

# Ledningens genomgång år 2025 samt 3-årsplan

## S:t Erik Försäkring

Beslutad 2025-12-03  
Reviderad [datum]

### **Ledningens genomgång**

**Dnr:** SEF 2025/50

**Kontaktperson:** Johan Gagner

***Ledningens genomgång*** är ett begrepp inom informationssäkerhet som syftar till att de som ansvarar för informationssäkerheten inom en organisation, minst årligen ska informera sig om hur arbetet går.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, så kallad "Ledningens genomgång" från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare och 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.<sup>1</sup>

I *Anvisningar för nämndernas arbete med verksamhetsplan 2024* uppmanades samtliga nämnder och bolagsstyrelser att ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet under de efterföljande tre åren. Denna bilades verksamhetsplanen. *Riktlinje för informationssäkerhet* i Stockholms stad följdes i denna planering.

Dessa aktiviteter redovisas i Ledningens genomgång. Inventering och informationsklassning är grunden i informationssäkerhetsarbetet.

Alla nämnder och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar.

---

<sup>1</sup> Tillämpningsanvisning till stadens riktlinje för informationssäkerhet

# Innehållsförteckning

<b>1</b>	<b>Ledningssystem för informationssäkerhet, LIS .....</b>	<b>4</b>
1.1	Vad påverkar S:t Erik Försäkrings informationssäkerhetsarbete? ..	4
1.1.1	<i>Omvärldsbevakning .....</i>	4
1.1.2	<i>Risk och sårbarhetsanalys.....</i>	5
1.1.3	<i>Risker som identifierats i GDPR-årsrapport .....</i>	5
<b>2</b>	<b>Förbättringar för verksamhetens LIS.....</b>	<b>6</b>
2.1	S:t Erik Försäkrings lokala anvisning för informationssäkerhet .....	6
<b>3</b>	<b>Åtgärder 2024 .....</b>	<b>6</b>
<b>4</b>	<b>Åtgärder 3-årsplan .....</b>	<b>6</b>
4.1	Under 2026 ska S:t Erik Försäkring .....	6
4.2	Under 2027 ska S:t Erik Försäkring .....	7
4.3	Under 2028 ska S:t Erik Försäkring .....	7

# 1 Ledningssystem för informationssäkerhet, LIS

Stockholms stads arbete med informationssäkerhet utgår från en så kallad ISO standard, ISO 27001. Det är en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information från hot och risker. Standarden ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet, LIS, som skyddar informationstillgångarna och ger en IT-process som är lättare att hantera, mäta och förbättra.

Stockholms stads informationssäkerhetsarbete regleras i en tillämpningsanvisning som är en bilaga till stadens Kvalitetsprogram<sup>2</sup>. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För S:t Erik Försäkrings räkning har VD fastställt en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom bolaget.

## 1.1 Vad påverkar S:t Erik Försäkrings informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska S:t Erik Försäkring ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering.

### 1.1.1 Omvärldsbevakning

- S:t Erik Försäkring lyder under försäkringsrörelselagen och de riktlinjer som Finansinspektionen utfärdar. Vidare omfattas bolaget av ett stort antal EU-förordningar för just försäkringsbolag. Regelverket är omfattande avseende intern styrning och kontroll.
- På informationssäkerhetsområdet finns särskilda regler för försäkringsbolag som inte omfattar staden i övrigt, EBA:s riktlinje GL/2019/02, EIOPA 20-002, Eiopas riktlinjer (20/600) för säkerhet och företagsstyrning avseende information och kommunikationsteknik (IKT).

---

<sup>2</sup> [Stockholms stads kvalitetsprogram \(start.stockholm\)](http://start.stockholm)

- Regelverket DORA (Digital Operational Resilience Act), är det nya gemensamma EU-regelverket för effektiv och övergripande hantering av digitala risker i finansbranschen. Den nya strukturen flyttar fokus från att endast handla om företagens finansiella ställning till att även säkerställa hur väl de kan upprätthålla verksamheten och stå emot vid olika incidenter, cyberhot och it-problem. Med införandet av en enhetlig tillsynsmetod för alla relevanta sektorer i hela EU säkerställs både konvergens och harmonisering av tidigare praxis vad gäller cybersäkerhet och motståndskraft vid olika digitala incidenter.
- S:t Erik Försäkring ingår i ett nätverk av kommunala försäkringsbolag. Samarbete gällande IKT risker utifrån ovan regelverk sker i detta nätverk.

