Stockholms stad

Lokal anvisning för informationssäkerhet

Serviceförvaltningen

Beslutad 2023-03-13

Lokal anvisning för informationssäkerhet

Dnr: SF 2022/541

Kontaktperson: Maria Wedenlid

1 Bakgrund

Denna lokala anvisning beskriver roller och organisation för serviceförvaltningens informationssäkerhetsarbete. Dokumentet fastställdes av serviceförvaltningens förvaltningschef den 2023-03-13. Den lokala anvisningen anmäls till servicenämnden.

Den lokala anvisningen revideras årligen och vid behov.

Den lokala anvisningen kompletterar stadens centrala riktlinje och tillämpningsanvisning för informationssäkerhet och dokumenterar hur serviceförvaltningen lokalt och praktiskt tillämpar och arbetar med informationssäkerheten. Den förtydligar hur ansvarsfördelning och roller har anpassats för serviceförvaltningen – vem som ansvarar, vilka stödfunktioner och kontrollfunktioner som finns, och vilka övriga roller som i sitt uppdrag arbetar med skydd av informationstillgångar.

Den lokala tillämpningsanvisningen beskriver också hur serviceförvaltningen systematiskt arbetar med, och följer upp, informationssäkerheten[1].

[1] Med informationssäkerhet menas all information som hanteras inom staden ska hanteras korrekt och i enlighet med regelverk, vara rätt och tillgänglig för dem som behöver använda den, men inte för t.ex. obehöriga personer eller organisationer.

Med information menas all information som du använder i din arbetsvardag för att utföra ditt arbete. Det kan till exempel handla om personuppgifter, information om stadens samhällsservice eller handläggning av ärenden.

Innehållsförteckning

2 Organisation och roller

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

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

2.1 Ledning (styrande)

2.1.1 Servicenämnden

Servicenämnden är ytterst ansvarig för informationen och formellt informationsägare och personuppgiftsansvarig för serviceförvaltningen. Servicenämnden ansvarar för att det finns ett ändamålsenligt och effektivt informationssäkerhetsarbete inom verksamheten samt att stadsövergripande riktlinjer och vägledande dokument för informationssäkerhet följs.

Serviceförvaltningen har i samarbete med stadsledningskontorets juridiska - och personalstrategiska avdelningar utrett personuppgiftsansvar i förvaltningens samtliga processer. Juridiska avdelningens slutsats är att servicenämnden som huvudregel är personuppgiftsbiträde i samtliga processer där uppdrag utförs åt annan nämnd eller bolag. En så kallad personuppgiftsbiträdes instruktion är framtagen och bilagd de serviceavtal som tecknas med stadens förvaltningar och bolag.

Servicenämnden ansvarar för att en ändamålsenlig organisation finns på plats och för att nödvändiga resurser tilldelas samtliga funktioner för att kunna genomföra ett effektivt informationssäkerhetsarbete. Genom detta dokument beskriver och beslutar Servicenämnden hur denna organisation fungerar i praktiken.

Servicenämnden har ett särskilt ansvar för att utse ett data-skyddsombud eller delegera ett sådant beslut till förvaltningschef/bolagschef. Ett dataskyddsombud har utsetts genom beslut inom servicenämnden.

Servicenämnden inhämtar årligen en så kallad GDPR årsrapport från dataskyddsombudet i samband med verksamhetsberättelse och bokslut. Syftet är att Servicenämnden med hjälp av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker för verksamheten. Denna rapport har senast inhämtats för år 2022 och godkänts av Servicenämnden.

I nämndens ansvar ligger även att delegera uppgiften att besluta om informationshantering och regler för detta. Denna uppgift beskrivs i rubrik 2.1.2 samt 2.1.3 i detta dokument.

2.1.2 Förvaltningschef

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

Förvaltningschef ansvarar för att:

- fastställa de lokala tillämpningsanvisningarna och andra övergripande styrdokument för serviceförvaltningen
- 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 serviceförvaltningen, minst genom att tillsammans med informationssäkerhetssamordnare gå igenom väsentlighets- och riskanalysen som är den så kallade ”Ledningens genomgång”
- se till att klassificeringsstruktur och hanteringsanvisningar har fastställts för verksamhetens informationshantering

2.1.3 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, riktlinjer och anvisningar. Ansvaret för informationshanteringen ska ligga så verksamhetsnära som möjligt, och inom serviceförvaltningen innebär det som lägst på verksamhetsområdesnivå. Chefen kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Chefer inom serviceförvaltningen ansvarar för att:

- årligen se till att samtliga medarbetare och konsulter genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- följa upp och utreda de incidenter som verksamheten anmäler i IA, samt att kontakta dataskyddhandläggaren som kontaktar dataskyddsombud och/eller informationssäkerhetssamordnare vid incidenter som rör personuppgifter eller andra informationssäkerhetsfrågor
- säkerställa att registervård genomförs inom sin verksamhet och att uppdatera och följa upp serviceförvaltningens behandlingsregister över hantering av personuppgifter. Serviceförvaltningen har inkluderat behandlingsregistret i förvaltningens hanteringsanvisningar. Hanteringsanvisningarna utgår från stadsarkivets informationsklassificering utifrån dataskyddsförordningen och offentlighets- och sekretesslagen. Det innebär att majoriteten av de personuppgiftsbehandlingar som förekommer inom förvaltningen finns dokumenterade.
- de inköp/upphandlingar som chef beslutar om följer gällande lagar vad gäller informationshantering, samt stadens och serviceförvaltningens styrdokument
- informationsinventering är gjord av den egna verksamheten med stöd från informationssäkerhetssamordnare, dataskyddshandläggare och arkivfunktioner
- 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.

2.1.4 Objektledare

En objektledare[2] ansvarar för drift och förvaltning av en it-tjänst. En objektledare är utsedd för samtliga digitala tjänster hos serviceförvaltningen som förvaltningen är objektägare för.

Vilka som tilldelats rollen objektledare inom förvaltningen framgår i den förteckning över verksamhetens informationstillgångar som upprättas av arkivhandläggaren. Förteckningen är en del av hanteringsanvisningarna.

När det gäller de it-tjänster där drift sköts på entreprenad eller av annan förvaltning, är verksamhetens (personuppgiftsansvarig) objektledare ansvarig för tjänsten i relation till den beställda (personuppgiftsbiträde) tjänsten och fungerar då som lokalt ansvarig för hur systemet används i verksamheten. I de fall både drift och verksamhet finns inom serviceförvaltningen förekommer ibland rollen objektledare specifikt för tjänstens drift.

[2] För rollbeskrivning se stadens metodstöd för Pm3

Objektledarens ansvar är att:

- tillse att informationstillgången är klassad och att handlingsplaner från klassning tas om hand för systemet
- se till att förvaltningsplan enligt pm3 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, dokumentera detta och se till att reglerna är kända av medarbetarna
- utse övriga nödvändiga funktioner inom it (t.ex. objektspecialist).

2.2 Stödjande och uppföljande

Serviceförvaltningen har tillsammans med kulturförvaltningen, idrottsförvaltningen, arbetsmarknadsförvaltningen, kyrkogårdsförvaltningen samt stadsarkivet förstärkt förvaltningarnas arbete med dataskyddsfrågor genom en gemensam konsult som ska utgöra dataskyddsombud för berörda nämnder. Nämnderna har tecknat avtal med Combitech AB för dataskyddsombud från och med 1 juni 2022.

I avtalet beskrivs att respektive förvaltning har olika interna organisationer för arbetet med dataskydd och informationssäkerhetsarbete, men samtliga har utsedda kontaktpersoner som driver det interna arbetet med frågorna och som konsulten ska stödja.

Inom serviceförvaltningen består den interna organisationen av de fyra funktionerna

- Informationssäkerhetssamordnare,
- dataskyddshandläggare,
- arkivhandläggare och
- upphandlingsjurist.

Gruppen är förvaltningens interna nätverk för informations- och dataskyddsfrågor. Funktionerna är också chefers och medarbetares primära kontaktpersoner vid frågor som kan uppstå inom dataskydd.

Dessa funktioner är de som primärt har kontakt med dataskyddsombudet i uppkomna frågor och för planering av informations- och utbildningsinsatser, samt vid framtagande av rutiner, i enlighet med ordinarie linjeuppdrag.

Dessa funktioner är dataskyddsombudets kontaktpersoner vid upprättande av förvaltningens GDPR årsrapport

Funktionerna är också dataskyddsombudets primära kontaktpersoner vid frågor som kan uppstå inom dataskydd.

2.2.1.1 Serviceförvaltningens interna rutiner gentemot externt dataskyddsombud

Förvaltningens dataskyddshandläggare utgör den primära kontaktyta för förvaltningens chefer och medarbetare i frågor som rör dataskydd och personuppgiftsbehandling.

Uppkomna frågor prövas i första hand av denna funktion, enskilt eller i samråd med övriga funktioner inom grupperingen. Samtliga funktioner inom grupperingen har fri tillgång till att kommunicera med upphandlat dataskyddsombud utifrån sina respektive funktioner.

I frågor som dataskyddsombud ska utreda eller hantera fungerar funktionerna var och en som beställare av detta.

