Stockholms stad

Lokal anvisning för informationssäkerhet

Skärholmens stadsdelsförvaltning

Beslutad 21/5-2024

Lokal anvisning för informationssäkerhet

Dnr: SKHLM 2024/499

Kontaktperson: Informationssäkerhetssamordnare

Förord

Denna lokala tillämpningsanvisning styr stadsdelsförvaltningens systematiska informationssäkerhetsarbete och utgör ett komplement till stadens centrala riktlinjer och anvisningar inom området.

Den förtydligar hur ansvarsfördelning och roller har anpassats för stadsdelsförvaltningen, vilka stödjande och granskande funktioner som finns, lokala rutiner och riktlinjer samt hur samtliga medarbetare inom förvaltningen ska arbeta för, och bidra till, en god informationssäkerhetsnivå.

Då förvaltningen främst använder centralt upphandlade IT-tjänster som förvaltas av tredjepartsleverantörer så har PM3 modellens begreppsanvändning frångåtts i denna anvisning, dock omhändertas informationssäkerheten på samma nivå. I avsnitt 9 finns ett fördjupat resonemang om PM3 modellen och varför stadsdelsförvaltningen valt att använda egna begrepp inom informationssäkerhetsorganisationen.

I anvisningen finns hyperlänkar markerat med blå text med hänvisningar och mer information.

Denna lokala anvisning uppdateras årligen enligt årshjulet.

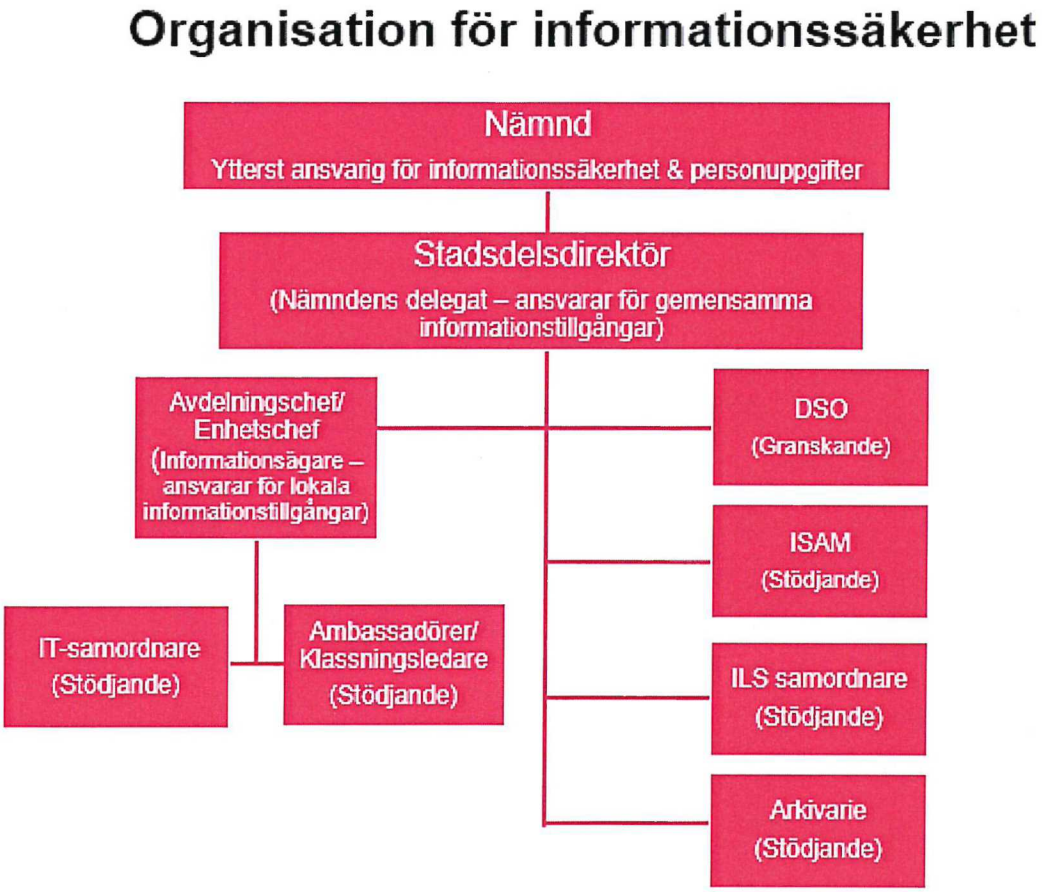
Dokumentet fastställdes av stadsdelsdirektören för nämndens räkning den 21/5-2024

Innehållsförteckning

1 Informationssäkerhetsorganisation

Nedan beskrivs stadsdelsförvaltningens organisation för informationssäkerhet samt utpekade roller och deras ansvar.

1.1 Organisation



Nämnden är ytterst ansvarig för informationssäkerheten och personuppgifter på förvaltningen.

Stadsdelsdirektören utgör nämndens delegat i informationssäkerhetsfrågor samt ansvarar för att säkerheten på de IT-tjänster och den information som förvaltningen gemensamt hanterar, lever upp till rättsliga och internt ställda krav.

Avdelningschefer/ enhetschefer/ områdeschef ansvarar för att säkerheten på de IT-tjänster och den information som avdelningen/ enheten lokalt hanterar, lever upp till rättsliga och internt ställda krav.

Informationsägarskapet (den som har informationssäkerhetsansvaret) följer linjeverksamheten och styrs av vilka avdelningar/ enheter som primärt använder IT-tjänsten och/ eller hanterar informationen.
Informationsägarskap innebär att man har ett särskilt ansvar för att informationen hanteras enligt gällande lagstiftning och riktlinjer.

Informationsägaren kan delegera och fördela uppgifter som följer av detta men kan inte delegera ansvaret. Till stöd i arbetet finns stödjande och granskande roller i informationssäkerhetsorganisationen.

