Stockholms stad

Lokal anvisning för informationssäkerhet

S:t Erik Försäkrings AB

Beslutad 230220
Reviderad

Lokal anvisning för informationssäkerhet

Dnr: SEF 2023/9

Kontaktperson: Johan Gagner

1 Bakgrund

Denna lokala anvisning beskriver roller och organisation för S:t Erik Försäkrings AB informationssäkerhetsarbete. Dokumentet fastställdes av VD den 230220.

Den lokala anvisningen uppdateras årligen enligt årshjulet.

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

Den lokala tillämpningsanvisningen beskriver också hur S:t Erik Försäkring systematiskt arbetar med, och följer upp, informationssäkerheten.

Innehållsförteckning

2 Organisation och roller

S:t Erik Försäkring 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 Styrelse

Styrelsen är ytterst ansvarig för informationen och formellt informationsägare och personuppgiftsansvarig för S:t Erik Försäkring. Styrelsen 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. Genom detta dokument beskriver Styrelsen hur denna organisation fungerar i praktiken.

Styrelsen har ett särskilt ansvar för att utse ett dataskyddsombud eller delegera ett sådant beslut till bolagschef. Ett dataskyddsombud har utsetts av VD datum 2018-05-22.

Styrelsen inhämtar årligen en så kallad GDPR årsrapport från dataskyddsombudet. Syftet är att styrelse 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 styrelsen.

I styrelsens 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 S:t Erik Försäkring.
- 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 S:t Erik Försäkring, 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.

Kommentar [JG1]: För att kunna styra arbetet ska förvaltningschef/bolagschef minst årligen informera sig om hur arbetet går. Det sker genom att förvaltningschef/bolagschef inhämtar en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare eller om informationsklassningar och registerförteckning är genomförda. Denna rapportering ska ge information och underlag till förvaltningschef/bolagschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltnings- och bolagschefer ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.

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

Chefer inom bolaget ansvarar för:

- Att se till att samtliga medarbetare och konsulter 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 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 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.

Kommentar [JG2]: PM3 ”light” utifrån Registerförteckningen

2.1.4 Objektledare

För rollbeskrivning se stadens metodstöd för Pm3

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

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

Kommentar [JG3]: Registerförteckning finns i mappen ”G:\2 Verksamhetsstöd\2.5 Kommunicera och informera\2.5.4 Personuppgifter\Register”

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 bolaget 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)

Bolagets ISAM är utsedd av bolagschefen. Nu tjänstgörande ISAM utsågs datum 2022-06-01.

ISAM ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet och att stötta samt vägleda hela bolagets verksamhet. ISAM ska arbeta utifrån bolagschefens 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 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)

Verksamhetens dataskyddsombud utses formellt av styrelsen. Nu tjänstgörande dataskyddsombud utsågs av VD, 2018-05-22.

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

Verksamhetens ILS-samordnare samordnar uppföljningen och beredningen av nämndens/bolagets ILS-arbete.
ILS-samordnaren ska aktivt arbeta för att informationssäkerhet är med och följs upp i bolagets 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 bolagets informationssäkerhetsarbete och i dess inventeringar av informationstillgångar – både digitala och fysiska.

Arkivansvarig och arkivarie är stödfunktioner i framtagandet av de dokument där hantering och arkivering av styrelsens 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, och ska därefter påminnas om kontraktets innehåll enligt en rutin som styrelsen beslutar om.

Kommentar [JG4]: Bilaga ”Användarkontrakt”

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 bolagets verksamhet rollerna it-chef, it-strateg, it-samordnare, it-tekniker och verksamhetsutvecklare it.

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. Objektledaren ansvarar för att utse den organisationen.

3 Nätverk och grupper

3.1.1 Centrala nätverk

Informationssäkerhetssamordnaren ingår och medverkar i Stadens centrala nätverk för informationssäkerhet, vilket leds av informationssäkerhetsansvarig (CISO)

4 Årshjul

4.1.1 Årshjul

Här beskrivs det årliga arbetet med informationssäkerhet.
Exempelvis uppföljning och arbete med informationssäkerheten

- Arbetet med VOR och RSA.
- Uppföljningar av informationssäkerhet i samtliga system
- Uppföljningar av informationssäkerhetsklassningar i samtliga system
- Uppföljningar av registret över personuppgiftsbehandlingar.
- Uppföljningar av annan rutindokumentation.

5 Rutiner och praktiskt arbete

Här beskrivs hur det praktiska arbetet går till vad gäller informationssäkerhet, samt vad som ska finnas på plats vad gäller informationsvärdering av processer och system.

Här listas också vilka övriga lokala rutiner som bolaget ska ha på plats, samt när de följs upp/revideras.

Rutin för

- Registerförteckning
  - Årlig genomgång med ansvariga för process/system avseende behandlingar
- Hemarbete
  - Samma krav på säkerhet som vid arbete på arbetsplatsen. Tillse att anställdas datorer har säkra uppkopplingar mot staden även vid arbete på distans.

Årsvisa systematiska kontroller och inventeringar, t.ex.

- Informationsklassificering
  - ISAM genomför årlig genomgång av informationsklassningar med respektive Objektledare.
- Behörighetsrevision
  - Kontroll systembehörigheter utförs av ISAM och Objektledare.
- e-utbildning
  - Årlig kontroll av ISAM att personal har genomgått stadens utbildningar inom informationssäkerhet.
- Internkontroll
  - ISAM kontrollerar att bolagets internkontrollplan innehåller kontroller av det systematiska arbetet med informationssäkerhet.
- Information till nyanställda
  - ISAM tillser att nyanställda utbildas inom informationssäkerhet.
- IKT plan
  - ISAM ansvarar för att i samverkan med Objektledare i bolaget och bolagets regelefterlevnadsfunktion uppdatera planen (minst årligen) och tillse att den följs genom att hantera processer i planen.

- Lokal anvisning
    - ISAM ansvarar för årlig översyn av denna anvisningen.

- Medgivande och samtycke genom avtal
    - ISAM hanterar samtycken vid behandling av personuppgifter, öppnande av post etc.