Stockholms stad

Lokal anvisning för informationssäkerhet

Södermalms stadsdelsförvaltning

Beslutad av: Södermalms stadsdelsnämnd

Beslutad: 2024-02-23

Dokumentansvarig: Informationssäkerhetssamordnare

Diarienummer: SÖD 2022/746

Innehåll

Södermalms stadsdelsförvaltning
Stab- och kansli

12022 Stockholm
elin.arestrom@stockholm.se
start.stockholm

1 Bakgrund

Denna lokala anvisning beskriver roller och organisation för Södermalms stadsdelsnämnds informationssäkerhetsarbete.

Dokumentet fastställdes av stadsdelsdirektör den 22 november 2022. Dokumentet ses över årligen av informationssäkerhetssamordnaren och den senaste uppdaterade versionen fastställdes av stadsdelsdirektör i januari 2024.

Den lokala anvisningen kompletterar stadens centrala riktlinje och tillämpningsanvisningar för informationssäkerhet som är en del av Kvalitetsprogrammet som beslutades av kommunfullmäktige den 21 februari 2022 och visar på hur Södermalm lokalt och praktiskt tillämpar och arbetar med informationssäkerhet. Anvisningen förtydligar hur ansvarsfördelning och roller har anpassats för Södermalms stadsdelsnämnd – vem som ansvarar, vilka stödfunktioner och kontrollfunktioner som finns, och vilka övriga roller som i sitt uppdrag arbetar med skydd av informationstillgångar.

Den lokala anvisningen beskriver också hur nämnden systematiskt arbetar med och följer upp informationssäkerheten. Målgruppen för anvisningen är samtliga medarbetare och chefer vid Södermalms stadsdelsförvaltning.

2 Informationssäkerhet

2.1 Vad är informationssäkerhet?

Informationssäkerhet handlar om de åtgärder som vi vidtar för att all information som vi inom förvaltningen har hanteras på ett säkert sätt så att den skyddas. Detta för att rätt information ska finnas tillgänglig för rätt mottagare vid rätt tidpunkt. Alla medarbetare inom förvaltningen är ansvariga för informationssäkerheten.

Informationen som ska skyddas är all information som vi använder för att utföra vårt arbete och kan till exempel bestå av det vi har i datorer och telefoner i form av mejl och anteckningar, utskrivna underlag samt muntlig information så som samtal. Allt som kan hamna i orätta händer.

Informationssäkerhet handlar därmed om vårt agerande i stort men kan delas in i två större delar. Första delen är teknisk säkerhet, i form av till exempel IT-säkerhet som brandväggar och fysisk säkerhet som till exempel passersystem, lås och dörrar. Den andra delen är administrativ säkerhet som inkluderar regelverk, rutiner inkluderat vårt mänskliga agerande, utbildning samt dataskydd. Praktiska exempel på arbete med informationssäkerhet kan handla om allt ifrån att logga ut från datorn när du lämnar den, inte släppa in okända personer på arbetsplatsen till att göra informationsklassningar vid upphandling av nya system.

Informationssäkerhet, eller med andra ord säker informationshantering, utgår från att all information vi hanterar ska hanteras på ett säkert och rätt sätt utifrån de tre aspekterna konfidentialitet, riktighet och tillgänglighet för att förhindra att information:

- görs tillgänglig för eller i övrigt kommer obehöriga till del (**konfidentialitet**),
- förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning (**riktighet**), och
- inte kan utnyttjas i förväntad utsträckning och inom önskad tid (**tillgänglighet**).

Ibland beaktas även ett fjärde kriterium, spårbarhet, vilket i vårt arbete främst syns genom loggar i system som kan visa vem som till exempel skickat ett mejl eller ändrat i ett ärende senast. Sammanfattat kan det förklaras som ovan, att rätt person ska ha tillgång till rätt information vid rätt tidpunkt. För att möjliggöra detta ska informationssäkerhetsarbetet finnas med inför

upphandlingar, införande av nya system eller arbetssätt men även förändringar av nuvarande.

Mer information om informationssäkerhet finns i den centrala riktlinjen med tillhörande tillämpningsanvisningar och på intranätet. Du hittar informationen genom att klicka på länken nedan eller söka på informationssäkerhet:
Stadsövergripande informationssäkerhet - Stockholms stads intranät

2.2 Vad är dataskydd?

Dataskydd är en del av informationssäkerhetsarbetet som är inriktat på säkerheten för personuppgifter och enskildas integritet. Behandlingen av personuppgifter regleras av dataskyddsförordningen GDPR och den kompletterande nationella dataskyddslagen. Därmed är det, precis som IT-säkerhet en del av informationssäkerhetsarbetet i stort. För att en behandling av personuppgifter ska vara laglig behöver laglig grund finnas och allmänna principer vara uppfyllda.

Mer information om dataskydd och GDPR finns på intranätet:
Dataskydd - Stockholms stads intranät

2.3 Varför informationssäkerhet?

Varför är informationssäkerhet så viktigt? Ett bristande informationssäkerhetsarbete kan leda till konsekvenser, både större som mindre vilket drabbat oss och andra kommuner i olika utsträckning. I ett värsta scenario skulle alla våra system kunna bli krypterade och därmed obrukbara så att vi inte kan utföra vårt uppdrag eller bedriva vår verksamhet. Det skulle i praktiken kunna innebära att vi inte kan nå journaler, publicera nämndärenden eller komma in i Paraply-systemen för att nämna några exempel. Informationssäkerhetsarbetet i staden sker därför systematiskt med utgångspunkt i de övergripande mål staden har samt för Södermalms del stadsdelsnämndens uppdrag.

Det finns även lagstiftning som kräver att vi har en ordnad hantering av vår information bland annat följande lagar:

- Dataskyddsförordningen
- NIS lagen 2018:1174
- Offentlighet- och sekretesslagen 2009:400
- Arkivlagen (1990:782)

Stockholms stad och därmed Södermalms stadsdelsnämnd, följer även den internationella standarden ISO27001/2 som ligger till grund för allt arbete med informationssäkerhet i staden.

2.4 Styrdokument

Staden har en central riktlinje för informationssäkerhet med tillhörande tillämpningsanvisningar som återfinns genom följande länk. I riktlinjen finns mer information om vad informationssäkerhet är.
Stadsövergripande informationssäkerhet - Stockholms stads intranät

På Södermalm finns följande styrdokument:

- Lokal anvisning för informationssäker på Södermalms stadsdelsförvaltning, dnr SÖD 2022/746
- Rutin för utredning och hantering av NIS-incident, SÖD 2022/1006

2.5 Kontakt

På Södermalm finns en funktionsbrevlåda för frågor gällande informationssäkerhet och dataskydd som är följande, använd i första hand funktionsbrevlådan vid kontakt:
Funktion.SD12.Informationssakerhetochdataskydd@stockholm.se

3 Organisation och roller

Det övergripande ansvaret för informationssäkerhet i staden har Kommunstyrelsen genom Kommunfullmäktige samt Stadsledningskontoret som tar fram den stadsgemensamma riktlinjen och tillämpningsanvisningarna.

Södermalms stadsdelsnämnds organisation för informationssäkerhet är indelad i tre nivåer. Den **styrande** omfattar beslutande roller och funktioner i verksamheten. Dessa har på olika nivåer en budget och ett personalansvar, vilket då även innefattar ansvar för informationshanteringen inom den delen av verksamheten.

De **stödjande** och **granskande** funktionerna som är specialistfunktioner som stödjer linjeverksamheten i dess informationssäkerhetsarbete. De granskande funktionerna, utöver stadens egna revisorer, följer även upp att riktlinjer och lagstiftning följs.

Alla som hanterar information har dock ett ansvar att upprätthålla informationssäkerheten i enlighet med de riktlinjer och anvisningar som finns. Arbetet omfattar personvalda, anställda och i viss mån även skolelever och leverantörer såsom konsulter och entreprenörer.