Stödjande och **granskande** roller:
Här återfinns specialister vars främsta uppgift är att stödja och granska verksamheten i informationssäkerhetsarbetet. Deras roll är att erbjuda expertis och hjälpa till för att säkerställa att rätt åtgärder vidtas för att skydda informationen och att alla relevanta riktlinjer och regler efterlevs.

1.2 Informationssäkerhetsansvariga

1.2.1 Nämnd

Nämnden ansvarar för att det finns ett ändamålsenligt och effektivt informationssäkerhetsarbete inom stadsdelsförvaltningen samt att stadsövergripande riktlinjer och anvisningar för informationssäkerhet efterlevs.

Nämnden ansvar även för att utse dataskyddsombud men kan delegera denna uppgift till stadsdelsdirektören som då ska anmäla sitt beslut till nämnden.

Årligen inhämtar nämnden "GDPR årsrapport" från dataskyddsombudet.
Syftet är att nämnden med stöd av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker inom stadsdelsförvaltningen och dess olika verksamheter.

1.2.2 Stadsdelsdirektör/ förvaltningschef

Stadsdelsdirektören är nämndens representant (delegat) när det gäller de övergripande lednings- och styrningsfrågorna inom informationssäkerhetsområdet.

Stadsdelsdirektören har fått delegation från nämnden/styrelsen att besluta i de ärenden som är listade i delegationsförteckningen.

Stadsdelsdirektören har i sin tur rätt att vidaredelegera ärenden till annan anställd inom stadsdelsförvaltningen på sådant sätt som framgår av delegationsordningen.
Skärholmen Delegationsordning (stockholm.se)

Stadsdelsdirektören är informationsägare för de IT-tjänster som används inom flera avdelningar på förvaltningen och ska skriva under klassningsprotokoll och PUB-avtal för dessa.

Stadsdelsdirektör ansvarar för:

- Att fastställa de lokala tillämpningsanvisningarna och andra övergripande styrdokument för förvaltningens informationssäkerhetsarbete samt tillse att de efterlevs.
- Att utse informationssäkerhetssamordnare och ansvara för att stödfunktioner för informationssäkerhet tilldelas de resurser som krävs.
- Att verksamheten tilldelas de resurser som behövs för att kunna upprätthålla god informationssäkerhet.
- Att hålla sig underrättad om informationssäkerheten och årligen inhämta årsrapporten "Ledningens genomgång" från ISAM.
- Att tillse att klassificeringsstruktur och hanteringsanvisningar har fastställts för verksamhetens informationshantering.

1.2.3 Avdelningschef/ Enhetschef/ Områdeschef

Chefer är informationsägare för lokala IT-tjänster som endast används på avdelningen/ enheten eller inom specifik verksamhetsområde och ska skriva under klassningsprotokoll och PUB-avtal för dessa.

Chef ansvarar för:

- Att en processdriven informationsinventering är utförd inom den egna verksamheten och att informationstillgångarna finns upptagna i systemförvaltningsregistret hos ISAM.
- Att utse informationssäkerhetsambassadör från sin avdelning.
- Att utse klassningsledare samt vilka roller/personer som ska delta i informationsklassningen.
- Att informationstillgångar är klassade och att de säkerhetsåtgärder som framkommer av handlingsplanen även innefattat de legala hanteringskraven implementeras.
- Informationsägaren ansvarar för att var tredje månad revidera tilldelade behörigheter på avdelningen eller enheten genom att beställa ut listor från IT-samordnare.
- Att medarbetare och konsulter årligen genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd.
- Att inom en månad följa upp och utreda de incidenter som verksamheten anmäler i IA samt informera informationssäkerhetssamordnare.
- Att skyndsamt informera dataskyddssamordnare vid personuppgiftsincidenter.
- Att skyndsamt informera nämnden vid personuppgifsincidenter.
- Att årligen revidera registerförteckningen.
- Att årligen revidera systemförvaltningsregistret.
- Att typ A klassning genomförs innan upphandling av nya IT-tjänster.
- Att löpande hantera och revidera åtkomsträttigheter till IT-tjänster för sina medarbetare och konsulter.

1.3 Stödjande och granskande roller

1.3.1 IT-samordnare

För de flesta av förvaltningens IT-system sköts driften av en tredjepartsleverantör (tjänsteleverantör). I de fall förvaltningen upphandlar egna IT-system ska en IT-samordnare vara utsedd IT-systemet.

IT-system där drift sköts av tredjepartsleverantör eller av annan förvaltning/centralt är IT-samordnarens huvudsakliga roll att agera sakkunnig och vara verksamhetens lokala representant mot stadsledningskontorets IT-avdelning och tjänsteleverantörer.

En IT-samordnare ansvarar för drift och förvaltning av en IT-tjänst samt att de tekniska säkerhetsåtgärder som framkommer vid informationsklassningen implementeras i enlighet med informationsägarens beslut.

Vilka som tilldelats rollen IT-samordnare ska framgå i klassningsprotokollet samt i systemförvaltningsregistret.

IT-samordnare ansvarar för:

- Att tillse att stadens riktlinjer och tillämpningsanvisningar följs vad gäller informationssäkerhet för IT-tjänster.
- Att överse tilldelning samt annullering av behörigheter i enlighet med informationsägarens beslut.
- Att agera sakkunnig vid klassning.

1.3.2 Informationssäkerhetssamordnare (ISAM)

ISAM ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet samt stötta och vägleda verksamheten i informationssäkerhetsfrågor.
ISAM ska arbeta utifrån stadsdelsdirektörens styrning av vilka verksamhetsrisker och åtgärder som ska prioriteras.

