Lokal anvisning för informationssäkerhet

Kungsholmens stadsdelsförvaltning

Beslutad 29 november 2023

Lokal anvisning för informationssäkerhet

Dnr: KUNG 2023/163

Kontaktperson: Frida Mattsson

Varför behövs en lokal anvisning?

I grunden är det ett lagkrav att kunna redovisa hur verksamheten arbetar med och organiserar sitt informationssäkerhetsarbete, och det står i de nya tillämpningsanvisningarna för informationssäkerhet att en lokal anvisning ska finnas. Följande står i tillämpningsanvisningarna:

”Förvaltningschef ska för nämndens räkning fastställa en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas i den egna verksamheten. Den lokala anvisningen ska gås igenom årligen och revideras vid behov. Den lokala anvisningen ska minst beskriva ansvarsfördelning inom den egna informationssäkerhetsorganisationen (roller och mandat), vilken effekt informationssäkerhetsarbetet ska leda till lokalt, specifik lagstiftning som gäller för verksamhetens informationshantering samt hur arbetet följs upp lokalt.”
Se sid 8 i Tillämpningsanvisningar för informationssäkerhet

1 Bakgrund

Denna lokala anvisning beskriver roller och organisation för Kungsholmens stadsdelsförvaltnings informationssäkerhetsarbete. Dokumentet fastställdes av förvaltningschef för stadsdelsnämndens räkning den 29 november 2023.

Den lokala anvisningen uppdateras årligen enligt årshjulet.

Den lokala anvisningen kompletterar stadens centrala riktlinje och tillämpningsanvisning för informationssäkerhet och dokumenterar hur Kungsholmens stadsdelsförvaltning lokalt och praktiskt tillämpar och arbetar med informationssäkerheten. Den förtydligar hur ansvarsfördelning och roller har anpassats för stadsdelsförvaltningen – 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 stadsdelsförvaltningen systematiskt arbetar med, och följer upp, informationssäkerheten.

Innehållsförteckning

2 Organisation och roller

Kungsholmens stadsdelsförvaltnings 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 Kungsholmens stadsdelsnämnd

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

Stadsdelsnämnden ansvarar för att en ändamålsenlig organisation finns på plats och för att nödvändiga resurser tilldelas samtliga funktioner för att kunna genomföra ett effektivt informationssäkerhetsarbete. I denna lokala anvisning beskrivs hur denna organisation fungerar i praktiken.

Stadsdelsnämnden har ansvar att utse ett dataskyddsombud. Stadsdelsnämnden kan även delegera uppgiften till förvaltningschef, som då ska anmäla sitt beslut till nämnden.

Stadsdelsnämnden 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 2022 och godkänts av stadsdelsnämnden.

I stadsdelsnämndens 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 stadsdelsförvaltningen.
- Att utse en 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 i stadsdelsförvaltningen, minst genom att inhämta den årliga rapporten ”VP-anvisning: Ledningens genomgång” från informationssäkerhetssamordnaren.
- Att 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 och riktlinjer. Ansvaret för informationshanteringen ska ligga så verksamhetsnära som möjligt, och inom stadsdelsförvaltningen innebär det som lägst på enhetschefsnivå. Chefen kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Chefer inom stadsdelsförvaltningen ansvarar för:

- Att se till att samtliga medarbetare och konsulter som hanterar stadens information genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd årligen.

- Att 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.
- Att säkerställa att registervård genomförs inom chefens verksamhet och att uppdatera och följa upp stadsdelsförvaltningens register över hantering av personuppgifter (det vill säga registerförteckningen).
- Att de inköp/upphandlingar som chef beslutar om följer gällande lagar vad gäller informationshantering, samt stadens och stadsdelsförvaltningens styrdokument.
- Att informationsinventering är gjord av den egna verksamheten med stöd från informations-säkerhetssamordnare och arkivfunktioner. Att se till att informationstillgångar är klassade och att verksamhetens it-tillgångar har en utsedd objektledare.
- Att ta fram lokala rutiner för den egna verksamheten vid behov.

2.1.4 Processägare

All informationshantering i stadsdelsförvaltningen 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.

2.1.5 Objektledare

En objektledare ansvarar för drift och förvaltning av en IT-tjänst. En objektledare är utsedd för samtliga digitala tjänster hos stadsdelsförvaltningen.

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

När det gäller de IT-tjänster där drift sköts på entreprenad eller på 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 stadsdelsförvaltningen förekommer ibland rollen objektledare specifikt för tjänstens drift.

Objektledarens ansvar är:

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

2.2 Stödjande och uppföljande

2.2.1 Informationssäkerhetssamordnare (ISAM)

Stadsdelsförvaltningens ISAM är utsedd av förvaltningschefen. Nu tjänstgörande ISAM utsågs 2023-02-23.

ISAM ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet och att stötta samt vägleda hela stadsdelsförvaltningens 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.