3.1 Ledning (styrande)

3.1.1 Södermalms stadsdelsnämnd

Nämnden är ytterst ansvarig för informationen och formellt informationsägare och personuppgiftsansvarig för förvaltningen.

Nämnden ansvarar därmed för att:

- det finns ett ändamålsenligt och effektivt informationssäkerhetsarbete inom verksamheten samt att stadsövergripande riktlinjer och vägledande dokument för informationssäkerhet följs,
- en ändamålsenlig organisation finns på plats och för att nödvändiga resurser tilldelas samtliga funktioner för att kunna genomföra ett effektivt informationssäkerhetsarbete. Genom denna lokala anvisning beskriver och beslutar nämnden hur denna organisation fungerar i praktiken,
- att utse ett dataskyddsombud (DSO) samt att från dataskyddsombudet årligen inhämta en rapport om dataskyddsarbetet. Nämnden kan även delegera uppgiften

till stadsdelsdirektör som då ska anmäla sitt beslut till nämnden.
- Syftet är att nämnden med hjälp av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker för verksamheten. Ett dataskyddsombud har utsetts genom beslut inom nämnden den 2020-09-29.

Nämnden inhämtar årligen en så kallad GDPR årsrapport från dataskyddsombudet. Syftet är att nämnden med hjälp av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker för verksamheten. Denna rapport har senast inhämtats för år 2023 och godkänts av nämnden i samband med beslut av verksamhetsberättelsen.

I nämndens ansvar ligger även att delegera uppgiften att besluta om informationshantering och regler för detta. Denna uppgift tas omhand i detta dokument, se rubrik 3.1.2 samt 3.1.3.

3.1.2 Stadsdelsdirektör

Södermalms stadsdelsdirektör är nämndens representant (delegat) när det gäller att besluta i de övergripande frågorna och ansvarar för att:

- fastställa de lokala tillämpningsanvisningarna och andra övergripande styrdokument för förvaltningen,
- utse en informationssäkerhetssamordnare och ansvara för att stödfunktioner för informationssäkerhet tilldelas de resurser som krävs,
- verksamheten tilldelas de resurser som behövs för att kunna upprätthålla god informationssäkerhet,
- hålla sig underrättad om informationssäkerheten i Södermalms stadsdelsförvaltning, minst genom att inhämta den årliga rapporten *Ledningens genomgång* från den lokala informationssäkerhetssamordnaren,
- fastställa klassificeringsstrukturen för verksamhetens informationshantering.

3.1.3 Chef

Ansvaret för att skydda informationen som hanteras inom verksamheten följer linjeansvaret. Varje chef har inom sin verksamhet ett särskilt ansvar för att informationen hanteras på ett korrekt sätt enligt gällande lagstiftning och riktlinjer. Ansvaret för informationshanteringen ska ligga så verksamhetsnära som möjligt, och inom förvaltningen innebär det som lägst på enhetschefsnivå.

Chefer kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Chefer inom förvaltningen ansvarar för att:

- se till att samtliga medarbetare och konsulter genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd årligen och sprida information om dessa,
- följa upp och utreda de incidenter som verksamheten anmäler i IA, samt att kontakta dataskyddsombud och/eller informationssäkerhetssamordnare vid incidenter som rör personuppgifter eller andra informationssäkerhetsfrågor,
- säkerställa att registervård genomförs inom chefens verksamhet och att uppdatera och följa upp nämndens register över hantering av personuppgifter (d.v.s. registerförteckningen).
- de inköp/upphandlingar som chef beslutar om följer gällande lagar vad gäller informationshantering, samt stadens och nämndens styrdokument,
- informationsinventering är gjord av den egna verksamheten med stöd från informationssäkerhetssamordnare och arkivfunktioner. Att se till att viktigare informationstillgångar är klassade och att verksamhetens it-tillgångar har en utsedd objektledare,
- ta fram lokala rutiner för den egna verksamheten vid behov,
- säkerställa att informationssäkerhetskrav och GDPR-krav (t.ex. tecknande av personuppgiftsbiträdesavtal) uppfylls vid avdelningens upphandlingar genom att kontakta dataskyddsombud/informationssäkerhetssamordnare.

Chefer har även ett ansvar när det gäller behörigheter. Vid avslut av anställning har chef ett ansvar att se till att behörigheter tas bort, detta är särskilt viktigt om personen i fråga ska fortsätta arbeta i Stockholms stad och därmed har tillgång till samma system som tidigare.

3.1.4 Processägare

All informationshantering i förvaltningen har en ansvarig chef. En ansvarig chef har utsetts för respektive process med särskilt uppdrag att se till att rutiner och instruktioner finns på plats för informationshanteringen inom processområdet. Dessa ska även följa

förvaltningens klassificeringsstruktur. Den chef som ansvarar för en specifik process har benämningen processägare. Processägaren beslutar vilka digitala verktyg som får användas i processen och hur information ska hanteras inom processen.

3.1.5 Objektledare

En objektledare ansvarar för drift och förvaltning av en it-tjänst. En objektledare ska utses för samtliga digitala system vid Södermalms stadsdelsförvaltning. Objektledarrollen kan med fördel delas upp i objektledare-verksamhet och objektledare-it och det arbetet pågår inom förvaltningen. Detta så att personer med rätt kompetens hanterar rätt frågor. Tydliggörandet av vad de olika delarna innebär är en del av det arbetet.

Vilka som tilldelats rollen objektledare inom förvaltningen framgår av den förteckning över verksamhetens informationstillgångar som upprättas av informationssäkerhetssamordnaren.

När det gäller de system där drift sköts på entreprenad eller på annan förvaltning, är objektledaren ansvarig för systemet i relation till beställd tjänst och fungerar även som lokal objektledare med ansvar för hur systemet används i verksamheten. I de fall både drift och verksamhet finns inom nämnden förekommer ibland rollen objektledare specifikt för systemets drift.

Objektledarens ansvar är att:

- tillse att informationstillgången är klassad och att handlingsplaner från klassning tas om hand för systemet.
- se till att förvaltningsplan och andra nödvändiga rutiner, finns på plats och följs upp,
- tillse att stadens riktlinjer och tillämpningsanvisningar följs vad gäller informationssäkerhet för it-tjänster,
- besluta om regler för tillgång till systemet och se till att dessa är kända av medarbetarna,
- utse övriga nödvändiga funktioner inom it (t.ex. objektspecialist).

Om det finns en utsedd central objektledare i staden behöver även en lokal objektledare vid Södermalm utses som kan agera kontaktperson/samordnare för systemet samt lokalt ansvara för att informationstillgången är klassad och att handlingsplaner tas om hand hos oss på Södermalm etc.

3.2 Stödjande och uppföljande

3.2.1 Informationssäkerhetssamordnare (ISAM)

Informationssäkerhetssamordnare ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet och att stötta samt vägleda hela förvaltningens verksamhet.

Informationssäkerhetssamordnaren ska arbeta utifrån stadsdelsdirektörens styrning av vilka verksamhetsrisker och åtgärder som ska prioriteras.

Kontaktuppgift:
Funktion.SD12.Informationssakerhetochdataskydd@stockholm.se

Informationssäkerhetssamordnare ansvar är att:

- vara kontaktpunkt för stadens centrala informationssäkerhetsansvariga (CISO) samt rapportera allvarliga incidenter till denna,
- fungera rådgivande gentemot objektledare, i projekt samt till ansvariga för upphandling,
- samverka med andra närbesläktade ansvarsområden och roller,
- stödja linjeverksamheten när det gäller det strategiska arbetet, kartlägga information, informationsklassificera den, hantera incidenter
- utbilda medarbetare och sprida kunskap om lokala rutiner,
- bevaka förändringar i lagstiftningen och händelser i omvärlden,
- genomföra uppföljning/revision av det lokala informationssäkerhetsarbetet.

Det finns även en central funktion för stadsövergripande informationssäkerhet. Funktionens uppdrag och ansvar är att styra, utveckla och följa upp det centrala informationssäkerhetsarbetet i staden.