ISAM ansvarar för:

- Att vara kontaktpunkt för stadens centralt informationssäkerhetsansvariga (CISO) samt rapportera allvarliga incidenter till denna.
- Att fungera rådgivande gentemot förvaltningen.
- Att samverka med andra ISAM och DSO inom staden.
- Att stödja linjeverksamheten när det gäller det strategiska arbetet, kartlägga information, informationsklassning, hantera incidenter samt utbilda medarbetare och verka för en ökad säkerhetsmedvetenhet.
- Att bevaka förändringar i lagstiftningen och informationssäkerhetshändelser i omvärlden och rapportera inåt.
- Att genomföra revisioner på det lokala informationssäkerhetsarbetet.
- Att samordna nätverket för informationssäkerhetsambassadörerna
- Att beställa loggar för e-post vid begäran om allmän handling.
- Att upprätthålla och underhålla registerförteckningen.
- Att upprätthålla och underhålla systemförvaltningsregistret.

- Att delta i det årliga RSA arbetet.
- Att årligen rapportera ledningens genomgång till förvaltningsledningen

1.3.3 Dataskyddsombud (DSO)

Dataskyddsombudets överordnade uppgift är att kontrollera att förvaltningen arbetar utefter de lagkrav och hanteringsregler som följer av dataskyddsförordningen (GDPR).

Dataskyddsombudet ska kunna agera självständigt och oberoende i sitt uppdrag och ska därmed inte utföra det operativa arbetet.

DSO ansvarar för:

- Att fungera rådgivande gentemot förvaltningen.
- Att samverka med andra ISAM och DSO inom Staden.
- Att stödja linjeverksamheten när det gäller det informationsklassning, konsekvensbedömning.
- Att utbilda medarbetare och verka för en ökad säkerhetsmedvetenhet.
- Att bevaka förändringar i lagstiftning och personuppgiftsincidenter i omvärlden och rapportera inåt.
- Att genomföra revision av det lokala dataskyddsarbetet.
- Att ge råd vid personuppgiftsincidenter, i enlighet med verksamhetens incidentrutin.
- Att årligen upprätta GDPR årsrapport och föredra den för Nämnden.
- Att samarbeta med tillsynsmyndigheten och fungera som förvaltningens kontaktpunkt

1.3.4 ILS-samordnare

Verksamhetens ILS-samordnare samordnar uppföljningen och beredningen av nämndens ILS-arbete.
ILS-samordnaren ska aktivt arbeta för att informationssäkerhet är med och följs upp i förvaltningens väsentlighets- och riskanalys samt införliva informationssäkerheten i verksamhetsplanen med stöd från informationssäkerhetssamordnaren.

1.3.5 Arkivarie

Övergripande arkivfunktioner har en viktig funktion i stadens informationssäkerhetsarbete. Arkivarie deltar aktivt i förvaltningens informationssäkerhetsarbete och i dess inventeringar av informationstillgångar – både digitala och fysiska.
Arkivarie är med stadsdelsarkivarie i framtagandet av förvaltningens hanteringsanvisningar och övrig arkivdokumentation. I dem beskrivs hantering och arkivering av stadsdelsnämndens samtliga informationstillgångar
Arkivorganisationen beskrivs närmare i förvaltningens arkivinstruktion

1.3.6 Informationssäkerhet/ Dataskyddsambassadörer

Minst en ambassadör per avdelningen ska vara utsedd, om möjligt. Syftet är att stötta och stärka sin avdelnings informationssäkerhetsarbete i den utsträckning som är möjlig för stunden sett till övrig arbetsbelastning. Ambassadörsrollen kombineras med ordinarie tjänst och förväntas därmed inte kunna bistå vid samtliga tillfällen. När ambassadör inte har möjlighet att stötta sin avdelning så tar ISAM över ansvaret. Ambassadör ska genomgå förberedande utbildning hos ISAM och stöttas sedan efter behov. För ambassadörer återfinns ett lokalt informationssäkerhetsnätverk som ISAM håller i. Nätverket syftar till att vara kompetenshöjande samt hitta synergier mellan avdelningarnas informationssäkerhetsarbete. Nätverket håller minst 4 protokollförda möten per år.

Ambassadören ansvarar för:

- Att stötta chef i det lokala informationssäkerhetsarbetet.
- Att verka för en god informationssäkerhetsmedvetenhet inom avdelningen.
- Att sprida kunskap och information om de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd.
- Att fungera som lokal länk mellan chef, avdelning, ISAM och DSO
- Att bistå chef med att samordna och sammanställa avdelningens registerförteckning.
- Att stödja vid rapportering av personuppgift och informationssäkerhetsincidenter.
- Att agera klassningsledare med stöd av ISAM.
- Att delta i arbetet med konsekvensbedömningar, handlingsplaner, riskanalyser samt förvaltningsplaner.
- Att delta i nätverksforumet för ambassadörerna.

1.3.7 Klassningsledare

På uppdrag av informationsägaren ansvarar klassningsledaren för att planera, förbereda och genomföra informationsklassningen tillsammans med informationsägarens utsedda arbetsgrupp

Klassningsledaren ansvarar för:

- Att undersöka om det finns tidigare genomförda klassningar med stöd ifrån ISAM (exempel på dokument: klassningsprotokoll, handlingsplan, riskanalys konsekvensbedömning och PUB-avtal).
- Att planera upplägg och uppskatta tidsåtgång för klassningens respektive steg. (ca 2 tim. per gång)
- Att förbereda klassningsprotokollet med grunduppgifter så att deltagarna kan fokusera på de viktiga bedömningsfrågorna under mötet..
- Att bjuda in deltagarna och kortfattat beskriva mötets syfte och arbetsgång samt vad de förväntas bidra med i klassningen.
- Att erbjuda deltagarna att förbereda sig genom att gå stadens e-utbildning: Förberedelse inför informationsklassning
- Att kalla till och leda deltagarna genom klassningen

1.4 Övriga ansvariga roller

1.4.1 Samtliga medarbetare

Samtliga medarbetare inom förvaltningen ska följa stadens och förvaltningens riktlinjer och tillämpningsanvisningar.

