika vanligt förekommande har utmaningar med tid och möjlighet att genomföra den digitala utbildningen identifierats. Vidare är de digitala utbildningarna inte fullt ut målgruppsanpassade, för medarbetare som exempelvis håller på att lära sig det svenska språket har utmaningar med att ta till sig utbildningen identifierats.

2.4.4 Förslag till åtgärder

Information och påminnelser om den obligatoriska utbildningen vid alla lokala utbildningstillfällen vid förvaltningen. Regelbundet erbjuda lokala utbildningar i informationssäkerhet vid förvaltningen ett par gånger per år som komplement.

Informationssäkerhetssamordnare erbjuder vid behov nyanställda medarbetare en kortare specialanpassad introduktion. Föra dialog kring lösningar om hur medarbetare i vissa verksamheter där kontorsarbetsuppgifter inte är lika vanligt förekommande kan genomföra utbildningen. Likaså bör kommande arbete vid stadsledningskontoret om att förbättra rapporteringsmöjligheterna för medarbetare som genomför utbildningen i grupp följas.

2.5 Incidenthantering

2.5.1 År 2024

Antal informationssäkerhetsincidenter som rapporterats in under 2024 i förvaltningens incidenthanteringssystem, IA, uppgår till totalt nio stycken vilket är en rapporterad incident mindre än under föregående år. Personuppgiftsincidenter omfattas inte av statistiken utan redogörs för i separat rapport av förvaltningens dataskyddsombud. Majoriteten av rapporterade incidenter består av borttappad eller stulen utrustning som kan innehålla känslig information, såsom mobil, dator eller padda. Minskningen av antal rapporteringar var inte lika stor 2024 som föregående år. Det låga antalet rapporterade incidenter beror sannolikt på att upptäckandegraden alternativt rapporteringsgraden bland medarbetare är låg.

incidenthanteringsrutin. Rutinen har spridits till aktuella enheter och finns även publicerad på intranätet.

Gällande övriga informationssäkerhetsincidenter har en ny rutin tagits fram vilken avser att underlätta rapporteringen av informationssäkerhetsincidenter för chefer och medarbetare. Rutinen ska under 2025 implementeras på förvaltningen.

2.5.2 Behov

Förvaltningen behöver öka kunskapen internt om betydelsen av incidentrapportering. Arbetssättet med incidentrapporteringssystemet behöver ses över och verksamheterna behöver fortsatt utveckla analyser och slutsatser utifrån statistiken i systemet.

2.5.3 Utmaningar

Förvaltningen behöver säkerställa att incidenter rapporteras efter att en incident har skett. Det nuvarande stadsgemensamma digitala verktyget för incidenthantering (IA) har brister gällande sammanställning av statistik för informationssäkerhetsincidenter.

2.5.4 Förslag till åtgärder

Kontinuerligt påminna chefer och medarbetare i nyhetsbrev om att rapportera informationssäkerhetsincidenter. Påminna om incidentrapportering på utbildningar i ännu högre grad. Implementera den uppdaterade incidenthanteringsrutinen. Genomföra en översyn av arbetsprocessen kring incidentrapporteringen på informationssäkerhetsområdet i samverkan med den arbetsgrupp som tar fram en förvaltningsgemensam process för kvalitetsavvikelsehantering. Översynen bör genomföras i enlighet med eventuella nya krav som framförs i lagförslaget till ny cybersäkerhetslag, implementeringen av NIS2.

2.6 Informationssäkerhet på upphandlingsområdet

2.6.1 År 2024

Informationssäkerhet på upphandlingsområdet sker genom att förvaltningens verksamheter och/eller förvaltningens upphandlare initialt uppmärksammar informationssäkerhetssamordnare på att anskaffning av ett nytt it-system eller tjänst är planerad. Informationssäkerhetssamordnare kan då bistå med stöd vid kravställan ur informationssäkerhetsperspektiv vid upphandlingen.

2.6.2 Behov

En process för arbetet med informationssäkerhet inom upphandlingsförfarandet togs fram under 2024. Processen behöver spridas och implementeras hos berörda funktioner.

2.6.3 Utmaningar

Det är en utmaning att information om att it-system och tjänster behöver informationsklassas inte alltid når informationssäkerhetssamordnare. Ansvar och roller inom arbetsprocessen behöver fortfarande förtydligas, vilket kan förbättras genom implementering av processen.