Kontaktuppgift:
Funktion.slk.informationssakerhetcentralt@stockholm.se.

3.2.2 Dataskyddsombudet (DSO)

Nu tjänstgörande dataskyddsombud utsågs 2020-09-29.

Kontaktuppgift:
Funktion.SD12.Informationssakerhetochdataskydd@stockholm.se

Dataskyddsombudets övergripande och viktigaste uppgift är att kontrollera att dataskyddsförordningen (GDPR) följs av verksamheten. Uppföljningen består bland annat av att utföra kontroller och informationsinsatser.

Dataskyddsombudet ska kunna agera självständigt och oberoende i sitt uppdrag och ska därför inte utföra det operativa arbetet. Dataskyddsombudet bör ha ett nära samarbete och kontakt med informationssäkerhetssamordnare, vilket är nödvändigt för att arbetet ska bedrivas effektivt och leda till största möjliga nytta.

Dataskyddsombudet har dessutom i uppgift att:

- vägleda, informera och ge råd till verksamheten om hur relevanta skyddsåtgärder ska väljas och implementeras för att person- och integritetsskyddet ska upprätthållas.
- ge råd vid personuppgiftsincidenter i enlighet med verksamhetens incidentrutin. Dataskyddsombudet ska alltid involveras i samband med konsekvensbedömningar och övervaka genomförandet av den,
- stötta chef så att informationssäkerhetskrav och GDPR-krav (t.ex. tecknande av personuppgiftsbiträdesavtal) uppfylls vid avdelningens upphandlingar.

3.2.3 Dataskyddsredogörare (inklusive informationssäkerhet)

Dataskyddsredogörare utgör informationssäkerhetssamordnarens och dataskyddsombudets länk till chefer och medarbetare i verksamheterna. Dataskyddsredogörares uppgifter är att:

- vara avdelningens kontaktperson gentemot dataskyddsombud och informationssäkerhetssamordnare
- ansvara för att samordna och sammanställa avdelningens och verksamheternas registerförteckning,
- en gång per år samverka med arkivredogörare för att sammanställa underlag till förteckning över informationstillgångar till informationssäkerhetssamordnare.

3.2.4 Samordnare av arbete med VP, uppföljningar vid T1, T2 och VB samt internkontroll

Verksamhetens samordnare av arbetet med VP, VB, T1, T2 samt väsentlighet- och riskanalysarbetet och internkontrollarbetet samordnar beredningen och uppföljningen av nämndens ILS-arbete. Samordnarna ska aktivt arbeta för att informationssäkerhet är med och följs upp i nämndens väsentlighets- och riskanalys samt införliva informationssäkerheten i verksamhetsplanen med stöd från informationssäkerhetssamordnaren.

3.2.5 Arkivansvarig och arkivarie

Övergripande arkivfunktioner så som stadsdelsarkivarier, arkivansvarig och arkivarie har en viktig funktion i stadens informationssäkerhetsarbete.

Arkivansvarig har ett övergripande samordnings- och resursansvar för förvaltningens informationshantering. I det ingår att uppmärksamma och tillgodose behov inom informationshantering i förvaltningens budgetarbete och övrig planering samt att besluta om arkivinstruktion.

Arkivarie har det strategiska ansvaret för att planera, följa upp och ständigt förbättra förvaltningens informationshantering. I det ingår att samordna och utveckla rutinerna för arkivredogörarnas arbete samt att utbilda och informera arkivredogörare och enhetschefer om hanteringsanvisningarna. Arkivarien bevakar förändringar i organisation och arbetssätt som påverkar informationshantering och informerar Stadsdelsarkivarierna och arkivansvarige vid behov.

För mer information om Södermalms arkivorganisation och roller, se arkivinstruktionen eller kontakta Södermalms lokala arkivarie.

3.2.6 Säkerhetssamordnare

I händelse av kris och då krisstab aktiveras inom förvaltningen så samordnas allt säkerhetsarbete av förvaltningens säkerhetssamordnare. I den samordningen innefattas även informationssäkerhetsarbetet i dialog med informationssäkerhetssamordnare.

3.3 Övriga funktioner

3.3.1 Medarbetare

Medarbetare inom förvaltningen ska följa stadens riktlinjer och regelverk, både centrala och lokala, ta del av den information som finns om informationssäkerhet och genomföra de obligatoriska utbildningarna inom informationssäkerhet och dataskydd. Medarbetare ansvarar även för att skyndsamt rapportera incidenter enligt gällande rutin.

Nyanställda medarbetare godkänner stadens generella användarkontrakt i samband med sin första inloggning i stadens it-miljö, och ska därefter påminnas om kontraktets innehåll enligt en rutin som nämnden beslutar om.

3.3.2 IT-funktioner

Roller med denna expertfunktion deltar aktivt i det operativa arbetet genom att t.ex. delge sin expertkunskap vid upphandlingar, införande av system eller produkter, informationsklassningar och drift och förvaltning. För varje IT-system finns en lokal objektledare-IT. För IT-system som är förvaltningsmensamma och används av flera eller alla avdelningar är IT även lokal objektledare verksamhet.

3.3.3 Särskild systemspecialist/objektspecialist

Inom förvaltningen finns även de som genom administratörsbehörigheter på olika sätt förvaltar IT-objekt i verksamheten. Strukturen/hanteringen för varje IT-objekt sätts för varje enskilt objekt, men det finns alltid minst en kontaktperson. Objektledaren ansvarar för att utse den organisationen.

3.3.4 Övriga roller med ansvar för informationssäkerhetsarbetet i linjen

3.3.4.1 Upphandlare

Upphandlare har ett ansvar att informera informationssäkerhetssamordnare och dataskyddsombud inför nya upphandlingar så att upphandlingskrav kan tas fram och en klassning av den nya processen/informationstillgången kan ske.

3.3.4.2 Kommunikatör

Har ett ansvar för att hjälpa informationssäkerhetssamordnare och dataskyddsombud att sprida information.

3.3.4.3 HR-personal

HR-personal har ett ansvar att säkerställa att informationssäkerhet och därmed även dataskydd beaktas vid hantering av anställdas uppgifter. Detta gäller särskilt eftersom det kan röra sig om känsliga personuppgifter.

4 Nätverk och grupper

4.1.1 Allmänt om nätverk och grupper

Inom staden finns nätverk och grupper som ska underlätta arbetet med informationssäkerhet och dataskydd, både centralt och lokalt.

4.1.2 Stadens nätverk för informationssäkerhetssamordnare

Sammankallas av Stadsledningskontoret och innefattar alla informationssäkerhetssamordnare i staden. Ansvarig för sammankallande är stadsledningskontoret. Inom nätverket sker informationsspridning om pågående arbete med informationssäkerhet i staden samt utbildning.

4.1.3 Nätverk för dataskyddsredogörare

Sammankallas av förvaltningens dataskyddsombud. För mer information kontakta dataskyddsombudet.

4.1.4 Södermalms nätverk för informationssäkerhet

Sammankallas av förvaltningens informationssäkerhetssamordnare. Nätverket omfattar informationssäkerhetssamordnare, säkerhetssamordnare, it-samordnare, dataskyddsombud och verksamhetsutvecklare.

5 Det årliga arbetet med informationssäkerhet

Informationssäkerhetsarbetet på förvaltningen pågår systematiskt och följs årligen upp av informationssäkerhetssamordnare och dataskyddsombud i samband med rapporten Ledningens genomgång respektive GDPR-rapporten.

5.1 Arbetet med väsentlighets- och riskanalys (VoR) och internkontroll

Systematiskt informationssäkerhetsarbete inklusive dataskyddsarbete planeras och följs även upp genom den internkontroll som utförs inom förvaltningen genom väsentlighets- och riskanalysen (VoR) och internkontrollplan (IKP).