Ansvarig för avtalet med externt dataskyddsombud är administrativ chef, som även samverkar med övriga förvaltningar inom avtalet kring det gemensamma uppdraget och uppföljning av avtal, aktuella frågor och tidsrapportering med mera.

2.2.2 Dataskyddsombud (DSO)

Verksamhetens dataskyddsombud utses formellt av Servicenämnden.
I syfte att utveckla och säkra kompetens, rutiner, arbetssätt i frågor som rör dataskyddsförordningen och personuppgiftshantering har förvaltningen etablerat ett samarbete med fem av stadens fackförvaltningar.

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

Dataskyddsombudet ska kunna agera självständigt och oberoende i sitt uppdrag och ska därför inte utföra det operativa arbetet. DSO har ett nära samarbete och kontakt med ISAM och dataskyddshandläggare, 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 ges möjlighet att övervaka genomförandet av dem
- vara kontaktperson för nationell tillsynsmyndighet och samverka med denna i initiala förhandssamråd och hantering av personuppgiftsincidenter
- tillsammans med dataskyddshandläggaren hantera personuppgiftsincidenter inom förvaltningen, ansvara för bedömning och anmälan till IMY efter samråd med förvaltningschef
- vägleda, informera och ge råd till förvaltningens kontaktpersoner i frågor om dataskyddsförordningen och andra regler inom dataskyddsområdet
- vägleda, informera och ge råd i utformningen av korrekta och relevanta skyddsåtgärder för person- och integritetsskydd så att behandlingen är förenlig med förordningen
- vägleda förvaltningens kontaktpersoner i utredning av misstänkta dataintrång
- övervaka förvaltningarnas efterlevnad av dataskydds-förordningen samt övriga dataskyddsbestämmelser
- granska hur väl dataskyddsförordningen efterlevs och skriver dataskyddsombudets årsrapport till förvaltningens verksamhetsberättelse
- övervaka och ge råd i samband med genomförandet av konsekvensbedömningar avseende dataskydd
- aktivt informera om förändringar och uppdateringar i regelverk och annat inom dataskyddsområdet till förvaltningens kontaktpersoner

2.2.3 Informationssäkerhetssamordnare (ISAM)

Serviceförvaltningens ISAM är utsedd av förvaltningschefen.

ISAM ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet och att stötta samt vägleda hela förvaltningens verksamhet. ISAM ska arbeta utifrån förvaltningschefens 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.
- fungera rådgivande gentemot förvaltningens objektledare, i projekt samt till ansvariga för upphandling.
- samverka med andra närliggande ansvarsområden och roller
- stödja linjeverksamheten när det gäller det strategiska arbetet, kartlägga information, informationsklassificera den, hantera incidenter samt att utbilda medarbetare och sprida kunskap om lokala rutiner.
- bevaka förändringar i lagstiftningen och händelser i omvärlden och informera om detta
- genomföra uppföljning/revision av det lokala informationssäkerhetsarbetet.
- årligen upprätta rapporten ”VP-anvisning: Ledningens genomgång”

2.2.4 Dataskyddshandläggare

Dataskyddshandläggaren utgör informationssäkerhetssamordnarens och dataskyddsombudets länk till och från chefer och medarbetare i verksamheterna.

Dataskyddshandläggarens uppgifter är bland annat:

- Att vara verksamhetsområdenas kontaktperson gentemot DSO och ISAM
- Att sprida information om de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd.
- Att stödja enheterna vid rapportering av personuppgiftsincidenter samt informationssäkerhetsincidenter.
- Att säkerställa att informationssäkerhetskrav och GDPR-krav (t.ex. tecknande av personuppgiftsbiträdesavtal) uppfylls vid förvaltningens egna upphandlingar.
- Att vara delaktig i utvecklingsarbetet av konsekvensbedömningar, handlingsplaner, riskanalyser samt förvaltningsplaner.

2.2.5 Arkivansvarig och arkivhandläggare

Arkivorganisationen har en viktig funktion i förvaltningens informationssäkerhetsarbete. Arkivansvarig, arkivhandläggare och arkivkonsult, deltar aktivt i serviceförvaltningens informationssäkerhetsarbete och i dess inventeringar av informationstillgångar – både digitala och fysiska.

Arkivansvarig och arkivhandläggare och arkivkonsult är ansvariga för framtagandet av de dokument där hantering och arkivering av Servicenämndens samtliga informationstillgångar beskrivs, det vill säga serviceförvaltningens hanteringsanvisningar och övrig arkivdokumentation.

Arkivorganisationens roller beskrivs i serviceförvaltningens arkivbeskrivning.