2.6.4 Förslag till åtgärder

Utökad samarbete mellan informationssäkerhetssamordnare, it-samordnare och upphandlare. Även utökad samverkan mellan it-strateg och utvecklingsenheterna. Berörda parter arbetar tillsammans för att implementera arbetsprocessen. Arbetsprocessen eller del av arbetsprocessen skrivs in i lokala styrdokument/rutiner på upphandlingsområdet så som förvaltningens riktlinjer och rutin för direktupphandling och kopplas till utvecklingen av förvaltningens upphandlingsprocess.

2.7 Nätverk och samarbeten

2.7.1 År 2024

Informationssäkerhetssamordnare ska under 2025 återetablera ett förvaltningsövergripande nätverk omfattande informationssäkerhetssamordnare, dataskyddsombud, it-samordnare, säkerhetssamordnare, verksamhetsutvecklare, arkivarie samt upphandlare. Ett första steg för nätverket bör vara att implementera den processkartläggning på området som genomfördes 2024 och är tänkt att ligga till grund för vidareutveckling och effektivisering av arbetsprocessen på informationssäkerhetsområdet.

Ett nära samarbete mellan förvaltningens informationssäkerhetssamordnare och dataskyddsombud sker löpande vid förvaltningen. Förvaltningens informationssäkerhetssamordnare deltar även vid centrala nätverksträffar i Stockholm stad med representanter från Stadsledningskontoret samt andra förvaltningar och bolag. Förvaltningens informationssäkerhetssamordnare deltar även vid den årliga informationssäkerhetskonferensen som anordnas av Sveriges kommuner och regioner, det s.k. KIS-nätverket.

samhällsskydd och beredskap, MSB, samt deltar vid lämpliga utbildningstillfällen och konferenser som myndigheten erbjuder. Vidare ingår förvaltningens informationssäkerhetsamordnare i kvalitetsnätverket.

Stadsdelsarkivarierna som arbetar för samtliga stadsdelsförvaltningar men är anställda av Södermalm stadsdelsförvaltning för dialog och samverkar med olika fackförvaltningar i staden kring säker hantering av information samt deltar i normerande klassningar i staden när så är lämpligt.

2.7.2 Behov

Förvaltningen är i behov av att fortsätta samarbeta och nätverka såväl internt som med externa parter på informationssäkerhetsområdet, särskilt kring implementering av arbetsprocesserna för informationssäkerhetsamordnare, it-samordnare och upphandlare.

2.7.3 Utmaningar

Det är en utmaning att arbetsprocesser, roller och ansvar på informationssäkerhetsområdet fortfarande inte är tillräckligt tydligt beskrivna eller implementerade i alla delar.

2.7.4 Förslag till åtgärder

Fortsätta samt förbättra nätverksarbetet mellan funktioner som har framträdande roller i informationssäkerhetsarbetet vid förvaltningen. Implementera de framtagna processerna för informationssäkerhet. Fortsätta processkartläggningen på informationssäkerhetsområdet inom ramen för kvalitetsnätverkets arbete med förvaltningens kvalitetsledningssystem samt analysera resultat och vidta lämpliga åtgärder utifrån resultat.

2.8 Övrigt

Under år 2024 har lättlästa informationsbroschyrer om informationssäkerhet och dataskydd reviderats för användning av förvaltningens medarbetare. Syftet med broschyrerna är att nå ut med information till så många medarbetare som möjligt samt att göra informationen så lättillgänglig som möjligt för förvaltningens medarbetare oavsett förkunskaper.

4 Treårsplan

4.1 Omvärldsbevakning på informationssäkerhetsområdet

4.1.1 Ett proaktivt förhållningssätt

Under år 2024 har informationssäkerhetsområdet fortsatt genomgått betydande förändringar på grund av såväl teknologiska framsteg

som förändrade angreppsmönster. Den digitala utvecklingen kräver en kontinuerlig utvärdering av organisationens informationssäkerhet och samarbete med andra organisationer och myndigheter för ökad kunskap. För att hantera kommande utmaningar på området behöver förvaltningen ha ett proaktivt förhållningssätt. Det är genom proaktivt arbete vi kan säkerställa förvaltningens framtida informationssäkerhet.