Det innebär att väsentliga arbetssätt inom det systematiska informationssäkerhetsarbetet identifieras, kontrollaktiviteter beskrivs och analys genomförs för att identifiera möjliga felkällor i verksamhetens arbete, bedöma sannolikheten för att oönskade händelser uppstår, bedöma vilka konsekvenser dessa skulle kunna ha samt prioritera vilka risker verksamheterna behöver arbeta med för att säkerställa att oönskade händelserna inte uppstår. Samtidigt planeras åtgärder för att sänka riskvärdet. Detta görs på enhets-, avdelnings- och förvaltningsnivå. Vid varje uppföljningstillfälle ses identifiering och bedömningar över för att se om exempelvis nya

risker kan ha uppstått under perioden eller om riskvärdet förändrats, till exempel sjunkit på grund av aktiva åtgärder.

Internkontrollplanen (IKP) tas sedan fram och innehåller de processer med de mest allvarliga riskerna i VoR. I IKP planeras och dokumenteras vilka kontroller som ska göras för att se om de systematiska kontrollerna har genomförts som planerat och/eller om de visat på några avvikelser. Syftet är att bedöma hur väl de systematiska kontrollerna fungerar. Kontrollaktiviteterna utgör en del av det underlag nämnden behöver för att bedöma om den interna kontrollen är tillräcklig. Det är nämnden som fattar beslut om nämndens VoR, IKP och system för intern kontroll.

Enhetschef ansvar för att genomföra analyser, planering, kontroller och uppföljning och dokumentera i VoR och IKP. Avdelningschef ansvarar för att granska och besluta om VoR och IKP på avdelningsnivå. Samordnare av planering och uppföljning (verksamhetscontrollers) och samordnare av internkontroll (samordnande utredare) på stab och kansli ger stöd till chefer och sammanställer VoR och IKP på nämndnivå. Informationssäkerhetssamordnare och dataskyddsombud deltar i övergripande analys, planering och uppföljning inom det systematiska informationssäkerhetsarbetet på nämndnivå och finns som stöd till verksamheterna när risker identifierats på området och när åtgärder planeras.

5.2 Ledningens genomgång – uppföljning av informationssäkerhet

Uppföljningen av informationssäkerhetsarbetet är numera en del av stadens styr- och ledningssystem ILS och följer det årshjul som staden har för planering och uppföljning, för att säkerställa ett likartat arbete i hela staden.

Varje år ska stadsdelsdirektören därför inhämta rapporten Ledningens genomgång som redovisas i samband med verksamhetsberättelsen. Rapporten bör exempelvis redogöra för lokala rutiner för incidenthantering, utbildning av medarbetare, om registerförteckning finns och om informationsklassningar är gjorda, vilka styrdokument som finns och incidenter och avvikelser som rapporterats under året. Denna rapportering ska ge information och underlag till stadsdelsdirektör att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

5.3 GDPR-rapport – uppföljning av dataskyddsarbetet

Dataskyddsarbetet följs upp i den årliga GDPR-rapport som sedan 2021 är obligatorisk och skickas in till stadsledningskontoret som en bilaga till verksamhetsberättelsen. Utifrån bestämmelserna i GDPR har staden fastslagit ett antal återkommande, obligatoriska granskningsområden. Utöver detta beslutar dataskyddsombudet om granskningsområden som anses extra angelägna.

Förutom den årliga rapporten upprättas under året delrapporter avseende de områden som dataskyddsombud i rapport över föregående år beslutat granska.

5.4 Övrig uppföljning informationssäkerhet

Utöver Ledningens genomgång följs informationssäkerhetsarbetet upp genom att informationsklassningar ses över årligen. Då kontrolleras projekt- eller åtgärdsplaner och befintliga informationsklassningar konstateras om de fortfarande är aktuella, behöver kompletteras eller göras om för att förutsättningarna ändrats.

6 Rutiner och praktiskt arbete

Hur vi agerar är avgörande för hur väl informationen inom vår förvaltning och staden skyddas. I följande avsnitt finns därför råd om vad du bör tänka på när det gäller informationssäkerhet i praktiken i ditt dagliga arbete både för dig som medarbetare och som chef men även rutiner för vårt arbete med informationssäkerhet och dataskydd på Södermalm.

6.1 Behörighetshantering

Behörighetshantering är en av de viktigaste delarna i informationssäkerhetsarbetet och ansvaret är uppdelat beroende på vilken process det gäller.

Chefer är ansvariga för att medarbetares behörighet tas bort vid avslut av anställning eller övergång till annan förvaltning/bolag i Stockholms stad. Det är extra viktigt vid det senare alternativet då personen fortfarande jobbar inom staden och därmed kan få tillgång till information om behörigheter ligger kvar. Detta ingår i de checklistor som finns vid avslut av tjänst på förvaltningen som HR-avdelningen ansvarar för.

I övrigt är det den som ansvarar för en process som är ansvarig för vilka som har behörighet. Regelbundet bör därför denne gå igenom

vilka som har behörighet och stickprovskontroller bör genomföras. Detsamma gäller vilka som har behörighet till funktionsbrevlådor och gruppdiskar, det bör kontrolleras åtminstone en gång i halvåret av den som ansvarar för gruppdisken eller funktionsbrevlådan. Kontakta dataskyddsombud eller informationssäkerhetssamordnare vid behov av stöd för att se över rutin.

6.2 Dator

Några viktiga saker att tänka på gällande din arbetsdator. Lås alltid datorn alternativ logga ut varje gång du lämnar den även om det bara är för en minut. Lämna inte inloggningskort- eller tjänstekort i datorn när du lämnar den utan ta med dig och förvara säkert det är en del av det skydd vi har för att obehöriga inte ska kunna ta sig in i stadens system.

Skulle din dator bli stulen eller förloras på annat sätt ska det rapporteras till dataskyddsombud och informationssäkerhetssamordnare för kännedom då det beroende på hur datorn försvunnit kan vara en incident som ska rapporteras.

I övrigt sker förlustrapportering av dator på följande sätt:

- Servicedesk portalen 11800 alt. Fujitsu-portalen 33900 vilka nås via intranätet
- IA-systemet (nås via intranätet)
- Polisanmälan där du uppger datornummer, spara en digital kopia. Vid beställning av ersättningsdator behövs polisens diarienummer
- IT-samordnare för att ordna en ny dator

6.3 Distansarbete

Efter coronapandemin har distansarbete blivit vanligare och med det kommer ytterligare krav på informationssäkerhet. Vid distansarbete är informationssäkerhet extra viktigt, lämna aldrig din dator obevakad på offentliga platser och överväg noga om det är lämpligt att jobba eller prata på offentliga platser överlag. Lämna inte utskrivet material framme även om det bara är personer i ditt hushåll i närheten så ska dessa inte heller se, se till att ingen kan höra samtal och använd hörlurar om det behövs. Iaktta stor försiktighet vid arbete med personakter dessa bör inte tas med hem då rekommenderas att scanna in materialet istället. Tänk också på att inte lämna till exempel din dator i bilen eller på annan plats och att inte låna ut den. Detta då transporten av arbetsmaterial, dator och liknande till och från arbetsplatsen kan innebära en risk. Förvara därför inte dator och tjänstekort tillsammans i din väska och ta inte

hem personakter då de vid ett eventuellt rån eller förlust av väska riskerar att gå förlorade.

Använd VPN, det står för Virtual Private Network och innebär att du som medarbetare kan nå din e-post och stadens övriga system på ett säkert sätt. VPN slås automatiskt på så länge som du är inloggad med ditt tjänste- eller SITHS-kort och ansluten till internet. Var försiktig med vilka nätverk du använder, logga inte in på offentliga nätverk då det kan ge obehöriga en möjlighet att ta sig in i stadens system. Använd istället mobildata från din privata telefon eller jobbtelefon.

