Lokal anvisning för informationssäkerhet

Stockholm Business Region

Beslutad: 2023-10-27
Reviderad: 2024-11-05

Lokal anvisning för informationssäkerhet

Dnr: SBR 2024/249

Kontaktperson: Emil Brynielsson, ISAM

1 Bakgrund

Stadens ledningssystem för informationssäkerhet sätter ramarna för hur staden styr, genomför och följer upp informationssäkerhets-arbetet. Ledningssystemet för informationssäkerhet består av flera delar, dels av styrdokument som är stadsövergripande och gäller för samtliga verksamheter och dels av lokalt framtagna styrdokument som enbart gäller för den egna verksamheten.

Denna lokala anvisning är utformad efter stadens modell och beskriver roller och organisation för Stockholm Business Regions informationssäkerhetsarbete.

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

Den lokala anvisningen uppdateras årligen.

Innehållsförteckning

2 Organisation och roller

Stockholm Business Regions organisation för informationssäkerhet är indelad i tre olika nivåer. Den styrande organisationen omfattar operativt beslutande roller och funktioner. 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 Styrelse

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

Styrelsen 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.

Styrelsen har ett särskilt ansvar för att utse ett dataskyddsombud eller delegera ett sådant beslut till bolagschefen. Ett dataskydds-ombud har utsetts genom styrelsebeslut den 1 juni 2018.

Styrelsen inhämtar årligen en så kallad GDPR årsrapport från dataskyddsombudet. Syftet är att styrelsen med hjälp av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker för verksamheten. Senast rapporten, 2023 års rapport, inhämtades och godkändes den 5 mars 2024.

I styrelsen för Stockholm Business Region 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 Bolagschef

Bolagschefen är styrelsens representant (delegat) när det gäller de övergripande lednings- och styrningsfrågorna.

Bolagschef ansvarar för:

- Att fastställa de lokala tillämpningsanvisningarna och andra övergripande styrdokument för Stockholm Business Region.
- 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 Stockholm Business Region.
- Att se till att klassificeringsstruktur och hanteringsanvisningar har fastställts för verksamhetens informationshantering.
- Att hålla sig underrättad om informationssäkerheten i Stockholm Business Region, minst genom att inhämta den årliga rapporten ”Ledningens genomgång” från informationssäkerhetssamordnaren.

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 Stockholm Business Region innebär det som lägst på avdelningschefsnivå. Chefen kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Chefer inom Stockholm Business Region 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 avdelningens verksamhet och ansvarsområde samt att uppdatera och följa upp bolagets register över hantering av personuppgifter (registerförteckningen).
- Att de inköp/upphandlingar som chef beslutar om följer gällande lagar vad gäller informationshantering, samt stadens och bolagets styrdokument.
- Att informationsinventering är gjord av den egna verksamheten med stöd från arkivfunktionen. Att se till att viktigare informationstillgångar är klassade och att verksamhetens IT-tillgångar har en utsedd ansvarig. Informationssäkerhetssamordnare är stödjande avseende informationsklassning och IT-tillgångar. Dataskyddsombudet ska ge råd avseende personuppgiftsbehandling och behandlingsregistret, s.k. registerförteckning.
- Att ta fram lokala rutiner för den egna verksamheten vid behov.

2.1.4 Processägare / Objektägare

All informationshantering i bolaget 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 bolagets hanteringsanvisningar för dokumenthantering (utifrån klassificeringsstruktur). Den chef som ansvarar för en specifik process har benämningen processägare. Processägaren beslutar vilka digitala verktyg/objekt som får användas i processen och hur information ska hanteras inom processen. Processägare likställs med Objektägare[1] när inget annat har överenskommits. Fler

[1] För rollbeskrivning se stadens metodstöd för Pm3

objekt/tjänster kan ingå i en process. Bolagschef tillsätter rollen som Processägare/Objektägare.

2.1.5 Objektledare

En Objektledare ansvarar för drift och utveckling av objekt/tjänst och rollen utses av dess Objektägare. Arbete pågår med att utse objektledare för samtliga digitala tjänster hos Stockholm Business Region.

