Lokal anvisning för informationssäkerhet

Stockholms Stadshus AB

Beslutad 12 september 2023
Reviderad [ ]

Lokal anvisning för informationssäkerhet

Dnr: SSAB 2022/160

Kontaktperson: Ingrid Storm

1 Bakgrund

Denna lokala anvisning beskriver roller och organisation för Stockholms Stadshus ABs informationssäkerhetsarbete. Dokumentet fastställdes av vice vd för Stockholms Stadshus AB räkning den 12 september 2023.

Den lokala anvisningen uppdateras vid behov årligen i samband med framtagande av verksamhetsplan.

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

Innehållsförteckning

2 Organisation och roller

Stockholms Stadshus ABs 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 Koncernstyrelsen för Stockholms Stadshus AB

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

Koncernstyrelsen 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.

Koncernstyrelsen har ansvar att utse ett dataskyddsombud. Koncernstyrelsen kan även delegera uppgiften till VD/Vice VD.

Koncernstyrelsen inhämtar årligen en så kallad GDPR årsrapport från dataskyddsombudet. Syftet är att koncernstyrelsen 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 koncernstyrelsen.

I koncernstyrelsen 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 VD/Vice VD

VD/Vice VD är koncernstyrelsens representant när det gäller de övergripande lednings- och styrningsfrågorna.

VD/Vice VD ansvarar för:

- Att fastställa de lokala tillämpningsanvisningarna och andra övergripande styrdokument för Stockholms Stadshus AB.
- 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 Stockholms Stadshus AB, minst genom att ta del av den rapportering som bolaget redovisar i anvisat system samt övrig rapportering om informationssäkerhet/GDPR som sker till koncernstyrelsen samt stämma av med bolagets informationssäkerhetssamordnare.
- Att se till att klassificeringsstruktur och hanteringsanvisningar har fastställts för verksamhetens informationshantering.

2.1.3 Vice VD

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 Stockholms Stadshus AB innebär det som lägst på vice VD nivå. Vice VD kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Vice VD inom Stockholms Stadshus AB ansvarar för:

- Att se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd årligen.
- Att följa upp och utreda de incidenter som verksamheten anmäler, samt att kontakta dataskyddsombud och/eller informationssäkerhetssamordnare vid incidenter som rör personuppgifter eller andra informationssäkerhetsfrågor.

- Att säkerställa att registervård genomförs och att uppdatera och följa upp Stockholms Stadshus ABs register över hantering av personuppgifter (det vill säga registerförteckningen).
- Att inköp/upphandlingar följer gällande lagar vad gäller informationshantering, samt stadens och Stockholms Stadshus ABs styrdokument.
- Att informationsinventering är gjord av den egna verksamheten med stöd från informations-säkerhetssamordnare och arkivfunktioner. Att se till att viktigare 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

Stockholms Stadshus AB är en verksamhet med få anställda och använder i princip enbart stadens obligatoriska system. Bolaget är inte systemägare till något system. Vice VD på Stockholms Stadshus AB är ansvarig för all informationshantering bolaget. En ansvarig person 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 bolagets klassificeringsstruktur. Den person 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[1] ansvarar för drift och förvaltning av en it-tjänst.

Bolaget har en liten organisation som framförallt använder sig av centralt upphandlade tjänster/system. För dessa har system/avtalsägare i Stockholms stad gjort konsekvensanalyser samt i relevanta fall tagit fram centrala PUB-avtal (exempelvis inom IT-tjänster, företagshälsovård, rekryteringssystem, statistiktjänster m.m.).

I sin dagliga hantering använder bolaget bara ett system, Visma Agda, som inte tillhandahålls genom Stockholms stad. Enligt DSO:s bedömning är det i första hand detta system bolaget bör överväga att göra en informationsklassning för. Avtalsägare för detta systemstöd är

[1] För rollbeskrivning se stadens metodstöd för Pm3

dotterbolaget Stockholm Business Region och en gemensam informationsklassning av systemet genomförs 2023.

Stockholms Stadshus AB har således inga utsedda objektledare för samtliga digitala tjänster. Hanteringen av informationen i systemen regleras i hanteringsanvisningar samt strategi för bevarande av digital information.

2.2 Stödjande och uppföljande

2.2.1 Informationssäkerhetssamordnare (ISAM)

Stockholms Stadshus ABs ISAM utses av vice VD. Nu tjänstgörande ISAM utsågs datum 2020-04-22.

ISAM ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet och att stötta samt vägleda hela bolagets verksamhet. ISAM ska arbeta utifrån vice VDs 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 bolagets medarbetare, 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.
- Att vara kontaktperson gentemot DSO.
- Att sprida information om de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd.
- Att samordna och sammanställa verksamhetens registerförteckning samt att denna uppdateras årligen.
- Att stödja verksamheten vid rapportering av personuppgiftsincidenter samt informationssäkerhetsincidenter.

- Att säkerställa att informationssäkerhetskrav och GDPR-krav (t.ex. tecknande av personuppgiftsbiträdesavtal) uppfylls vid upphandlingar.
- Att vara delaktig i utvecklingsarbetet av konsekvensbedömningar, handlingsplaner och riskanalyser.