Mer information om hemarbete generellt finns på följande länk:
Tips vid distansarbete - Stockholms stads intranät

6.4 E-post, nätfiske, bluffmejl

När det gäller e-post finns några viktiga saker att ha i åtanke. Det som skickas från din e-post kan uppfattas som stadens e-post och den bör därför inte användas i privat bruk. En del av de meddelanden som skickas är eller blir allmänna handlingar även tillhörande bilagor enligt 5 kap. offentlighet- och sekretesslagen (2009:400). Mer information om vilken typ av e-post som ska diarieföras och arkiveras finns i hanteringsanvisningarna som Stadsdelsarkivarierna tagit fram vilka återfinns på intranätet. De loggar och förteckningar som skapas över skickade meddelanden är allmänna handlingar som kan begäras ut, tänk därför på vad du skriver i ämnesraden skriv till exempel inte ut känsliga uppgifter så som till exempel namn på klienter.

Mer information om e-post reglerna generellt i Stockholms stad finns på följande länk:
Regler för e-post - Stockholms stads intranät

Det har tydliggjorts att e-post som skickas internt inom staden är delvis krypterad, vilket innebär att den är krypterad när den skickas mellan två personer inom staden. Dock är e-posten inte krypterad när den ligger i mottagarens inkorg eller avsändarens skickat-korg, därför ska vi undvika att skicka känslig information via e-post då känslig eller sekretessbelagd information riskerar att röjas. Om du behöver göra det ändå kan ett lösenordskyddat dokument vara ett alternativ. Om du har e-post med känslig information bör du därför även flytta den från din inkorg eller skickat korg så snabbt som möjligt och istället spara ner relevant information på lämplig plats på din dator. Alla som använder e-post ska även kontrollera sin brevlåda och säkerställa att kollega gör det vid frånvaro. Var extra

försiktig med vilka uppgifter du skickar till externa mejladresser, det vill säga utanför Stockholms stad.

Alternativ till att mejla filer med känsligt innehåll kan vara att skapa en gruppdisk där de som brukar mejla har behörighet för att minimera att flera versioner av filen sparas i mejlkorgen och att fel personer får tillgång.

I e-posten kan det förekomma skräppost i form av bluffmejl och så kallat nätfiske, phishing-e-mails på engelska. Dessa kan se ut på olika sätt, det kan vara allt från att det finns ett paket att hämta hos ombud, då bör du ställa dig själv frågan om du faktiskt väntar på något och aldrig betala det som står till utpressningsmejl där någon uppger att du varit inne på olämpliga sidor och behöver betala. Gällande nätfiske är det ofta så att mottagaren luras att klicka på en länk som sedan leder till en sida där uppgifter som lösenord, koder och bankkontonummer ska anges. Uppge aldrig sådana uppgifter och var medveten om att inga företag, myndigheter eller andra organisationer använder det sättet för att be om uppgifter. Om obehöriga får tillgång till lösenord kan de ta sig in i stadens system och där plantera skadlig kod som går att läsa mer om under avsnitt 6.13. Att stoppa spridning av nätfiske är därför viktigt. Kontakta alltid informationssäkerhetssamordnare eller dataskyddsombud vid osäkerhet. Dessa mejl ska markeras skräppost och hanteras enligt en guide som finns i 11800-portalen för Tietoleveransen på följande länk: Självhjälp Guide - Hantering av bluffmejl

Allvarligare fall av nätfiske ska rapporteras i IA-systemet som nås via intranätet eller app i din arbetstelefon. Det gäller även om det är via telefon, så kallad vishing (voice phishing på engelska eller muntligt nätfiske). Ett sådant samtal kan vara att någon låtsas vara från IT-supporten och ber dig uppge inloggningsuppgifter eller att släppa in en besökare.

I övrigt kan skräppost vara mejl som endast innehåller en länk eller text eller bilaga. Öppna aldrig bilagor och klicka aldrig på länkar om du inte är helt säker på vem avsändaren är och vad innehållet är. Varningssignaler att vara uppmärksam på är oväntad avsändare, vilket även innebär kända avsändare men att innehållet gör att situationen framstår som konstig. Att det är skrivet på engelska, att du ska göra något skyndsamt eller att meddelande innehåller länkar som tidigare nämnt som du måste klicka på för att få tillgång till resten av meddelanden.

Beroende på allvarlighetsgrad av till exempel nätfiske mejl så kan även en polisanmälan behöva upprättas.

Även kalenderverktyget i Outlook kan utgöra en personuppgiftsbehandling, särskilt eftersom många delar kalendrar med andra. Tänk därför på att *inte* skriva ut namn på klienter vid kalenderbokningar.

6.5 Flerfaktorautentisering

Flerfaktorautentisering är en del av den tekniska säkerheten vi har i staden och på Södermalm. Det innebär att mer än ett steg behövs för att logga in vilket gör det svårare för utomstående att ta sig in än om endast lösenord hade behövts. Till exempel krävs det för att kunna logga in på våra datorer två steg, tjänstekort alternativt inloggningskort samt kod. Om kortet lämnas i datorn försvinner därmed halva autentiseringen och det blir osäkrare eftersom det endast krävs kod för att kunna logga in. Därför är det viktigt att alltid ta ut tjänstekort alternativt inloggningskort ur datorn när ni lämnar den för att säkerställa att det skydd vi har fungerar.

6.6 Fritextfältpolicy

Ur ett dataskyddsperspektiv så ska så få personuppgifter som möjligt behandlas, därför ska det också finnas en policy för fritextfält för exempelvis Excel-dokument. Södermalms policy är att endast nödvändiga uppgifter får fyllas i och uppgifterna ska vara så relevanta och neutrala som möjligt. Kommentarer som personliga reflektioner och liknande sparas på annat sätt och det används inte för anteckningar gällande brukare, klienter eller liknande. Det ska även vara tydligt utifrån filen vilka fält som bör fyllas i och inte.

Vid användning av textfält i exempelvis eDok eller andra system gäller uppgiftsminimering, så få personuppgifter som möjligt ska behandlas och endast de där det finns ett syfte.

6.7 Förebyggande arbete

En viktig del av informationssäkerhetsarbetet är att ha en kontinuitetsplan för hur verksamheten kan fortsätta vid till exempel ett strömavbrott, ofta är det via analoga arbetssätt. En del handlar även om att vara medveten om de leverantörer vi har, deras säkerhet och vårt beroende av dem. Denna information är bland annat det som en informationsklassning tar fram. Andra delar som är viktiga i det förebyggande arbetet är att vara vaksam mot mejl och särskilt länkar och bilagor. Installera de uppdateringar på datorer och telefoner som kommer ut, ofta åtgärdar de säkerhetsbrister som upptäckts samt rapportera incidenter och avvikelser i tid. Mer information om incidentrapportering finns i avsnitt 8 i denna anvisning.

6.8 Gruppdiskar

Behörighet till gruppdiskar bör kontrolleras av ägare och utdelas enligt minsta möjliga behörighet. Det vill säga så få som möjligt ska ha tillgång till gruppdiskar och finns flera gruppdiskar inom en enhet eller avdelning ska arbetsmaterial sparas på den gruppdisk där endast de som behöver materialet har behörighet. Stor försiktighet ska iakttas vid att spara material på gruppdiskar där ett stort antal personer har behörighet.

6.9 Internet

Allt du gör på internet kan spåras, det vill säga använd det inte för privata saker utan främst för jobb. Det står i kontraktet du läste första gången du loggade in på datorn.

6.10 Loggar

Informationssäkerhetssamordnare har möjlighet att begära ut loggar samt åtkomst till e-postlådor och hemkatalog från Tieto och Fujitsu. Begäran om loggar sker enligt stadsledningskontorets centrala rutin och hanteras restriktivt.

Kontakta förvaltningens lokala informationssäkerhetssamordnare via e-post för att begära uttag av loggar: Funktion.SD12.Informationssakerhetochdataskydd@stockholm.se.

6.11 Lösenord

I de fall du får välja egna lösenord använd säkra lösenord. Gäller det sifferkombinationer använd inte din födelsedag, ditt barns eller annan närståendes födelsedag eller liknande.