Vem som tilldelats rollerna som Processägare/Objektägare och Objektledare inom Stockholm Business Region framgår i “SBRs Objektlista” publicerad på det interna intranätet.

När det gäller de IT-tjänster där drift sköts på entreprenad eller på annan förvaltning, är verksamhetens objektledare ansvarig för tjänsten i relation till den beställda tjänsten och fungerar då som lokalt ansvarig för hur systemet används i verksamheten. I de fall både drift och verksamhet finns inom bolaget förekommer ibland rollen objektledare specifikt för tjänstens drift.
Personuppgiftsansvarig är Stockholms Business Region när bolaget bestämmer ändamålen och medlen för behandlingen av personuppgifter. När annat externt bolag eller bolag/nämnd inom Stockholms stad behandlar personuppgifter för Stockholms Business Regions räkning är externt bolag eller bolag/nämnd personuppgiftsbiträde.

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.

2.2 Stödjande och uppföljande

2.2.1 Dataskyddsombud (DSO)

Nu tjänstgörande dataskyddsombud anmäldes till Integritetsmyndigheten, IMY, den 1 februari 2024.

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 agera självständigt och oberoende i sitt uppdrag. 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 dataskyddslagstiftningen och hur praxis styr relevanta skyddsåtgärder som ska väljas och implementeras för att person- och integritetsskyddet ska upprätthållas.
- Vägleda, informera och ge råd till bolaget i frågor om integritetsskyddet.
- Ge råd vid personuppgiftsincidenter enligt gällande lagstiftning
- Vara kontaktperson för nationell tillsynsmyndighet, IMY, och samverka med denna i initiala förhandssamråd och hantering av personuppgiftsincidenter
- Tillsammans med ISAM hantera personuppgiftsincidenter inom bolaget, ansvara för bedömning och anmälan till IMY efter samråd med bolagschefen.
- Dataskyddsombudet ska alltid involveras i samband med konsekvensbedömningar och övervaka genomförandet av dem.
- Aktivt informera om förändringar och uppdateringar i regelverk och annat inom dataskyddsområdet.
- Granska hur väl dataskyddsförordningen efterlevs och skriva dataskyddsombudets årsrapport till bolagets styrelse

2.2.2 Informationssäkerhetssamordnare (ISAM)

Bolagets ISAM är utsedd av bolagschefen. Nu tjänstgörande ISAM utsågs den 28 april 2022.

ISAM ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet och att stötta samt vägleda hela bolagets verksamhet. ISAM ska arbeta utifrån VD och ledningsgruppens 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 alla i bolaget, 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 samt följa upp dessa
- Att samordna och sammanställa verksamhetens registerförteckning samt att den 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 inköp och upphandlingar.
- Att var delaktig i utvecklingsarbetet med konsekvensbedömningar, handlingsplaner och riskanalyser.

2.2.3 Arkivansvarig

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 stödfunktioner i framtagandet av de dokument där hantering och arkivering av styrelsens samtliga informationstillgångar beskrivs, d.v.s. bolagets hanteringsanvisningar och övrig arkivdokumentation.

Arkivfunktionernas roller beskrivs i bolagets arkivorganisation.

2.3 Övriga funktioner

2.3.1 Medarbetare

Medarbetare inom Stockholm Business Region 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 (automatiskt), och ska därefter påminnas om kontraktets innehåll i samband med årliga utbildning/information.

2.3.2 ILS-samordnare

Verksamhetens ILS-samordnare samordnar uppföljningen och beredningen av bolagets 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 avdelningschefer.

2.3.3 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 bolagets verksamhet rollen IT-ansvarig.

2.3.4 Objektspecialist

När Objektledaren valt att peka ut Objektspecialister ansvarar dessa 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 eller processutvecklare.

3 Nätverk och grupper

ISAM och DSO träffas 1-2 gånger i månaden för att lyfta utstående frågor, sprida information och se över respektive rollers arbete inom bolaget. ISAM är sammankallande.

3.1.1 ISAM

Rollen deltar i ”Stadens nätverk för informationssäkerhetssamordnare” som leds av Stadens Informationssäkerhetsansvarig/CISO.

