**Riktlinje för informations- och kommunikationsteknik - IKT**

 **1 Inledning**

Försäkrings AB Göta Lejon (Bolaget) bedriver försäkringsrörelse. Denna rörelse är tillståndspliktig enligt försäkringsrörelselagen (2010:2043). Och i enlighet med EIOPA-BoS-20/600 ska Bolaget upprätta ett styrdokument och strategi avseende information och kommunikationsteknik (IKT).

Riktlinjen kompletteras med Policy och Riktlinjer utfärdade av Göteborgs Stad.

**2 Syfte och mål**

Denna riktlinje ska ange Bolagets principer och strategi avseende information och kommunikationsteknik för att främja en effektiv riskhantering.

Avsikten är att säkerställa att IT -system och information som är av väsentlig betydelse för att Bolaget ska kunna bedriva sin verksamhet på ett ändamålsenligt sätt och uppnå sina strategiska och affärsmässiga mål därför är tillgänglig och tillförlitlig.

Bolagets hantering av egen, kunders, anställdas och övriga intressenters information ska ske i enlighet med interna och externa regelverk för att säkerställa att Bolaget upprätthåller en trygg och säker hantering.

Som captivebolag med verksamheten begränsat till koncernens egna risker tillämpar Bolaget regelverket för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik på ett sätt som står i proportion till arten, omfattningen och komplexiteten av Bolagets inneboende risker.

**3 Strategi för IKT**

Denna riktlinje har antagits av styrelsen och anger de övergripande strategier och principer för Bolagets arbete kring IKT. Syftet är att skydda konfidentialitet, korrekthet och fullständighet samt tillgänglighet avseende Bolagets information. Bolagets strategi för informationssäkerhet grundar sig på den befintliga riskstrategin inom Bolagets riskhanteringssystem. Bolagets riskaptit för incidenter har även bäring på Bolagets informationssäkerhet vilket ger grunderna för en effektiv uppföljning och efterlevnadskontroll. Riktlinjen fastställer även det interna ansvaret för IKT och informationssäkerhet inom Bolaget. Denna riktlinje och strategi ska alltid beaktas och vara del av Bolagets affärsutveckling enligt nedan underrubriker:

### Affärsutveckling

- affärsstrategi (verksamhetsplanering)

- organisationsstruktur

- affärsmodeller /försäkringsprodukter

- nyckelberoende av tjänsteleverantörer av utlagd verksamhet

### IKT arkitektur

- utveckling av IT-arkitektur

- nyckelberoende av tjänsteleverantörer av utlagd verksamhet

**4 Tillämpliga regler**

### Göteborg Stads regelverk

* Regler för användande av e-post
* Regler för chefers informationssäkerhetsansvar
* Regler för IT användare
* Regler gällande driftsdokumentation för IT baserad information
* Riktlinjer för hantering av säkerhetsrisker
* Riktlinjer för informationssäkerhet
* Säkerhetspolicy

### Bolags relaterade styrdokument

* Riktlinje för riskhantering
* Riktlinje för datakvalité
* Riktlinje för utlagd verksamhet
* Riktlinjer för hantering och rapportering av händelser av väsentlig betydelse
* Riktlinje för Internrevision
* Riskpolicy
* Policy och riktlinje för hantering av personuppgifter
* Bolagets kontinuitetsplan och krisledningsplan
* Manualen för företagsstyrning
* Bolagets riskregister och informationsklassnings dokumentation

Riktlinjen reglerar all informationsbehandling oavsett driftsmiljö och gäller oavsett om behandlingen sker internt eller hos en tjänsteleverantör av outsourcad verksamhet. Instruktionen avser även information i pappersformat.

Riktlinjen ska göras tillgängliga för och tillämpas av Bolagets styrelseledamöter, VD, medarbetare och konsulter. I förekommande fall måste instruktionerna också meddelas och tillämpas av företagets tjänsteleverantörer av outsourcad verksamhet.

Vid eventuell diskrepans mellan Göteborgs Stads regler och de i denna angivna riktlinje, ska Göteborgs Stads riktlinjer och strategi i första hand äga företräde. Bolaget ska dock alltid hålla sig inom ramarna för vad som krävs och är tillåtet för Bolaget tillämpliga regelverk varpå det i vissa situationer är Göta Lejons riktlinjer som har företräde.

**5 Roller och ansvarsfördelning**

**Styrelsen**

Styrelsen ska se till att Bolagets hantering och kontroll av risker är tillfredsställande och har det yttersta ansvaret för Bolagets arbete med IKT och informationssäkerhet. Styrelsen ansvarar för att upprätta och fastställa Bolagets strategi för IKT, som en del av Bolagets affärsstrategi. Styrelsen har i denna riktlinje angivit mål och inriktning för Bolagets arbete med IKT och informationssäkerhet.