När det gäller lösenord bestående av bokstäver, siffror och tecken använd gärna långa lösenord som är lätta att komma ihåg t ex en ramsa bestående av fyra ord snarare än ett. Detta då alla lösenord upp till ett visst antal tecken kan slås upp i så kallade regnbågstabeller och därmed är lättare att knäcka för en dator. Se även alltid till att byta lösenord om du får ett slumpmässigt och det är möjligt. Förvara inte lösenord på ditt skrivbord eller nära din dator eller telefon, ett alternativ då är att istället använda så kallade lösenordshanterare.

6.12 Minnesanteckningar

Generellt är minnesanteckningar inte allmänna handlingar och går därför att göra i ett Word dokument. Välj då lämplig plats att spara på, vad gäller gruppdiskar tänk på vilka som har behörighet så att så få som möjligt och endast de som behöver har tillgång.

För socialtjänsten så går det att spara minnesanteckningar i Word-dokument, men det som behöver tas i beaktande är dels att spara dokumentet i en åtkomstbegränsad mapp, att gallra korrekt samt att det ska finnas ett klart motiverat skäl till behandlingen om det är en personuppgiftsbehandling.

I ett optimalt läge ska alla personuppgifter kunna knytas till ett ärende och ska då finnas i något av våra ärendehanteringssystem men det kan ibland vara berättigat att spara de på andra sätt men då vara klart motiverat utifrån verksamhetens behov.

6.13 Skadlig kod

Skadlig kod är det samlingsbegrepp som används för att beskriva oönskade datorprogram som olika sorters virus som till exempel ransomware, trojaner också kallat trojanska hästar och spionprogram. Dessa installeras på nätverk och datorer utan tillstånd med olika syfte, det kan vara att samla in information eller störa alternativt ta kontroll över IT-system. Skadlig kod kan även ge åtkomst till obehöriga utan vetskap för ägaren av datorn så att obehöriga är inne i systemet och ser allt som görs. Så kallad ransomware krypterar datorer, mobiler eller surfplattor så att innehållet inte går att nå mot en lösensumma. Den skadliga koden kan spridas genom att ett USB-minne körs i en dator, när e-post bilagor öppnas, filer laddas ner från internet eller när du klickar på en länk.

Alla våra datorer är utrustade med skydd mot skadlig kod men det handlar även om hur vi agerar för att skyddet ska fungera. Använd aldrig okända USB-minnen. Klicka aldrig på länkar och öppna inte bilagor som du inte är säker på, uppge inte information som efterfrågas och var uppmärksam. Ett tecken på att datorn kan vara utsatt för skadlig kod är att den blir långsammare eller att du märker att dokument försvinner eller ändras.

Nätfiske är ett sätt som kan ge angripare möjlighet att plantera skadlig kod och går att läsa mer om under e-post avsnittet 6.4.

Mer information om skadlig kod och nätfiske finns på följande länk till intranätet:
Så fungerar nätfiske och skadlig kod - Stockholms stads intranät

6.14 Skyddad identitet

I Stockholms stad hanteras skyddad identitet både gällande våra medborgare men även anställda vilket är det som kommer kommenteras här. Har du som anställd skyddad identitet av nivå 1 eller 2 är det ditt ansvar att se till att HR-avdelningen är informerad

och även att du påtalar det vid tilldelande av behörigheter. Har du skyddad identitet får du en anonym sida på intranätet och då kan du inte få verktyg länkade utan får spara ner det du behöver som bokmärken.

När det gäller SITHS-kort finns en rutin för utgivande av dessa som ska följas. Kontakta informationssäkerhetssamordnare eller IT-samordnare för mer information.

6.15 Zoom-, Skype- och Teamsmöten

När det gäller distansmöten ska vi använda de tjänster som staden har. För Tieto-leveransen används i första hand Zoom X (läs mer under avsnitt 7.5) och i andra hand Skype for business. De pedagogiska verksamheterna använder Teams. Båda är krypterade och skyddade genom en VPN-tunnel. VPN aktiveras när du är utanför kontoret, inloggad med kort och datorn är ansluten till internet och det är viktigt att du ser till att det är aktiverat.

Hantera distansmöten med stor försiktighet, det är stor skillnad mellan ett fysiskt möte och ett distansmöte. Dokument bör inte delas utan använd istället gemensam gruppdisk. Detsamma gäller Teams där känslig information inte bör delas eller sparas. Chatt- och konversationshistorik loggas och kan begäras ut via informationssäkerhetssamordnare.

6.16 Spara dokument

Spara alltid på rätt plats, aldrig lokalt på datorn utan alltid på (H:) eller dokument om det gäller material för eget bruk alternativt gruppdisk (G:) så att du kan nå dem även om din dator går sönder. Det som sparas på den lokala hårddisken (C:) säkerhetskopieras inte.

6.17 Skalskydd

På Virkesvägen och andra arbetsplatser finns ett skalskydd i form av att tjänstekort plus kod behövs för att komma in. Var därför noga med vem du släpper in med dig. Är du osäker på om någon obehörig vistas i lokalerna kontakta vakt på telefonnummer 08 – 508 12 307. Har du en arbetsplats som saknar skalskydd är det ännu viktigare att du säkerställer att ingen obehörig vistas i lokalerna, även om det är obekvämt.

6.18 Samtal

Vi är många anställda på Södermalm och alla har vi olika arbetsplatser men huvudkontoret är Virkesvägen. Generellt gäller att vi inte diskuterar ärenden, frågor gällande personuppgifter eller

liknande i fikarummet utan där pratar vi generellt om sådant som det inte gör något om andra hör. Detsamma gäller i hissen och matsalen.

Policyn är sådan att det är okej att ta samtal och distansmöten vid sin plats, men var då extra noga med vad du säger och om du märker att samtalet går i en riktning där det finns risk att fel personer hör känsliga uppgifter bör du gå till ett samtalsrum istället om det är möjligt.

6.19 Skrivbord

Några viktiga saker att tänka på när det gäller din arbetsplats eller ditt skrivbord är att alltid logga ut från datorn, lämna aldrig tjänstekort i datorn, lämna inte känsliga handlingar vid skrivbordet om du planerar att vara borta en längre stund. Tänk på att alla på Virkesvägen har tillgång till alla plan samt att externa personer som lokalvårdspersonal rör sig i lokalerna och därmed kan se det som finns vid skrivborden och i närheten.

6.20 SMS

Det har förekommit spam-sms, eller bluff-sms i olika varianter, dessa ska rapporteras som bluff-mejl i 11800-portalen. Exempel är att paket finns att hämta med länkar men precis som går att läsa under avsnitt 6.4 om bluffmejl så bör du ställa dig frågan om du väntar på något paket eller liknande annars är det bara att radera sms:et men kontakta gärna informationssäkerhetssamordnare så att denne får kännedom.

6.21 Social manipulation

En annan informationssäkerhetsrisk är det som på engelska kallas för social engineering, på svenska social manipulation och ofta beskrivs människan som den svagaste länken när det gäller informationssäkerhet. Det innebär att personer manipulerar andra att utföra handlingar eller ge ut information frivilligt i motsats till t ex intrång.

Det handlar om att vara vaksam mot telefonsamtal, besök i reception och i allmänhet mot okända personer som vill ha information. Även information som inte verkar känslig som vilket våningsplan en enhet sitter på kan vara precis vad den personen det behöver för att nå den information den är ute efter. Det kan vara att någon följer med in genom dörren, vill låna en telefon, att ett USB-minne placerats ut med en märkning som tyder på att det är någon som tappat det. Därför ska okända USB-minnen aldrig användas i våra datorer om du hittar ett kontakta informationssäkerhetssamordnare.

6.22 Telefon

Använd den möjlighet som finns med skärmlås på din jobbtelefon då den innehåller känslig information som mejl och tillgång till intranätet. Tänk på att inte läsa mejl eller prata i telefon på offentliga platser som t ex i kollektivtrafiken.

Skulle din telefon bli stulen eller förloras på annat sätt ska det rapporteras till dataskyddsombud och informationssäkerhetssamordnare för kännedom då det beroende på hur telefonen försvunnit kan vara en incident som ska rapportera.