Samtliga medarbetare ansvarar för:

- Att ta del av och hålla sig uppdaterad om den information som finns inom informationssäkerhetsområdet på intranätet.
- Att årligen genomföra de obligatoriska utbildningarna inom informationssäkerhet Informationssäkerhet och dataskydd Dataskydd
- Att medverka för att informationssäkerheten upprätthålls på en adekvat nivå genom hög säkerhetsmedvetenhet och efterlevnad av denna anvisning.
- Utan dröjsmål rapportera incidenter och säkerhetsbrister till närmaste chef.
- Beakta informations skyddsvärde genom perspektiven konfidentialitet, riktighet och tillgänglighet.

2 Nätverk och grupper

Stadsdelsförvaltningen innehar representation i följande nätverk och arbetsgrupper:

- ISAM nätverket leds av SLK och CISO. I nätverket ingår ISAM från stadens olika förvaltningar och bolag där aktuella frågor avhandlas och aktuella utbildningar hålls.
- Ambassadörsnätverket leds av ISAM. I nätverket ingår lokala representanter från respektive avdelning och syftar till höja kompetensnivån samt identifiera behov hos avdelningarna, sammankallas minst 4 gånger per år
- GUG "GDPR utan gränser": Nätverk för stadsdels- och fackförvaltningar. Sammankallas och leds genom delat ansvar av DSO:erna. Syfte är att diskutera och lösa gemensamma frågor samt utbyta kunskap.

3 Årshjul

Q1 jan-mars Bedöm nuläge

- Förvaltningen utser informationssäkerhets- och dataskyddsambassadörer
- Möte med ambassadörer/GDPR infosäk x1
- Beslut handlingsplan
- Föredragning GDPR årsrapport nämnd
- Obligatoriska digitala utbildningar GDPR/Infosäk
- Inventering informationstillgångar
- Information till ledningsgrupp

Q2 april-juni Kontroll över informationstillgångar

- Möte ambassadörer GDPR/Infosäk x1
- Inventera informationstillgångar
- Uppdatera registerförteckning
- Utreda verksamhetens rutiner för informationssäkerhet/GDPR
- Framtagning/ revidering styrdokument lokal anvisning
- Granska PUB-avtal/leverantör
- Information till ledningsgrupp

Q3 juli-sept. Sprida information och kontroll

- Möte ambassadörer GDPR/Infosäk x1
- Beslut om styrdokument lokal anvisning
- Uppföljning genomförda utbildningar för medarbetare och chefer
- Revidera behörigheter gemensamma lagringsytor
- Uppdatera registerförteckning GDPR
- Förskolan, kontrollera giltiga samtycken GDPR
- Information till ledningsgrupp

Q4 okt- dec Uppföljning

- Möte ambassadörer GDPR/Infosäk x1
- Revidering handlingsplan
- Översyn av GDPR/Infosäk organisationen
- Internkontroller
- ISAM Rapport "Ledningsgruppens genomgång"
- GDPR Årsrapport

4 Lokala rutiner

4.1 Avgränsning

Följande beskrivningar utgör de lokala rutinerna för stadsdelsförvaltningen.
Om svar inte ges i denna lokala tillämpningsanvisning så rekommenderas att söka information i:

- ”Tillämpningsanvisningar till stadens riktlinjer för informationssäkerhet” Central tillämpningsanvisning
- ”Riktlinje för informationssäkerhet i Stockholms stad” Central riktlinje
- ”Handbok för informationsklassning” Handbok

Samt ta del av de utbildningar och övrig information som finns på intranätet.
Informationssäkerhet (stockholm.se)

4.2 Inventering och informationsklassning

I enlighet med stadens tillämpningsanvisning för informationssäkerhet som utgår från den internationellt vedertagna informationssäkerhetsstandarden ISO/IEC 27001 så ansvarar respektive chef för att identifiera sin information genom en processdriven informationsinventering.

Process i detta fall kan beskrivas som det arbete inom verksamheten som utförs för att skapa ett externt eller internt mervärde.
Ett exempel på process kan vara dialog med medborgare. Den information som framkommer och de IT-tjänster som används i processen/ dialogen behöver informationsklassas.

Informationsklassning syftar till att bedöma informationens skyddsvärde med hänsyn till konfidentialitet, riktighet och tillgänglighet och görs genom en konsekvensbedömning där man tittar på skadan för individ, verksamhet, ekonomi och samhälle om informationen röjs, förvanskas eller görs otillgänglig.

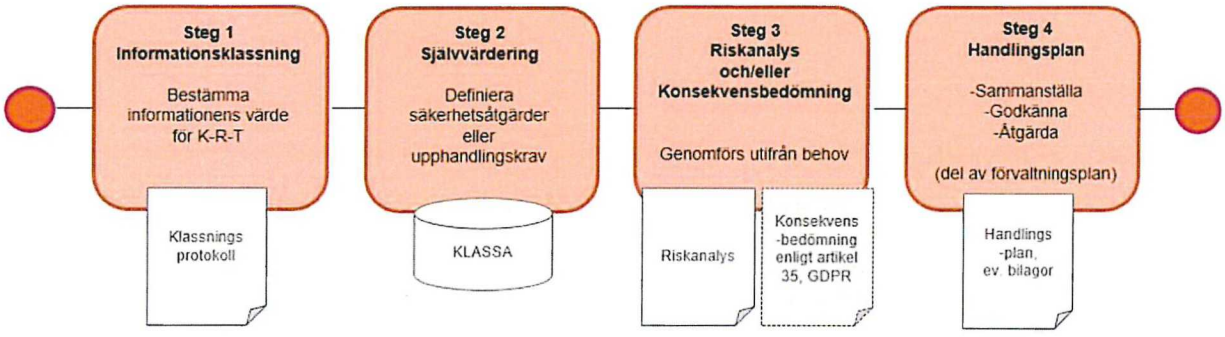
I klassningen bedöms även vilka rättsliga och legala krav som åligger informationen. Personuppgifter utgör en stor del av verksamhetens informationsmängd varpå Dataskyddsförordningen (GDPR) har därmed en stor inverkan på hur verksamheten arbetar med informationssäkerhet och hantering av information.