4.1.2 Nya lagar införs

NIS2 började gälla den 18 oktober 2024 i de EU-länder som var färdiga med sitt nationella förberedelsearbete. I Sverige gäller fortfarande NIS1 eftersom det nationella lagstiftningsarbetet har dragit ut på tiden. Propositionen ”Ett starkare skydd för nätverks- och informationssystem - en ny cybersäkerhetslag” väntas i maj 2025. Riksdagsbehandling av det nya lagförslaget är planerat till hösten 2025. Ny lagstiftning kan därför antas börja gälla hösten 2025 eller under 2026. Nya regelverk innebär att förvaltningen, externa partners och leverantörer behöver anpassa verksamheten. Omställningen kan leda till behov av ökade resurser och kostnader samt ställer krav på ökad kunskap. Förvaltningen kan behöva prioritera regelefterlevnad genom bland annat en kontinuerlig uppdatering av processer och rutiner. Kompetensutveckling genom information och utbildning riktad till förvaltningens medarbetare kan bli aktuellt. Resursfrågor kan uppstå i samband med nya arbetssätt. Ökade kostnader för utbildning, kompetensutveckling samt rekrytering kan uppkomma.

4.1.3 Nya it-lösningar införs och existerande it-lösningar kompletteras eller byts ut

Förändringen av it-lösningar kan påkallas av nya regelverk vilket innebär nya arbetssätt för medarbetare, externa partners och leverantörer att förhålla sig till. I förlängningen kan det innebära förändrade arbetssätt för förvaltningen. Rekrytering av nya medarbetare eller kompetensutveckling av befintliga medarbetare som ska arbeta i aktuella it-lösningar kan bli aktuellt. Nya och kompletterande it-lösningar kräver informationsspridning samt nya arbetssätt med uppdaterade processer och rutiner. Hantering av eventuell påverkan på kommunmedlemmar krävs, så som vid exempelvis identifiering via BankID. Ökade kostnader för utbildning, kompetensutveckling samt rekrytering kan uppstå. Även ökade kostnader för inköp, upphandling och förvaltning av it-tekniska lösningar och tjänster kan uppstå.

4.1.4 Antalet potentiella externa partners och leverantörer vid kommande partnerskap samt inköp och upphandling blir färre

I takt med att nya lagar med krav på högre informationssäkerhet införs ökar förvaltningens kravställen på partners och leverantörer.

Förvaltningen ställer högre informationssäkerhetskrav på externa partners och leverantörer vilket kan leda till färre potentiella partners och anbudsgivare och således även dyrare inköp och upphandlingar. Behov av kompetensutveckling i informationssäkerhet på inköps- och upphandlingsområdet kan uppstå. Likväl kan behov av mer omfattande leverantörsuppföljning och avtalsförvaltning uppstå för att säkerställa att förvaltningen lever upp till ställda informationssäkerhetskrav. Ökade kostnader för utbildning, kompetensutveckling samt eventuell rekrytering kan aktualiseras. Ökade kostnader för leverantörsuppföljning och avtalsförvaltning samt dyrare upphandlingar kan även behöva beaktas.

4.1.5 Ransomware och cyberattacker ökar

En betydande ökning av sofistikerade attacker har de senaste åren observerats riktade specifikt mot den offentliga sektorns infrastrukturer. Attackerna utnyttjar ofta sårbarheter i äldre system vilket understryker behovet av regelbundna systemuppdateringar och ökad cybersäkerhet. En attack kan i värsta fall leda till att förvaltningens verksamheter inte kan utföra sina uppdrag om it-system och tjänster blir otillgängliga. Risk finns för att känsliga uppgifter sprids eller tas som gisslan. En kartläggning av förvaltningens prioriterade processer har genomförts. En analys av processerna och externa beroendekedjor bör genomföras. Kontinuitetsplaner behövs för förvaltningens alla prioriterade verksamhetsområden. Åtgärdsarbetet utifrån fastställda kontinuitetsplaner bör påbörjas. Ökade kostnader för inköp, upphandling och förvaltning av it-tekniska lösningar och tjänster kan uppstå. Ökade kostnader för utbildning, kompetensutveckling samt eventuell rekrytering kan uppstå.