I övrigt sker förlustrapportering av telefon på följande sätt:

- Servicedesk portalen 11800 alt. Fujitsu-portalen 33900 vilka nås via intranätet
- IA-systemet (nås via intranätet)
- Polisanmälan, spara en digital kopia
- IT-samordnare för att ordna en ny

6.23 Tjänstekort (inloggningskort)

Inloggningskortet, eller tjänstekortet, ska inte förvaras tillsammans med din dator då det är en del av den flerfaktorautentisering vi har för att skydda åtkomst till stadens system.

Du ska aldrig låna ut ditt tjänstekort, inte sätta några kännetecken som går att koppla till dig på kortet varken namn, klistermärken eller annat.

Vid förlust av tjänstekort anmäl till:

- Servicedesk 11800-portalen alt. Fujitsu 33900-portalen vilka nås via intranätet
- IA-systemet(nås via intranätet)
- Tjänstekortsadministratör
- Informationssäkerhetssamordnare och dataskyddsombud
- Närmaste chef

Förlust av SITHS-kort ska anmälas till polisen. Spara diarienummer.

6.24 Vanor och beteende

Informationssäkerhet handlar även om vanor, om du alltid lämnar ditt tjänstekort i datorn kan andra lägga det på minnet och därmed är det lättare att planera för att ta sig in i datorn. Samma sak om du har för vana att ta jobbsamtal på väg till och från jobbet kan du riskera att känslig information läcker ut. Det handlar även om att utvärdera sina arbetssätt regelbundet. Förr kanske det var bäst att mejla en

Excel-fil fram och tillbaka men idag kanske det finns ett program eller en gruppdisk som är säkrare och bättre att använda. Det är därför det är viktigt att regelbundet gå de obligatoriska utbildningarna i informationssäkerhet och dataskydd för att ha kunskapen som behövs nära i minnet.

7 Identifiera och inventera

7.1 Informationstillgångar och personuppgiftsbehandlingar

Det är viktigt att kunna avgöra hur skyddsvärd den information vi har är samt riskvärdera den, vilket är anledningen till klassningen och inventeringen. Det är viktigt att ha ordning på alla informationstillgångar vi har, därför ska alla system klassas. Södermalm har en rutinbeskrivning som beskriver det arbetet.

Du hittar rutinbeskrivningen via följande länk.
Rutinbeskrivning Södermalm - Stockholms stads intranät

7.2 Personuppgiftsbiträdesavtal

Om en annan myndighet eller privat aktör behandlar personuppgifter för nämndens räkning utan att själv besluta om behandlingens syfte och medel ska ett personuppgiftsbiträdesavtal tecknas. Genom detta avtal förbinder sig den andra aktören att behandla personuppgifterna på ett sätt som lever upp till bestämmelserna i GDPR och att informera den personuppgiftsansvariga (i detta fall nämnden) om eventuella personuppgiftsincidenter eller förändringar av tjänsten. I den instruktion som ska upprättas som bilaga till personuppgiftsbiträdesavtalet ger den personuppgiftsansvariga övriga instruktioner till biträdet om behandling av personuppgifter. Om huvudavtalet är centralt ska också personuppgiftsbiträdesavtalet vara centralt. Södermalms stadsdelsförvaltning har en rutin för uppföljning av personuppgiftsbiträdesavtal.

7.3 Registerförteckning

Alla personuppgiftsbehandlingar vi har ska finnas förtecknade i vår registerförteckning som i nuläget görs i systemet DraftIt Privacy records. Att förteckna behandlingar är en grundläggande del i att som personuppgiftsansvarig skaffa sig den överblick som behövs för att identifiera riskfyllda behandlingar och kunna visa att man följer dataskyddsförordningen. Kontakta dataskyddsredogörare vid din avdelning alternativt DSO. Vid en ny behandling ska dataskyddsredogörare eller DSO kontaktas.

7.4 Medgivande eller samtycke

Eventuella samtycken eller medgivande som samlas in, ska dokumenteras och förtecknas. Det är viktigt för att säkerställa att laglig grund för personuppgiftsbehandling finns. Samtycke ska undvikas som laglig grund om det är möjligt att hitta en annan eftersom den ojämlika relationen mellan en myndighet och den registrerade generellt gör samtycke olämpligt.

7.5 Molntjänster

7.5.1 Bakgrund molntjänster

Molntjänster kan innebära att ytterligare personuppgiftsbehandlingar sker och därför är det viktigt att veta vilka sådana vi använder samt underrätta dataskyddsombud och informationssäkerhetssamordnare vid användning. Oftast innebär molntjänster att data i någon form behandlas extern på en annans server, utanför Stockholms stad. I vissa fall kan servern finnas i ett tredje land, utanför EU/EES och då är det inte nödvändigtvis en laglig användning.

7.5.2 Deltagande i videomöten

Inom staden används i första hand Zoom X eller Skype (Skype fasas ut under första delen av 2024) alternativt Teams beroende på IT-leverantör. Vid deltagande vid externa möten kan ibland andra tjänster användas. Generellt innebär det en passiv användning av molntjänst som ännu inte informationsklassats samt att data behandlas i molnet och därmed personuppgifter i form av namn, bild och video. Tänk därför noga igenom innan du deltar i ett sådant möte vad ni ska prata om, generellt sett så kan nyttan av deltagandet väga över risken men en bedömning bör alltid göras inför deltagande.

Passiv användning av molntjänster kan även förekomma genom att någon besvarar förfrågningar i online-tjänster eller använder olika appar som till exempel Kahoot! för quiz eller liknande. Även det räknas som användning och riskanalys bör alltid genomföras inför även sådan typ av användning.

7.5.3 Kontrollfrågor inför användning

- Är det en molntjänst, lagras eller bearbetas data på någon annans server?
- Finns det något alternativ till tjänsten t ex upphandlad inom staden?
- Vilka risker finns avseende konfidentialitet, riktighet och tillgänglighet?

- Vilka personuppgifter kommer behandlas (t ex IP-adress, namn, bild)?
- Behandlas känsliga personuppgifter?
- Riskeras att personuppgifterna överförs till tredjeland, direkt eller indirekt t ex genom support i tredje land (dvs. land utanför EU/EES)?
- Finns personuppgiftbiträdesavtal?

7.6 Informationsklassningar

7.6.1 Informationsklassning

Stadens riktlinjer säger att alla informationstillgångar och personuppgiftsbehandlingar inom staden ska vara klassade för att säkerställa att det har rätt skydd. En informationsklassning ska därför genomföras inför upphandling, vid införande av nytt system, arbetssätt eller process eller för system, arbetssätt eller process där det inte gjorts. Informationsklassningarna ska även anpassas efter omvärlden om system eller annat ändrats som kan påverka informationen.

En informationsklassning består av flera steg och finns beskrivet i dokumentet ”*Rutinbeskrivning informationssäkerhet och dataskydd*”. Dokumentet samt även den senaste versionen av informationsklassningsprotokollet och annan allmän information återfinns via följande länk.
Informationssäkerhet - Stockholms stads intranät

7.6.2 Konsekvensbedömning

Om en analys visar att en process, arbetssätt eller teknisk lösning innebär risker för de registrerades personuppgifter, till exempel på grund av att en stor mängd uppgifter, känsliga personuppgifter och/eller uppgifter om särskilt utsatta personer behandlas behöver verksamheten göra en fördjupad analys av personuppgiftsbehandlingen. Detta kallas en konsekvensbedömning och genomförs tillsammans med förvaltningens dataskyddsombud. Mer om konsekvensbedömningar finns att läsa på stadens sida om GDPR på intranätet via följande länk.
GDPR - Stockholms stads intranät

8 Incidenthantering

Det är viktigt att rapportera när någonting går fel och att vi lär oss av det. Rapportera hellre en gång för mycket än en gång för lite. Det är viktigt att incidenthanteringen sker på rätt sätt så att alla

incidenter hanteras korrekt och även för att undvika liknande incidenter framöver. Alla incidenter ska rapporteras i vårt IA-system och vem som helst kan rapportera.