Personer och kompetenser som bör delta vid informationsklassning är klassningsledare, IT-samordnare, DSO, ISAM, jurist och en eller flera personer som arbetar i och har goda kunskaper om IT-tjänsten och vilken information som behandlas.

Inventering och klassning beskrivs mer utförligt i Stadens Handbok för informationsklassning.
Kortfattat består informationsklassning av följande steg:

- Processdriven informationsinventering (Utförs av chef eller den denna utser, exempelvis ambassadör eller medarbetare med lång erfarenhet).
- Identifierade informationstillgångar delges ISAM som ansvarar för att upprätthålla ett systemförvaltningsregister över alla informationstillgångar.
- Klassningsledare utses av chef/ informationsägare som förbereder klassning genom att samla in de grunduppgifter som efterfrågas i klassningsprotokollet. Se länk: Mall för klassningsprotokoll
- Klassningsledare bjuder in till klassningen
- Workshop 1 informationsklassning, fyll i resterande klassningsprotokoll (bestäm informationens värde) med hjälp av Vägledning för skadebedömning. Se länk: Vägledning skadebedömning
- Diarieför ifyllt klassningsprotokoll (utförs av klassningsledare eller ISAM)
- Workshop 2, fyll i och svara på frågorna i klassa 4 verktyget. Avgör om riskanalys och konsekvensanalys (DPIA) ska utföras.
- Ladda ner handlingsplan som framkommer i Klassa 4 verktyget och utse ansvariga för att införa säkerhetsåtgärder som saknas enligt framkomna krav. Chef/ informationsägare är ytterst ansvarig för att säkerhetsåtgärderna i handlingsplanen implementeras.
- Chef/ informationsägare skriver under klassningsprotokoll.
- Chef/ informationsägare skriver under eventuellt PUB-avtal
- Chef/ informationsägare meddelar driftstart i samband med underskrift
- Klassningsledare ansvarar för att diarieföra underskrivet klassningsprotokoll med tillhörande dokument som exempelvis riskanalys, konsekvensbedömning, PUB-avtal, handlingsplan etc. i samma ärende hos arkivarien.

Nedan bild visar klassningsprocessens olika steg



4.3 Behörighetshantering

En behörighetsstruktur styr vad en användare kan se och göra i en IT-tjänst och ska vara baserat på deras roll i verksamheten.
En viktig princip för en behörighetsstruktur är att endast de användare som behöver tillgång till uppgifterna för att kunna utföra sina arbetsuppgifter ska ges tillgång till dem utifrån lagkrav, verksamhetens behov och roller.
Behörigheter ska dokumenteras av verksamheten och beslutas av informationssägaren.

Chef/Informationsägaren 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 om behörigheter ligger kvar.

I övrigt är det den som ansvarar för informationen, d.v.s. informationsägaren 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 samarbetsytor, det bör kontrolleras åtminstone en gång i halvåret av den som ansvarar för gruppdisken eller funktionsbrevlådan.

4.3.1 Samarbetsorienterade ytor

Generellt bör inte känslig information hanteras eller sparas på samarbetsorienterade ytor där flertalet medarbetare har tillgång till informationen då åtkomstkontroll övertid är svår att upprätthålla.

Ägare av samarbetsytor ansvarar för tilldelning och återkallande av behörigheter för användare. Precis som vid behörighetshantering för IT-tjänster ska tilldelning ske restriktiv och löpande revideras.

Ägaren är ansvarig för att informationen som hanteras på samarbetsytan får finnas där. Vid avslut eller förändring av tjänst ska ägaren överlåta ansvaret för samarbetsytan till sin chef.

4.4 Incidenthantering

Det är viktigt att rapportera in när någonting går fel och att vi lär oss av det. Alla incidenter ska rapporteras i vårt IA-system och vem som helst kan rapportera. Informations- och personsuppgiftsincidenter ska även rapporteras till informationssäkerhetssamordnare och/eller dataskyddsombud.

4.4.1 Förlust av utrustning

Förlust av dator/ mobil/ läsplatta

Ska anmälas till:

- Servicedesk
- IA (stadens incidentrapporteringsverktyg – nås via intranätet)
- Polisen
- Informera din närmaste chef

4.4.2 Förlust av tjänstekort

Ska anmälas till:

- Servicedesk
- IA (stadens incidentrapporteringsverktyg – nås via intranätet)
- Tjänstekortsadministratören på din arbetsplats
- Informera din närmaste chef
- Blir du av med ditt SITHS-kort ska det även anmälas till polisen.

4.4.3 NIS-incidenter

NIS-direktivet ställer höga krav på informationssäkerhet för samhällsviktiga IT-tjänster. Ett krav är att det ska finnas kontinuitetsplaner för alla IT-tjänster som berörs av direktivet. Ett annat krav är att alla it incidenter ska rapporteras till myndigheten för samhällsskydd och beredskap (MSB) inom 6 timmar. Underrätta omgående Enhetschef/tjänstgörande sjuksköterska vid incident. Informationssäkerhet (stockholm.se) Incidentrapportering (stockholm.se)

4.4.4 Personuppgiftsincidenter

En personuppgiftsincident är en oönskad händelse som påverkat sekretessen, integriteten eller tillgängligheten för personuppgiften.
En personuppgiftsincident har till exempel inträffat om uppgifter för en eller flera registrerade personer har blivit förstörda, försvunnit på något sätt eller kommit i orätta händer.
Det spelar ingen roll om det har skett oavsiktligt eller med avsikt.