3.1.2 DSO

Rollen deltar i ”Stadens nätverk för dataskyddsombud”, ett nätverk för dataskyddsombud och dataskyddshandläggare som leds av Stadsledningskontorets Dataskyddsombud på SLK.

4 Årshjul

I samband med verksamhetsberättelse och bokslut tar bolaget del av årliga rapporter från till exempel dataskyddsombudet och revisorer där stor hänsyn tas till eventuella rekommendationer. Stockholm Business Region bedriver flera löpande och/eller årliga aktiviteter vilket listas nedan.

Aktivitet - årlig översyn av	Tid	Ansvarig för innehåll och användning av system	Ansvarig för att leda och samordna aktiviteten
Rutiner för Informationssäkerhet inklusive GDPR	Q1	ISAM	ISAM
Integritetspolicy	Q1	OÄ/OL	ISAM
Objektlistan	Q1	IT-ansvarig	IT-ansvarig
On/off-boarding avseende IT och behörigheter	Q1	IT-ansvarig	IT-ansvarig
Informationsklassning nya system	Löpande vid behov	OÄ/OL	IT-ansvarig
Årlig genomgång av Informationsklassningar	Q2	OÄ/OL	IT-ansvarig
Agera på handlingsplaner efter informationsklassning	Q2	OÄ/OL	IT-ansvarig
Årlig uppdatering av registerförteckningen	Q2	OÄ/OL	ISAM
Årlig genomgång av avtal och PUB-avtal	Q2	OÄ/OL	IT-ansvarig
Lokala anvisningar	Q2-Q3	ISAM	ISAM
Ledningens genomgång	Q2-Q3	ISAM	ISAM
Behörighetsrevision (identitet och åtkomst) av objekt	Q3	OÄ/OL	IT-ansvarig
Obligatoriska utbildningar GDPR och informationssäkerhet	Q4	IT-ansvarig	IT-ansvarig

Löpande eller regelbundet återkommande aktiviteter tillsammans med verksamheten:

- Informationsklassificering
  - ISAM ansvarar löpande för att leda arbetet med klassificering av nya system samt för den årliga genomgången av informationsklassningar tillsammans med respektive objektledare.
- Behörighetsrevision
  - ISAM ansvarar för att leda arbetet med kontroll av systembehörigheter tillsammans med objektledare.
- Internkontroll
  - ISAM medverkar i framtagandet av bolagets internkontrollplan och säkerställer att den innehåller kontroller av det systematiska arbetet med informationssäkerhet och dataskydd.
- Stadens generella användarkontrakt
  - ISAM uppmanar medarbetarna att årligen ta till sig stadens generella användarkontrakt (lokalt från datorns hårddisk).

- Personuppgiftsbehandlingar och registerförteckning
    - Årligen genomför dataskyddsombudet tillsammans med ISAM granskning av personuppgiftsbehandlingar med ansvariga för process/system. Utifrån granskningsresultat ges råd avseende behov av uppdatering.
    - ISAM ansvarar för att leda och samordna den årliga genomgången av registerförteckningen tillsammans med objektledare.

5 Rutiner och praktiskt arbete

Rutin, med ansvar och lagringsplats, finns för:

- Hemarbete
    - Administrativ chef har publicerat information på intranätet som ett komplement till stadens riktlinjer.

- Information till nyanställda
    - ISAM tillser att nyanställda grundutbildas inom informationssäkerhet under planerade möten i samband med onboardingprocessen.

- Start och avslut av tjänst
    - HR-ansvarig tillser att närmaste chef får uppdaterat informationsunderlag och checklistor vid on- och offboarding.

- Avslut av gruppdiskar, funktionsbrevlådor, samarbetsytor.
    - Ansvarig chef ansvarar för att arkivering i enlighet med hanteringsanvisningarna sker innan resursytor stängs ner. Teknisk personal har rutin att endast stänga ner resursytor på uppdrag av ansvarig chef.

- Hanteringsanvisningar diariet & arkivet
    - Arkivansvarig tillser löpande att diariets och arkivets hanteringsanvisningar finns och är uppdaterade.