Göteborgs Stad

Dokumentnamn: Försäkrings AB Göta Lejons handbok för systematiskt informationssäkerhetsarbete

Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
[Nämnd/styrelse/befattning]	[Text]	[Nummer]	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
[Dokumentsort]	Tills vidare	2026-03-11	Säkerhetschef

Bilagor:
Bilaga 1 Styrmiljö risk och säkerhet
Bilaga 2 Definitioner och Ordlista

Försäkrings AB Göta Lejons handbok för systematiskt informationssäkerhetsarbete

Syftet med denna handbok

Syftet med denna handbok är att säkerställa systematiskt informationssäkerhetsarbete enligt:

- Dora
- Solvens II
- MSBs metodstöd för systematiskt informationssäkerhetsarbete

Arbetet med informationssäkerhet ska vara integrerat i bolagets ordinarie styrmodell (strategi, planering och uppföljning samt kontrollsystem), riskhanteringsprocess och styrning av IKT.

Vem omfattas av rutinen

Denna rutin gäller tills vidare för Försäkrings AB Göta Lejon.

Koppling till andra styrande dokument

För Göta Lejon finns ett flertal styrande dokument inom området informationssäkerhet. En schematisk illustration över styrmiljön och dokumenthierarkin återfinns i Bilaga 1.

Riktlinjer

Riktlinje för riskhantering och intern styrning och kontroll

Riktlinje för säkerhet

Riktlinje för kontinuitet

Anvisningar

Anvisning för informationsklassning

Anvisning för riskhantering

Anvisning för incidenthantering

Rutiner

Rutin för utkontraktering av IKT-tjänster

Rutin för informationsklassning

Rutin för specifik riskbedömning av äldre IKT-system

Rutin för leverantörsuppföljning

Stödjande dokument och resurser

Leverantörsregister

Processbeskrivningar

Mallar kopplat till riskanalys

ISDB

Stratsys Risk och kontroll

Stratsys Informationssäkerhet

Vägledande principer

Följande principer gäller för styrmiljön och arbetet med informationssäkerhet.

- Informationssäkerhet ska följa integrerat i bolagets verksamhet och inte vara ett sidospår.
- Informationssäkerhetsarbetets årshjul definierar miniminivån och är tidstyrt med återkommande aktiviteter.
- Utöver årshjulet kan ytterligare, händelsestyrda, aktiviteter triggas. Dessa aktiviteter utförs när det anses nödvändigt och kan utlösas av nya system, större förändringar, nya leverantörer, incidenter, regelverksförändringar eller resultat från granskningar.

Årshjul

Q1

- Analys av föregående års incidenter
- Genomföra övning i incident och kontinuitetshantering, inkl krisledning

- Informationsägarnas årliga klassningsöversyn
- Uppdatering och kvalitetssäkring av register
- Informationsregister till Finansinspektionen (FI)
- Uppdatering av rapport över riskhanteringram

Q2

- Riskanalys informations- och IKT-säkerhet
- Årlig översyn av riktlinjer och instruktioner
- Utbildningsinsatser

Q3

- Mognadsbedömning/gapanalys mot krav
- Omvärldsbedömning
- Strategisk planering

Q4

- Fastställande av bolagets samlade riskbild (inkl informationssäkerhet/IKT)
- Uppföljning av leverantörer
- Fastställande av årshjul och plan till nästkommande år
- Ledningens genomgång

Tidsstyrda och händelsestyrda triggers

Tidsstyrda aktiviteter

Se separat årshjul.

Händelsestyrda aktiviteter

Nedanstående aktiviteter är exempel på händelser som kan trigga aktiviteter inom informationssäkerhetsområdet.

Vid nytt system eller större systemförändring

- Uppdatera informationsklassning
- Genomför riskanalys
- Uppdatera tillgångsregister
- Uppdatera behandlingsregister (GDPR)
- Uppdatera kontinuitetsplaner

Vid ny eller förändrad leverantör

- Uppdatera leverantörsregister
- Genomför riskbedömning
- Framtagning av avtalskrav
- Framtagning av exitplaner

Vid allvarlig incident

- Incidenthantering
- Rapportering
- Orsaksanalys
- Uppdatering av riskregister och kontroller

Vid ny eller förändrad reglering

- Gap-analys
- Uppdatering av riktlinjer och instruktioner
- Utbildning

Årshjul månad för månad

Se separat årshjul