**VD**

VD ansvarar för att de grundläggande inriktningarna som framgår av denna riktlinje tillämpas i den dagliga verksamheten och att de efterlevs. Vidare ska VD säkerställa att det finns tillräckliga resurser och erforderlig kompetens för att efterleva vad som anges i denna riktlinje och övriga tillämpliga interna regler avseende hanteringen av IKT och informationssäkerhet. VD ska även tillse att berörda parter/medarbetare regelbundet får lämplig utbildning inom IKT och säkerhetsrisker, inklusive informationssäkerhet.

**Ansvarig för informationssäkerhet**

Bolagets operativa hantering av informationssäkerhet är främst utlagt på IT-support inom Göteborg Stad för närvarande via uppdragsavtal med Intraservice.

Ansvarig för informationssäkerhet ska tillse att;

* utveckla och förvalta ledningssystem för informationssäkerhet,
* utveckla interna regler och säkerhetsåtgärder,
* förvalta Bolagets register över informationstillgångar,
* genomföra hotbildsanalyser,
* medverka i de riskanalyser som berör informationssäkerhet och
* utvärdera säkerhet avseende Bolagets IKT-system, genom deltagande via relevant IT-personal i samband med den årliga uppdatering av riskregistret.

**Medarbetare**

Medarbetare ska ansvara för att

* säkerställa att respektive informationstillgångar hanteras i enlighet med de interna regler som ingår i Bolagets ledningssystem,
* delta i de aktiviteter som beslutas av Bolagets informationssäkerhetsansvarig
* delta i hantering av inträffade informationssäkerhetsincidenter,
* skydda integritet och informationssäkerhet enligt rubriken Tillämpliga regler, och
* genomföra obligatoriska utbildningar och säkerhetskampanjer anvisade av Göteborg Stad eller Bolaget.

**5 Utlagd verksamhet**

Upphandling och utkontraktering

Bolaget ska inför nya upphandlingar och utläggning av verksamhet och funktioner beakta eventuella IKT-risker. Bolaget ska identifiera och ställa de krav som Bolaget anser nödvändiga för att Bolagets information ska hanteras säkert hos externa leverantörer.

Vid kravställande ska Bolaget beakta vilken möjlighet som ges till olika former av granskningar av leverantörens säkerhetskrav. Detta kan avse exempelvis rätten till revision, krav på åtkomst till resultat av leverantörens egenkontroller eller externa granskningar initierade av leverantören själv, stöd från leverantören vid granskningar och Finansinspektionens rätt till insyn etc.

Bolagets styrelse har antagit separata riktlinjer för utlagd verksamhet.

Beroenden gentemot tjänsteleverantörer

När IKT-tjänster och IKT-system utkontrakteras ska Bolaget se till att relevanta krav för sådana tjänster och system uppfylls, utan att det påverkar tillämpningen av dessa interna IKT-riktlinjer samt EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer.

I de fall kritiska eller viktiga funktioner utkontrakteras ska Bolaget se till att tjänste-leverantörens avtalsförpliktelser omfattar krav på innehåll i sådana avtal enligt EIOPA:s IKT-riktlinjer samt EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer.

Vid hantering av tredjepartsleverantörer ska Bolaget även beakta Göteborgs stads riktlinjer för informationssäkerhet.

**6 IKT och säkerhetsrisker inom Bolagets riskhanteringssystem**

### Riskhanteringsprocess

Bolaget ska regelbundet genomföra en kartläggning över Bolagets affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar). Syftet med kartläggningen är att identifiera deras betydelse och ömsesidiga beroendeförhållanden beträffande IKT-risker och säkerhetsrisker.

Hantering av IKT-risker och säkerhetsrisker ska vara en del av Bolagets allmänna riskhanteringssystem och riskhanteringsprocess som finns beskrivet i Bolagets interna riktlinjer för riskhantering. Detta inbegriper att, i enlighet med Bolagets riskstrategi, fastställa risktolerans för IKT-risker och säkerhetsrisker. IKT-risker ska inkluderas i Bolagets riskregister som tas fram av Bolaget tillsammans med funktionen för riskhantering.

### Ansvarig för IKT - riskhantering

Som captive försäkringsbolag inom Göteborg Stad tillhandahåller Bolaget inte IT-drift för egen räkning – se ovan under rubriken Tillämpliga regler. Stadens IT-ansvarig (intraservice) ansvarar för att Bolaget har de säkerhetsåtgärder, rutiner och funktioner som krävs för att säkerställa en tillräckligt hög säkerhetsnivå i enlighet med externa och interna krav.