### 1.1.2 Risk och sårbarhetsanalys

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleddes under 2024.

Bolagets organisation avseende riskhantering är organiserat med för försäkringsbolag lagstadgade centrala funktioner (riskhanteringsfunktion, regelefterlevnadsfunktion, internrevision samt aktuarie) samt därutöver ISAM och DO.

Vad avser RSA hanteras dessa risker av verksamheten i samarbete med bolagets ovan beskrivna riskhanteringsfunktion. Varje risk har en riskägare och åtgärdsplan (såvida inte risken accepteras). Riskhanteringsfunktionen rapporterar risknivåer, riskhantering m.m. till styrelsen vid varje styrelsemöte samt vid behov. Riskhanteringsfunktionens arbete kontrolleras av internrevisionen.

### 1.1.3 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudet har i årsrapporten skrivit att information om tekniska och organisatoriska åtgärder, bland annat

1. Verksamheten bör klassa samtlig informationshantering och uppdatera tidigare gjorda klassningar. För information i centrala system (stadens) kan ev. utförda centrala klassningar dokumenteras och justeras efter verksamhetens förutsättningar.
2. Verksamheten bör göra en konsekvensbedömning av behandlingen i IA samt uppdatera de andra gjorda konsekvensbedömningarna.
3. Behörighetsrevision ska utföras och dokumenteras.

Dessa tre punkter har omhändertagits under året.

## **2 Förbättringar för verksamhetens LIS**

### **2.1 S:t Erik Försäkrings lokala anvisning för informationssäkerhet**

Den 20 februari 2023 fastställde Tf Vd bolagets Lokala anvisning för informationssäkerhet.

Anvisningen är diarieförd och finns tillgänglig för alla medarbetare på bolagets gruppdisk.

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

## **3 Åtgärder 2025**

Under året har bl a nedan arbete utförts:

- Inrapportering till Finansinspektionen avseende DORA regelverket
- Informationsklassningar
- Översyn av organisationen enligt PM3 (light)
- hanteringsrutin för informationssäkerhetsincidenter uppdaterad
- årlig översyn av lokal anvisning för informationssäkerhet
- behörighetsrevision utförd
- medarbetare certifierade i Stadens utbildningar gällande informationssäkerhet och dataskydd
- årlig uppdatering av IT-avbrottsplan

## **4 Åtgärder 3-årsplan**

### **4.1 Under 2026 ska S:t Erik Försäkring**

Under 2026 ska Bolaget prioritera att:

- utföra PEN tester gentemot skadesystem
- säkerställa att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbete som pågår inom verksamheten, särskilt för nya digitala tjänster som erbjuds.
- se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- uppföljningar av registret över personuppgiftsbehandlingar utförs.
- avseende 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.
- årlig översyn av Lokal anvisning för informationssäkerhet
- uppföljningar av övrig rutindokumentation t ex avbrottsplan, hanteringsrutin för informationssäkerhetsincidenter och behörighetsrevision utförs
- följa den framtagna rutinen för regelbundna informationsklassningar.
- öva utifrån kontinuitetsplaner/avbrottsplaner.

## **4.2 Under 2027 ska S:t Erik Försäkring**

Under 2027 ska Bolaget prioritera att:

- se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- uppföljningar av registret över personuppgiftsbehandlingar utförs.
- avseende 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.
- årlig översyn av Lokal anvisning för informationssäkerhet
- uppföljningar av övrig rutindokumentation t ex avbrottsplan, hanteringsrutin för informationssäkerhetsincidenter och behörighetsrevision utförs
- följa den framtagna rutinen för regelbundna informationsklassningar.
- öva utifrån kontinuitetsplaner/avbrottsplaner.

## **4.3 Under 2028 ska S:t Erik Försäkring**

Under 2028 ska Bolaget prioritera att:

- se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- uppföljningar av registret över personuppgiftsbehandlingar utförs.

- avseende 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.
- årlig översyn av Lokal anvisning för informationssäkerhet
- uppföljningar av övrig rutindokumentation t ex avbrottsplan, hanteringsrutin för informationssäkerhetsincidenter och behörighetsrevision utförs
- följa den framtagna rutinen för regelbundna informationsklassningar.
- öva utifrån kontinuitetsplaner/avbrottsplaner.

*Fastställd av VD 2025-12-03*