Varje medarbetare ansvarar för att rapportera risk för, misstanke om eller inträffande av en personuppgiftsincident till närmaste chef. Chef ansvar för att, kontakta dataskyddsombudet, utreda incidenten, och efter samråd med dataskyddsombudet anmäla till IMY samt anmäla det till nämnden. En personuppgiftsincident ska även anmälas i IA.
Chef ansvar för att utreda incidenten, anmäla till IMY samt anmäla det till nämnden. Instruktion finns på intranätet.
Skärholmen Personuppgifter (stockholm.se)

4.4.5 Informationssäkerhetsincidenter

Om information har gått förlorad, är felaktig, är otillgänglig eller blivit åtkomlig för obehörig ska närmste chef omedelbart informeras samt IA-anmälan upprättas.

Vid bedömning av incident så ska följande kriteriemodell användas: Kriteriemodell
Informationssäkersamordnaren ska kontaktas för rådgivning.

Vid allvarliga incidenter ansvarar ISAM att rapportera till stadens CISO.

Exempel på informationssäkerhetsincidenter:

- E-post som skickats till fel mottagare
- Nätfiske – bedräglig e-post, exempelvis falsk avsändare
- Vishing – bedrägligt samtal, exempelvis person som uppger falsk identitet och vill att du loggar in med BankId eller uppge inloggningsuppgifter
- Stöld/ förlust av dator/ mobil/ läsplatta
- IT-tjänst blir otillgänglig
- Om någon obehörig av misstag har hört eller sett känslig information

4.4.6 Utredning Informationssäkerhetsincidenter

Samtliga incidenter ska utredas av ansvarig chef.
Utredning ska dokumenteras i IA-systemet och vara klar inom en månad från rapporteringsdatum.
Syfte med utredning är att kunna vidta säkerhetsåtgärder för att minska sannolikheten att incident uppstår igen samt i lärande syfte för organisationen.

Utredning ska rapporteras till DSO och ISAM.

4.5 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 de 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.

4.6 E-post

4.6.1 Säker e-post

Samtliga medarbetare inom stadsdelsförvaltningen har ett personligt arbetsrelaterat e-postkonto. Det är inte tillåtet att använda sitt arbetsrelaterade e-postkonto i privata ärenden eller skicka e-post mellan sitt privata och arbetskonto.

En av dem vanligaste angreppsmetoderna då det kommer till cyberattacker är att skicka falsk e-post (även kallat nätfiske/ phishing) till anställda.

Dessa e-post meddelanden framstår ofta vid en första anblick som legitima där mottagaren uppmanas klicka på en bifogad fil eller länk. Vanligtvis har meddelandet en brådskande ton i syfte att få mottagaren att flytta fokus från helheten i meddelandet och istället snabbt klicka sig vidare. Det kan röra sig om uppgifter som behöver uppdateras eller viktig information och se ut att komma från exempelvis HR avdelningen.

Det är viktigt att granska inkommen e-post, rapportera misstänkta mejl enligt följande rutin natfiske-och-skadlig-kod och att aldrig klicka på bifogade filer eller länkar om du inte med säkerhet kan säga att meddelandet är legitimt.

Om du ändå har eller är osäker på om du klickat på något skadligt så kontakta omedelbart servicedesk samt informera din närmaste chef.

Att tänka på är att skadliga meddelanden kan skickas med alla typer av kommunikationsmedel som Skype, Zoom, Linkedin, sms etc.

Var noga med att kontrollera att mejl skickas till rätt avsändare. Det finns alltid en risk för misstag som leder till att andra än den avsedda mottagaren får tillgång till information. Dubbelkolla innan du trycker på ”skicka”.

Vidarebefordra aldrig e-post utan att säkerställa att all information som finns i mejlet är lämplig att skicka vidare. Det kan finnas känslig information som inte bör spridas, personuppgifter som mottagaren inte behöver eller så har någon i en tråd av korrespondens uttryckt sig på ett sätt som inte är lämpligt att skicka vidare.

4.6.2 Standardsignatur e-post

Alla medarbetare ska ha en signatur för att underteckna e-postmeddelanden som följer den standard som Stockholms stad har satt upp.

Obligatorisk information i varje medarbetares e-postsignatur:

E-postsignaturen

Förnamn Efternamn
Titel

Förvaltningsnamn eller Verksamhetsnamn
Avdelningsnamn eller Enhetsnamn eller Förvaltningsnamn (om det är en verksamhet)
Adress, postnummer Stockholm
Telefon: 08-508 xx xxx
E-post: fornamn.efternamn@stockholm.se
(fornamn.efternamn@edu.stockholm.se för pedagogiska verksamheter)
xxxxx.stockholm

Stockholms stad

Information om behandling av personuppgifter
Inom Stockholms stad är det respektive nämnd eller styrelsen i det bolag som hanterar personuppgifterna, som är personuppgiftsansvarig. På start.stockholm/dataskydd hittar du information om stadens behandling av personuppgifter.

GDPR-texten på engelska

Handling of personal data
Within the City of Stockholm organisation, each committee or board, is responsible for the handling of all its personal data. You can find information on how the City of Stockholm handles personal data on start.stockholm/dataskydd.

4.6.3 Känslig information i e-post

Att helt undvika behandling av personuppgifter i e-post är inte möjligt i stadsdelsförvaltningens verksamhet.
Alla medarbetare på förvaltningen ska sträva efter att kontinuerligt gallra känsliga uppgifter i vår e-post samt undvika i så lång utsträckning som möjligt att skicka personuppgifter via e-post.

Det är av största vikt att anställda säkerställer och kontrollerar att mejl går till avsedd mottagare och att ingen kompromet terande information följer med innan mejl skickas.

Om det ändå är nödvändigt att skicka personuppgifter i tjänsten:
All e-post inom staden har en grundkryptering.
Inom staden är det godkänt att skicka vad Integritetsmyndigheten klassar som **Personuppgifter** (se nivåer nedan) med standardinställningarna för e-post kontot.