2.2.6 Upphandlingsjurist

Upphandlingsjuristen arbetar inom verksamhetsområde upphandling och inköp. Som en del i det ordinarie uppdraget ingår även att säkerställa dataskyddsfrågorna inom verksamhetsområde upphandling och inköps olika uppdrag.

Upphandlingsjuristen utgör den primära kontaktytan för verksamhetsområdets chefer och medarbetare i frågor som rör dataskydd och informationssäkerhet vid upphandlingar och avtalsförvaltning.

- Att säkerställa informationssäkerhetskrav och krav som ställs i GDPR (PUB-avtal)vid förvaltningens upphandlingar
- Att stödja verksamhetsområdets medarbetare i frågor som rör dataskydd och informationssäkerhet vid centrala upphandlingar och avtalsförvaltning.

2.3 Övriga funktioner

2.3.1 Medarbetare

Medarbetare inom serviceförvaltningen 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.

Nyanställda medarbetare godkänner stadens generella användarkontrakt i samband med sin första inloggning i stadens it-miljö.

2.3.2 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 informationssäkerhetssamordnare och verksamhetsområdeschefer.

2.3.3 Arkivredogörare

Arkivredogörarna är en del av förvaltningens arkivorganisation och utses inom varje verksamhetsområde till hjälp för arkivhandläggaren. Rollen innebär bland annat ett ansvar att ta emot och förmedla vidare information från arkivhandläggare och arkivkonsult inom den egna verksamheten. Arkivredogörare ska också delta i arbetet med att hålla hanteringsanvisningar och behandlingsregister uppdaterade samt informera arkivhandläggare och arkivkonsult om eventuella förändringar i verksamhetens informationshantering som kan påverka till exempel hanteringsanvisningar eller behandlingsregister.

2.3.4 It-funktioner

Roller med denna expertfunktion deltar aktivt i det operativa arbetet genom att t.ex. delge sin expertkunskap vid upphandlingar, införande av system/produkt, informationsklassningar och drift. It-funktioner innebär i serviceförvaltningens verksamhet rollerna it-strateg och it-tekniker.

2.3.5 Särskild systemspecialist/objektspecialist

Objektspecialister ansvarar för att utföra det verksamhetsnära operativa arbetet samt avrapportera till objektledaren. Rollen objektspecialist är ett samlingsnamn och bemannas av t ex: superanvändare, systemförvaltare med verksamhetsfokus, verksamhetsutvecklare och processutvecklare. I större objekt kan det vara effektivt att utse produktansvariga om verksamhetskomponenterna rör många olika verksamheter.

Inom serviceförvaltningen 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 Årshjul

Serviceförvaltningen har inte ett fastställt årshjul för arbetet med informationssäkerhet, utan planerar arbetet utifrån väsentlighets- och riskanalysen som genomförs i samband med verksamhetsplaneringen och framtagande av intern kontrollplan.

I samband med verksamhetsberättelse och bokslut tar förvaltningen del av dataskyddsombudets årsrapport och stor hänsyn tas till eventuella rekommendationer till personuppgiftsansvarig som lämnas i rapporten.

4 Serviceförvaltningens befintliga rutiner

Här listas en del övriga lokala rutiner som serviceförvaltningen har på plats som hjälp i arbetet med informationssäkerhet och dataskydd.

Rutin	Beslutad av	Förvarad
Stödmaterial till dig som chef inför bedömning av önskemål om att delvis arbeta hemma	SLK, personalstrategiska avdelningen, 2021-09-16	
Arbeta hemifrån	HR-konsult	Samarbets-ytan
Riktlinje för hantering av personuppgifter i system på serviceförvaltningen.	Förvaltningschef, 2021-03-09	e-Dok
Informationshantering vid start och avslut av gruppdisk, funktionsbrevlådor och samarbetsytor	Administrativ chef	
Arkivbeskrivning och Hanteringsanvisningar och behandlingsregister för Servicenämnden	Administrativ chef serviceförvaltningen	Samarbets-ytan
Hantera personuppgiftsincident	Dataskyddshandläggare, 2022-02-10	Samarbets-ytan
Hantera begäran om registerutdrag	Administrativ chef, 2022-12-15	Samarbets-ytan

5 Rutiner serviceförvaltningens ska ta fram under verksamhetsår 2023

Här listas de rutiner som förvaltningen har planerat att ta fram alternativt revidera under verksamhetsåret som behövs för ett fullgott informationssäkerhetsarbete.

Identifierat behov	Ansvarig
Incidenthanteringsrutin	ISAM
Uppdatering av hanteringsanvisningar och behandlingsregister	Administrativ chef

Charlotte Goliath

Elektroniskt undertecknad av Charlotte Goliath
Datum: 2023.03.13 17:02:25 +01'00'