2.2.2 Dataskyddsombud (DSO)

Bolagets dataskyddsombud upphandlas externt, nuvarande avtal är med JP Infonet AB. Nu tjänstgörande dataskyddsombud anmäldes till Integritetsskyddsmyndigheten (IMY) 2020-08-20 och lämnar årsrapport till koncernstyrelsen årligen i enlighet med centrala anvisningar.

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.
- Årligen ta fram en GDPR årsrapport till bolagets styrelse.

2.2.3 ILS-samordnare

ISAM/administrativ chef är den som arbetar aktivt för att informationssäkerhet är med och följs upp i bolagets väsentlighets- och riskanalys samt införlivar informationssäkerheten i verksamhetsplanen. Bolagets ILS-samordnare säkerställer att ISAM har rätt behörigheter/kunskap i systemet för att genomföra uppföljningen.

2.2.4 Arkivansvarig och arkivarie

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

Arkivansvarig är bolagets administrativa chef och arkivkonsult är konsult från stadsarkivet. Dessa roller är stödfunktioner i framtagandet av de dokument där hantering och arkivering av koncernstyrelsens samtliga informationstillgångar beskrivs, dvs bolagets hanteringsanvisningar och övrig arkivdokumentation.

Arkivfunktionernas roller beskrivs i bolagets arkivbeskrivning.

2.3 Övriga funktioner

2.3.1 Medarbetare

Medarbetare inom bolaget 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 It-funktioner

Stockholms Stadshus AB har en liten verksamhet och saknar egen IT-chefskompetens. IT-hanteringen sköts av bolagets administrativa chef med hjälp av administratör. För vissa uppgifter inhämtas stöd från stadsledningskontorets IT-support funktion.

2.3.3 Särskild systemspecialist/objektspecialist

Inom bolaget 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. Detta gäller exempelvis systemen eDok, ILS, Agresso, Ocra osv.

2.3.4 Dataskyddshandläggare

Dataskyddshandläggaren utgör informationssäkerhetssamordnarens och dataskyddsombudets länk till chefer och medarbetare i verksamheterna. På Stockholms Stadshus AB som har en liten verksamhet finns inga dataskyddshandläggare, uppgifter hanteras av informationssäkerhetssamordnare tillika administrativ chef.

3 Nätverk och grupper

Bolagets informationssäkerhetssamordnare bjuds regelbundet in och deltar vid stadens nätverksträffar, utbildnings- och informationsträffar för informationssäkerhetssamordnare som leds av stadsledningskontorets funktion för stadsövergripande informationssäkerhet.

Bolagets externa dataskyddsombud bjuds in till stadens dataskyddsombudsnätverk.

4 Årshjul

Planering och uppföljning av bolagets arbete med informationssäkerhet ingår i väsentlighets- och riskanalys med tillhörande internkontrollplan som tas fram i samband med budget/verksamhetsplan och följs upp i samband med årsredovisning/verksamhetsberättelse.

Bolaget arbetar även med informationssäkerhet i samband med risk- och sårbarhetsanalys enligt stadens anvisningar (oktober respektive december vartannat år) samt vid framtagandet av verksamhetsplan, verksamhetsberättelse i början/slutet av verksamhetsåret.

Registerförteckningen över bolagets behandlingar av personuppgifter uppdateras vid årlig revidering eller vid verksamhetsförändringar/införande av nya personuppgiftsbehandlingar/upphandlingar/tecknande av PUB-avtal.

Utbildning av medarbetare sker årligen via e-utbildning och vartannat år via intern/extern utbildning av samtliga medarbetare i informationssäkerhet respektive dataskydd. Bolaget tar även del av

de utbildningsinsatser som anordnas av stadsledningskontorets funktion för stadsövergripande informationssäkerhet.

Uppdateringar av lokala rutindokument sker vid behov eller i enlighet med anvisningar från staden. De dokument som staden publicerar på intranätet kring informationssäkerhet kommuniceras ut i hela bolaget.

5 Rutiner och praktiskt arbete

- I staden finns en riktlinje för informationssäkerhet.
- Stockholms Stadshus AB har en framtagen rutin för hantering av informationssäkerhetsincidenter samt allmänna informationssäkerhetsrutiner
  Ny gemensam/Personal/Interna rutiner SSAB\Dokument för anställda att ta del av vid behov\Informationssäkerhet
- Här finns bolagets registerförteckning.
  Styr- och stöddokument\GDPR\Registerförteckning
- Här finns rutin för registrerades rättigheter vid begäran om registerutdrag
  Styr- och stöddokument\GDPR\Registerutdrag - begäran och hantering
- Här finns Rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen
  Styr och stöddokument\GDPR\OSL vs GDPR
- Här finns info för nyanställda att ta del av
  Personal\interna rutiner\Nyanställd
- Stockholms Stadshus AB är personuppgiftsansvarig för de personuppgifter som hanteras inom bolaget. Här finns bolagets integritetspolicy. Bolaget har ett externt dataskyddsombud.
- Dessa två kurser är obligatoriska för alla medarbetare och ska genomföras årligen.
  Informationssäkerhet för medarbetare i staden (nytt fönster)
  Grundkurs i dataskydd (nytt fönster)
- Här finns rutiner för att påbörja och avsluta anställning, behörighetshantering.
  Personal\Interna rutiner SSAB
- Vid behov av ytterligare vägledning finns mer information också att nå via stadens intranät:
  Informationssäkerhet (stockholm.se)