Om integritetskänsliga och känsliga personuppgifter måste skickas ska stadens särskilda krypteringsfunktion användas som beställs av Tieto. Även mottagaren av mejlet måste ha funktionen aktiverad för att det ska fungera.

Särskild krypteringsfunktion beställs av TietoEvery enligt följande instruktion:
Beställ hårdvara och tjänster - Portalen 11800 (stockholm.se)
Aktivera Säker e-post och E-postkryptering

I stadens pedagogiska verksamhet (SPV) finns inte denna möjlighet för närvarande.

Med personuppgifter enligt Dataskyddsförordningen avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person.
Exempel på personuppgifter är

- namn
- adress
- personnummer
- id-kortnummer
- telefonnummer
- foton på personer
- ljudinspelningar
- elektroniska identiteter som IP-adresser och cookies, om de kan kopplas till en fysisk person
- e-postadresser som förnamn.efternamn@företag.se.

Känsliga personuppgifter är uppgifter om

- etniskt ursprung
- politiska åsikter (till exempel uppgift om att du är med i ett visst politiskt parti)
- religiös eller filosofisk övertygelse (till exempel uppgift om att du tillhör en viss religion eller inte tillhör någon religion alls)
- medlemskap i en fackförening

- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter
- biometriska uppgifter som används för att entydigt identifiera en person.

Dessutom finns det personuppgifter som är extra skyddsvärda. De är inte känsliga personuppgifter enligt dataskyddsförordningen men i Sverige har vi valt att ha ett särskilt skydd för våra personnummer, och för de samordningsnummer som man kan få om man inte är folkbokförd i Sverige.
Det finns många andra typer av personuppgifter som är särskilt skyddsvärda. Det kan till exempel vara:

- löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala förhållanden.

4.6.4 Bevarande och arkivering

Meddelanden som sänds eller tas emot via elektronisk post ska behandlas enligt de regler som gäller för allmänna handlingar.

4.6.5 Loggning

All information som hanteras i din e-post loggas och sparas på en extern plats. Allmänheten har möjlighet att begära ut delar eller hela din e-post. Detta föregås av en sekretessprövning innan något lämnas ut.

4.6.6 Vid avslutad anställning

Då du avslutar din anställning ska din e-post, om nödvändigt, övertas av din chef eller den denne utser för att bevaka inkommande e-post. Efter 45 dagar avslutas e-post kontot.

4.7 "Rent skrivbord och ren skärm"

Riktlinjen syftar till att tydliggöra delar av ditt informationssäkerhetsansvar.

I verksamheten hanterar vi återkommande känsliga och sekretessbelagda uppgifter. I ditt tjänsteutövande har du tystnadsplikt vilket innebär att du inte får delge känslig information till dina kollegor förutsatt att de inte behöver den i sitt tjänsteutövande. Det innebär att du även ansvarar för de fysiska och digitala uppgifterna du arbetar med, både då det kommer till överhörning och synlighet. Om man bryter mot denna riktlinje så kan det leda till disciplinära åtgärder.

4.7.1 Obemannad arbetsplats

När arbetsplats eller annan arbetsyta lämnas obevakad, även för en kort stund, ska konfidentiella och/ eller känsliga dokument tas med eller låsas in. Dator/ mobil/ läsplatta ska låsas eller tas med (se avsnitt 4.7.6).

4.7.2 Utskrifter

Vid utskrift av känslig information ska användaren säkerställa att korrekta utskriftsinställningar valts. Pull-print ska alltid användas.
Utskrivet material ska omedelbart avlägsnas från skrivaren.
Skrivare som är placerade i allmänna utrymmen får inte användas för utskrift av känslig information.

4.7.3 Skanning

Vid inskanning av känslig information ska användare säkerställa att korrekta mottagaruppgifter valts. Inskannade dokument ska omedelbart avlägsnas från skrivaren.

4.7.4 Lagring

När dokument och andra handlingar ska lagras är utgångspunkten att endast originalhandlingar ska förvaras. Kopior av dokument som innehåller känslig information ska endast lagras i undantagsfall.
Känslig information ska i första hand förvaras i digital form på avsedd yta för att tillse att åtkomstkontroll och säkerhetskopiering upprätthålls.

4.7.5 Destruering

Känsliga uppgifter ska strimlas genom dokumentförstörare eller slängas i sekretesskärl. Känsliga uppgifter ska hållas inlåsta fram tills att de förstörs.

4.7.6 Ren skärm

Riktlinje syftar till att skydda information som finns på tilldelad utrustning såsom dator, mobiltelefon och läsplatta.
När utrustningen lämnas utan uppsikt ska skärm låsas och tjänstekortet tas ur datorn och tas med.
Inloggning och användning av datorer och annan teknisk utrustning ska alltid kräva inloggningsuppgifter såsom tjänstekort och lösenord/kod. Avvikelser ska skyndsamt rapporteras till chef.
Lösenord/koder får inte förvaras i anslutning till utrustning eller arbetsplats.
Tjänstekort får inte förvaras med datorn.
Förlust av lösenord ska skyndsamt rapporteras till Servicedesk och närmaste chef.

4.7.7 Informationstillgångar receptionen

Förvaltningens reception mottar en stor mängd besökare varje dag.
Receptionen ska vara så ren som möjligt från informationstillgångar.
Informationstillgångar som innehåller personuppgifter eller känslig eller konfidentiell information ska alltid förvaras utom syn- och räckhåll för besökare.