4.1.6 Otillbörliga påverkanskampanjer mot myndigheter ökar

Kampanjerna innebär i regel att felaktig information sprids till allmänheten vilket leder till minskat förtroende för myndigheter och myndigheters verksamheter. Förvaltningens och enskilda medarbetares arbete kan därmed försvåras. Externa partners, leverantörer och medborgare kan påverkas i förlängningen. Löpande bevakning av och närvaro i informationsflöden, exempelvis sociala medier och andra plattformar, bör upprätthållas. En proaktiv åtgärdsplan vid desinformation och otillbörliga påverkanskampanjer med processer och rutiner för att förbereda och informera medarbetare inom förvaltningen bör upprättas. Ökade kostnader för utbildning, kompetensutveckling samt eventuell rekrytering kan uppstå.

4.2 Prioriteringar under år 2025

- Utifrån kartläggningen och analysen av arbetsprocesserna på informationssäkerhetsområdet som genomfördes år 2024 vidareutvecklar förvaltningen arbetsprocesserna, implementerar dem samt vidtar eventuella nödvändiga åtgärder för att säkerställa förvaltningens informationssäkerhet.
- Arbetet med att implementera Stockholms stads styr- och samverkansmodell för digitala stöd, pm3, på informationssäkerhetsområdet fortsätter.
- Intensifieringen av arbetet på informationssäkerhetsområdet som genomfördes under år 2023 och 2024 resulterar i att förvaltningen under år 2025 har informationsklassat samtliga relevanta informationstillgångar/informationsobjekt/informationsmängder där tillräckligt underlag från normerande klassningar finns att tillgå. Förvaltningen har även upprättade arbetssätt och rutiner för att uppdatera och förvalta genomfört arbete.
- Utredda och analysera vilka åtgärder förvaltningen behöver vidta med anledning av NIS2-direktivet.
- Påbörja en insamling av vanligt förekommande frågor på informationssäkerhetsområdet.
- Utforma ett effektivt sätt att delge medarbetare inom förvaltningen svar på vanligt förekommande frågor.
- Genomföra eventuella åtgärder utifrån den översyn av arbetsprocessen kring incidentrapporteringen på informationssäkerhetsområdet som genomfördes år 2024.
- Fortsätta arbetet med översynen av förvaltningens medarbetares kompetenshöjningsbehov på samtliga nivåer inom organisationen på informationssäkerhetsområdet.
- Utifrån den översynen som gjordes år 2024 vidta eventuella åtgärder för att kunna hitta hållbara och långsiktiga arbetssätt för att underlätta samarbete med andra förvaltningar inom Stockholms stad vad gäller informationsklassningar.
- Ta fram lokala rutiner för användning av AI samt för utveckling av AI-tjänster inom förvaltningen.
- Informationssäkerhet är en naturlig del i förvaltningens verksamhetens löpande arbete på samtliga nivåer inom organisationen.

4.3 Prioriteringar under år 2026

- Utifrån kartläggningen och analysen av arbetsprocesserna på informationssäkerhetsområdet som genomfördes år 2024 samt det vidareutvecklingsarbete som genomfördes under år 2025 på området ska roller, arbetsuppgifter och ansvar på informationssäkerhetsområdet vara klarlagda.

- Fortsatt arbete med vidareutveckling och implementering av förvaltningens tillämpning av Stockholms stads styr- och samverkansmodell för digitala stöd, Pm3.
- Klarlägga och genomföra eventuella nödvändiga åtgärder som behöver vidtas med anledning av NIS2-direktivet utifrån den utredning och analys som genomfördes under år 2025.
- Utifrån resultatet av den analys av förvaltningens medarbetares kompetenshöjningsbehov som genomfördes år 2024 och 2025 ska nödvändiga insatser genomföras så att förvaltningens medarbetare har en tillfredställande förståelse och kunskap om informationssäkerhet.
- Informationssäkerhet är en naturlig del i förvaltningens verksamheters löpande arbete på samtliga nivåer inom organisationen.

4.5 Prioriteringar under år 2027

- Effektiva arbetssätt och rutiner ska finnas på plats utifrån det arbete som genomfördes under åren 2024-2026 med att implementera Stockholms stads styr- och samverkansmodell för digitala stöd, pm3.
- Bibehålla och utveckla kompetensförsörjningen inom förvaltningen för att säkerställa att förvaltningens medarbetare har en tillfredställande förståelse och kunskap om informationssäkerhet.
- Informationssäkerhet är en naturlig del i förvaltningens verksamheters löpande arbete på samtliga nivåer inom organisationen.