- Att fungera rådgivande gentemot förvaltningens objektledare, i projekt samt till ansvariga för upphandling.
- Att samverka med andra närliggande ansvarsområden och roller.
- Att stödja linjeverksamheten när det gäller det strategiska arbetet, kartlägga information, informationsklassificera den, hantera incidenter samt att utbilda medarbetare och sprida kunskap om lokala rutiner.
- Att bevaka förändringar i lagstiftningen och händelser i omvärlden.
- Att genomföra uppföljning/revision av det lokala informationssäkerhetsarbetet.

2.2.2 Dataskyddsombud (DSO)

Nu tjänstgörande dataskyddsombud anmäldes till nämnd/styrelse datum 2018-04-19.

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, 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.

2.2.3 ILS-samordnare

Stadsdelsförvaltningens ILS-samordnare samordnar uppföljningen och beredningen av nämndens ILS-arbete. ILS-samordnaren ska aktivt arbeta för att informationssäkerhet är med och följs upp i stadsdelsförvaltningens väsentlighets- och riskanalys samt införliva

informationssäkerheten i verksamhetsplanen med stöd från informationssäkerhetssamordnaren.

2.2.4 Arkivansvarig och arkivarie

Övergripande arkivfunktioner har en viktig funktion i stadens informationssäkerhetsarbete. Arkivfunktionen, arkivansvarig och arkivarie deltar aktivt i stadsdelsförvaltningens informationssäkerhetsarbete och i dess inventeringar av informationstillgångar – både digitala och fysiska.

Arkivansvarig och arkivarier är stödfunktioner i framtagandet av de dokument där hantering och arkivering av stadsdelsnämndens samtliga informationstillgångar beskrivs, dvs stadsdels-förvaltningens hanteringsanvisningar och övrig arkivdokumentation.

Arkivfunktionernas roller beskrivs i stadsdelsförvaltningens arkivinstruktion/arkivorganisation.

2.3 Övriga funktioner

2.3.1 Medarbetare

Medarbetare inom stadsdelsförvaltningen 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. Alla medarbetare får regelbunden påminnelse om sina skyldigheter vad gäller informationssäkerhet och dataskydd.

2.3.2 It-funktioner

Roller med denna expertfunktion deltar aktivt i det operativa arbetet genom att t.ex. delge sin expertkunskap vid upphandlingar, införande av system/produkt, informationsklassningar och drift. It-funktioner innebär i stadsdelsförvaltningens verksamhet rollen IT-samordnare.

2.3.3 Objektspecialist

Inom stadsdelsförvaltningen 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.

- Sociala system
- ILS web
- BER (barn och elevregistret)
- eDok
- Agresso

2.3.4 Dataskyddshandläggare

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

Dataskyddshandläggarens uppgifter är bland annat:

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

3 Årshjul

- Ledningsgruppens genomgång
- Revidering av de lokala anvisningarna för informationssäkerhet
- Arbetet med VoR och RSA.

- Uppföljningar av informationssäkerhet för medarbetare
- Uppföljningar av registret över personuppgiftsbehandlingar.
- Uppföljningar av informationsklassningar i våra system

4 Rutiner och praktiskt arbete

4.1 Incidenthantering

4.1.1 Personuppgiftsincidenter

En personuppgiftsincident är varje avsiktlig eller oavsiktlig händelse där det finns risk för att personuppgifter används på otillåtet sätt, förloras, ändras eller bli tillgängliga för någon obehörig, till exempel vid dataintrång, felskickade mail eller borttappade telefoner.

Personuppgiftsincidenter rapporteras i incidentrapporteringssystemet IA. Allvarliga incidenter rapporteras till Integritetsskyddsmyndigheten (IMY) inom 72 timmar.

4.1.2 NIS-incidenter

Nis handlar om nätverks- och informationssäkerhet vilket ställer krav på säkerhetsåtgärder och incidentrapportering när digitala tjänster inte fungerar och får konsekvenser för hälso-och sjukvården. Incidenten ska rapporteras till MSB (Myndigheten för samhällsskydd och beredskap) **inom sex timmar** från det att en incident har upptäckts.
Ansvarig för att göra anmälan till MSB är ISAM, ISAM sammankallar berörda funktioner för hantering av incidenten.

4.1.3 Behörighetshantering

Identitet och åtkomst är ett av de högst prioriterade områdena i stadens informationssäkerhetsarbete. Huvudprincipen för hur identitet och åtkomst ska tilldelas utgår från att användare ska ha den åtkomst som krävs för att arbetet ska kunna utföras på ett lämpligt och riktigt sätt.
Behörighetshantering ska därmed ske på ett informationssäkert sätt. Alla chefer, objektspecialister alt. objektledare kontrollerar (lägger

till och tar bort) behörigheter på sina respektive system/tjänster. Regelbunden hantering av behörigheter för resursägare gällande funktionsbrevlådor, gruppdiskar, tjänstekort, passerbrickor, IT-utrustning, IT-administratörsrättigheter, program-licenser m.m.

Underskriftens äkthet valideras här: https://underskriftpas.stockholm.se/validera

Undertecknad av
Ann-Christine Hansson

Datum
2023-11-29 12:19:36

Elektronisk underskrift

underskrift.stockholm.se