Om det är en pågående incident och kontakt behövs med informationssäkerhetssamordnare eller dataskyddsombud när dessa inte i tjänst finns en backup lista hos stab och kansli, kontakta registraturen för mer information på soder@stockholm.se. En händelse kan vara både en personuppgiftsincident och informationssäkerhetsincident varför både informationssäkerhetssamordnare och dataskyddsombud ska kontaktas.

8.1 Incidentrapportering i praktiken

Alla incidenter ska rapporteras i IA -systemet. Informations- och personuppgiftsincidenter ska även rapporteras till informationssäkerhetssamordnare och/eller dataskyddsombud och i vissa fall ska det även rapporteras i 11800-portalen alternativt 33900-portalen. Du kan även ta kontakt med din Servicedesk för att få hjälp.

Ta gärna skärmklipp av eventuella bluffmejl, men klicka aldrig på länkar och skicka aldrig vidare dem eller andra mejl som du tror är skadliga på något sätt. Dokumentera även händelseförloppet så att underlag finns för att kunna utvärdera, till exempel i ett Word dokument och lämna sedan till informationssäkerhetsamordnare och/eller dataskyddsombud. Viktig information att få med är följande:

- Hur situationen uppstod, till exempel att du klickade på en länk i ett mejl
- Vilken information och tjänster som troligen har påverkats eller röjts, till exempel att du uppgav bankkontonummer eller lösenord
- Vilka andra konsekvenser du misstänker kan ha uppstått
- Hur incidenten hanterats hittills om det skett

8.2 Personuppgiftsincident

En personuppgiftsincident innebär att personuppgifter på ett felaktigt sätt har spridits, röjts, ändrats eller förstörts. En misstänkt personuppgiftsincident ska omedelbart rapporteras till förvaltningens dataskyddsombud. Denne tar därefter ställning till om det räcker att upprätta en intern incidentrapport eller om händelsen också behöver rapporteras till Integritetsskyddsmyndigheten. I så fall måste detta ske 72 timmar

efter upptäckt. En personuppgiftsincident ska även anmälas i IA. Detta görs av den verksamhet där den skedde.

Exempel på personuppgiftsincidenter kan vara följande:

- E-postmeddelande med känsliga uppgifter skickas till fel mottagare
- En mobiltelefon, surfplatta eller dator som innehåll personuppgifter blir stulen
- Personuppgifter exponeras för obehörig till följd av dataintrång eller inbrott

För att rapportera personuppgiftsincident i IA, gå till ”Övriga” och välj sedan ”Personuppgiftsincident”.

Verksamheten behöver också ta ställning till om händelsen också ska föranleda till exempel en Lex Sarah.

Kontakta alltid dataskyddsombud Anna Remmets vid en personuppgiftsincident.

8.3 Informationssäkerhetsincident

En informationssäkerhetsincident är en incident där information blivit påverkad på något sätt utifrån de kriterierna som nämndes i avsnitt 2.1. Det vill säga att information har förändrats, försvunnit, inte är tillgänglig eller är felaktigt eller att en risk finns för att informationen skulle kunna bli det. Praktiska exempel kan t ex vara:

- Mejl som skickas till fel mottagare
- Bluffmejl
- Virusattacker
- Skadlig kod
- Intrång/IT-angrepp
- Stöld av dator
- Brister i efterlevnaden av dessa riktlinjer

Informationssäkerhetsincidenter ska därmed särskiljas från allmänt datorstrul som att datorn till exempel hänger sig. Om information däremot försvunnit, påverkats eller blivit otillgänglig på grund av att datorn hängt sig så har informationens tillgänglighet påverkats och det bör därför rapporteras som en informationssäkerhetsincident.

En informationssäkerhetsincident rapporteras i IA-systemet under ny händelse och sedan egendom/säkerhet.

Gränsen mot en personuppgiftsincident kan vara svår att dra, därför är det alltid bättre att kontakta både dataskyddsombud och

informationssäkerhetssamordnare vid osäkerhet så att en bedömning kan ske. Vissa incidenter kan även vara både en personuppgiftsincident som informationssäkerhetsincident.

Gäller det bluffmejl finns en guide för hur dessa ska hanteras på följande länk för Tietoanvändare:
Självhjälp - Guide - Hantering av bluffmejl (stockholm.se)

8.4 NIS-incident

En NIS-incident är en incident som rör ett system som går under NIS-direktivet, Direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Dessa ska rapporteras till MSB inom en viss tid och därför är det extra viktigt att de rapporteras omgående. Det gäller för Södermalms stadsdelsförvaltnings del system inom hälso- och sjukvård, men generellt omfattar NIS de sju sektorerna bankverksamhet, digital infrastruktur, energi, finansmarknadsinfrastruktur, leverans och distribution av dricksvatten samt transport, utöver hälso- och sjukvård.

En NIS-incident rapporteras till MSB i olika steg, det första efter 6 timmar. För rapportering se ”*Rutin för rapportering av NIS-incidenter Södermalm*” och tillhörande frågestöd, finns som bilaga till denna rutin.

Mer information finns hos MSB länk: Incidentrapportering för leverantörer av samhällsviktiga tjänster (msb.se)

9 Utbildning och aktiviteter

9.1 E-utbildning

Inom stadens finns två obligatoriska digitala utbildningar som alla medarbetare ska gå regelbundet en gång per år då material kan uppdateras. Det är chefens ansvar att medarbetarna genomför utbildningarna. Statistik över deltagande kan tas fram av informationssäkerhetssamordnare. Dessa obligatoriska utbildningar som finns på Utbildningsplattformen och nås via intranätet är Informationssäkerhet för medarbetare i staden samt Grundkurs i dataskydd. Chefer rekommenderas även att gå utbildningen Informationssäkerhet för chefer.

Under 2024 lanseras två nya e-utbildningar av stadsledningskontoret för chefer och medarbetare. Utbildningarna är tänkta som ett komplement till stadens obligatoriska utbildningar.

9.2 Övrig utbildning

Stadens sida för informationssäkerhet där även stadens centrala riktlinje samt tillämpningsanvisningar finns:

Stadsövergripande informationssäkerhet - Stockholms stads intranät

Utbildningar och information om informationssäkerhetsarbetet vid distansarbete återfinns på Myndigheten för samhällsskydd och beredskaps (MSB) sida via följande länk:

MSB - informationssäkerhet vid distansarbete

Digital informationssäkerhetsutbildning för alla (DISA), MSB, återfinns via följande länk:

Digital informationssäkerhetsutbildning för alla (DISA) - MSB

9.3 Information till nyanställda

Vid alla nyanställningar ska du som chef informera om att de ska gå de två obligatoriska utbildningarna samt berätta om Stockholms stads riktlinje för informationssäkerhet och denna lokala anvisning och att dessa ska följas.

Övrig allmän information som kan vara bra att nämna är:

- Informationssäkerhetsarbetet ska finnas med inför upphandlingar av nya system och införande av nya arbetssätt
- Lämna inte dator-/tjänstekort i datorn när du lämnar skrivbordet
- Släpp inte in obehöriga på arbetsplatsen
- Koppla bort skärm i konferensrum när ni använder VIA
- Dela bara information med den som behöver, tänk på var du pratar om vad
- Använd inte okända USB-minnen, kan innehålla skadlig kod
- Stor försiktighet vid hantering av information vid hemarbete
- Använd säkra lösenord, använd inte samma till flera tjänster, flerfaktorautentisering när möjligt
- Läs på om social manipulation
- Koppla alltid bort skärmen i konferensrummen när VIA används
- Se till att eventuella kontinuitetsplaner är kända
- Kontakta alltid informationssäkerhetssamordnare eller dataskyddsombud vid osäkerhet och frågor

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Alexandra Wynn, Stadsdelsdirektör	2024-01-18
Emma Liljenberg, Avdelningschef	2024-01-18