4.7.8 Vid slutet av arbetsdagen

Varje medarbetare ska i samband med arbetsdagens slut säkerställa att känslig information är säker. Dokument ska låsas in eller tas med. Bärbara datorer, mobiltelefoner, kameror och läsplattor får inte lämnas obevakade och ska förvaras i låsbara skåp eller tas med hem. Detta gäller även USB-minnen. Vid arbetsdagens slut ska du logga ut för att säkerhetsuppdateringar m.m. kan ske under kvällen/natten. Vid resa till och från arbetsplatsen ska utrustningen hållas under uppsikt. Personlig utrustning tilldelad av din arbetsgivare får inte delas med någon annan och du är alltid ansvarig för dess skick och säkerhet. (Vid förlust, se 4.4.1)

4.8 Distansarbete

Distansarbete ska alltid godkännas av din chef. Arbete och medförande av utrustning utanför arbetsgivarens lokal innebär en ökad risk för informationssäkerheten som man behöver ta hänsyn till. Utrustningen ska alltid hållas under uppsikt utanför arbetsplatsen och hemmet för att minska risken för stöld eller förlust. Hemmanätverk är godkänt att koppla upp sig emot förutsatt att VPN aktiveras. Det är inte tillåtet att koppla upp sig mot publika wifi-nätverk utan här ska du istället dela internet via din tjänstetelefon. I hemmet ska utrustningen skyddas mot skador som kan uppkomma. Det är viktigt att tänka på tystnadsplikten och säkerställa att ingen obehörig överhör eller kan se informationen du arbetar med.

5 Obligatoriska utbildningar

Stockholm stad har två obligatoriska utbildningar för all personal inom stadsdelsförvaltningen: Utbildningsplattformen

- Grundkurs i dataskydd (obligatorisk att gå årligen)
- Informationssäkerhet för medarbetare (obligatorisk att gå årligen)

För chefer finns också:

- Informationssäkerhet för chefer

För personalgrupper som önskar gå utbildningarna gemensamt ska deltagandet rapporteras till ISAM som följer upp statistiken på antalet som genomför utbildningarna.

6 Kontinuitetsplan

Kontinuitetsplan syftar till att kunna upprätthålla en kritik process vid störning. Det kan exempelvis handla om elavbrott eller att ett kritiskt system inte är tillgängligt när

det behövs. Förvaltningen arbetar kontinuerligt med att identifiera vilka kritiska processer som finns inom verksamheten. Exempel på kritiska processer är de system som faller under NIS-lagstiftningen. Om du identifierar att en IT-tjänst faller under NIS-lagstiftningen vid exempelvis informationsklassning så måste du säkerställa att systemet är upptaget i befintlig kontinuitetsplan, annars ska kontinuitetsplan tas fram. Kontinuitetsplaner kan innehålla känslig information och sparas därför separat från denna lokal tillämpningsanvisning. Vid frågor om vilka kritiska processer som finns i din verksamhet och hur kontinuitetsplanen ser ut kontakta din närmaste chef.

En kontinuitetsplan ska innehålla:

- Reservrutin
- Återställningsrutin
- Återgångsrutin
- Nödvändiga kontaktuppgifter
- Aktiveringsrutiner

7 Registerförteckning dataskydd

Stadsdelsförvaltningen använder verktyget Draft It Privacy för arbetet med registerförteckningen. Ansvarig för att lägga in personuppgiftsbehandlingar i registerförteckning är chef för respektive process/verksamhetsområde (enhetschef). Praktiskt hanteras registerförteckningen av ISAM, men respektive chef är ansvarig för att deras hantering av personuppgifter finns korrekt förtecknade där. Chef vänder sig till ISAM för införande och uppdateringar i registerförteckning.

Registerförteckningen ska uppdateras kontinuerligt vid förändringar. ISAM ska också i samband med uppföljningar årligen skicka ut registerförteckningarna till chef för kontroll.

8 Systemförvaltningsregistret

Stadsdelsförvaltningen har ett register över de system och digitala externa tjänster som den använder. Ansvarig för att lägga in system i registerförteckningen är chef för respektive process/verksamhetsområde (enhetschef). Praktiskt hanteras systemförvaltningsregistret av ISAM, men respektive chef är ansvarig för att deras system finns korrekt förtecknade där. Chef vänder sig till ISAM för införande och uppdateringar i registret. Registret ska uppdateras kontinuerligt vid förändringar. Årligen ska också systemförvaltningsregistret kontrolleras att det är korrekt och uppdaterat.

9 Om PM3 modellen

Staden beskriver syftet med PM3 modellen som ”styrning och samverkan i arbetet med underhåll och utveckling av stadens IT-tjänster”. Vidare går att läsa att ”modellen är obligatorisk för stadens förvaltningar och bolag och stödjer de som på strategisk, taktisk och operativ nivå arbetar med underhåll och utveckling av stadens digitala stöd.”

Majoriteten av de IT-tjänster medarbetarna på stadsdelsförvaltningen använder är sedan tidigare centralt upphandlade och förvaltas hos tredjepartsleverantörer. Stadsdelsförvaltningen arbetar därmed i mycket liten utsträckning med underhåll och utveckling av de IT-tjänster som används i dagsläget.

I syfte att förenkla, förtydliga och effektivisera stadsdelsförvaltningens informationssäkerhetsarbete har de rollbeskrivningar som beskrivs i PM3 modellen frångåtts men beskrivs här nedan för att förenkla eventuell kommunikation med Stockholmstads övriga verksamheter.

Ordlista – PM3 modellen
Objekt = IT-tjänst eller process som innehåller en eller flera IT-tjänster
Objektägare = Huvudansvarig för upphandlad IT-tjänst/ process
Objektägare IT = Huvudansvarig för objektets IT-komponenter
Objektstyrgrupp = Objektägare + Objektägare IT
Objektledare = Utförandeansvarig åt Objektägare
Objektledare IT = Utförandeansvarig åt Objektägare IT

10 Beslut

Denna lokala anvisning för informationssäkerhet vid Skärholmens stadsdelsförvaltning är ett kompletterande dokument till stadens riktlinje för informationssäkerhet.

Beslut fattat den 2024-05-21

Lisa Kinnari
Stadsdelsdirektör