Analog till andra identifierade risker ska Bolagets riskhanteringssystem inkludera hantering av IKT-risker och säkerhetsrisker och riskhanteringsfunktionen ansvarar för att identifiera och bedöma risker kopplade till informationssäkerhet. De närmare reglerna för funktionen finns i Riktlinjer för riskhantering och Riskpolicy.

### Oberoende funktion för informationssäkerhet, riskhanteringsfunktion

Bolaget ska ha en oberoende funktion eller person för informationssäkerhet. Riskhanteringsfunktionen ansvarar för att identifiera och bedöma risker kopplat till informationssäkerhet, och ska därvid även vara oberoende gentemot utvecklings- och driftprocessen inom IKT. Särskilt när det kommer till IKT-risker ska riskhanteringsfunktionen

* utgöra ett stöd till Bolagets ledning i samband med fastställande och upprätthållande av Bolagets IKT-riktlinjer,
* regelbundet rapportera och ge vägledning om informationssäkerhetens status och utveckling,
* övervaka och granska genomförandet av informationssäkerhetsåtgärder,
* följa upp hur informationssäkerhetskrav följs upp av tjänsteleverantörer,
* följa upp anställda och ledningens kunskap och kännedom om Bolagets IKT-riktlinjer, och
* samordna granskningar av operativa incidenter eller säkerhetsincidenter och rapportera granskningar till Bolagets ledning och vd.

De närmare reglerna för funktionen finns i riktlinjer för riskkontroll och Riskpolicy.

**Internrevision**

Området för IKT och informationssäkerhet ska ingå som del av funktionen för internrevision granskningsplan med lämplig frekvens, (se också Riktlinjer för internrevision).

**Definitioner**

|  |  |
| --- | --- |
| Informationsägare  | Medarbetare med ansvar för, och tillgång till information och IKT-tillgång. |
| Tillgänglighet | En möjlighet att kunna använda information i förväntad utsträckning och inom önskad tid. |
| Konfidentialitet | Förhållandet att information inte görs tillgänglig eller avslöjas för obehöriga (individer, enheter eller bolag, processer eller system). |
| Cyberattack | Alla former av sabotage eller utnyttjande av IKT-system för att angripa en tredje part genom att förstöra, exponera, inaktivera, stjäla eller tillförskansa sig obehörig tillgång till en informationstillgång.  |
| Cybersäkerhet | Bevarande av konfidentialitet, korrekthet, fullständighet och tillgänglighet rörande on-line- eller webb-baserad information och/eller informationssystem. |
| IKT-tillgång | Mjuk- eller hårdvara. |
| IKT-projekt | Projekt eller del av projekt där IKT-system och tjänster ändras, byts ut eller implementeras. |
| IKT- och säkerhetsrisk | Del av operativ risk; risk att förlora system och data till följd av brott mot konfidentialitetskrav, icke fullständig eller korrekt information i system eller data, opassande eller otillgängliga system och data eller oförmåga att byta IKT inom rimlig tid och till rimlig kostnad när miljö eller affärskrav ändras (”agility”). Inkluderar både cyberrisker och informationssäkerhetsrisker till följd av icke passande eller misslyckade interna processer eller externa händelser, cyberattacker inräknade, eller otillräcklig fysisk säkerhet. |
| Informationssäkerhet | Skydd av informations och/eller informationssystems konfidentialitet, riktighet och tillgänglighet samt säkerställande av spårbarhet av information och/eller informationssystem. |
| IKT-tjänster | Tjänster som tillhandahålls en eller flera interna eller externa användare genom IKT-system och tjänsteleverantörer av utlagd verksamhet. |
| IKT-system | Uppsättning av applikationer, tjänster, IKT-tillgångar eller andra komponenter som hanterar information som innefattar driftsmiljön |
| Informationstillgång | Allt materiellt eller immateriellt som innehåller, eller bär på information, exempelvis informationssystem, dokument, register, datorer, mobiltelefon, nätverk etc. |
| Integritet | Korrekt och fullständig information. |
| Operativa risker eller säkerhetsrisker | En enskild händelse eller serie av sammanlänkade oplanerade händelser som har eller som troligtvis kommer att ha en negativ inverkan på korrekthet, fullständighet, tillgänglighet eller konfidentialitet i IKT-system och tjänster.  |
| Tjänsteleverantör | Tredje part som utför en utlagd process, tjänst eller annan aktivitet, eller del därav i enlighet med ett avtal om utlagd verksamhet.  |
| ”Threat Led Penetration Testing” | Ett kontrollerat försök att pröva en enhets cybermotstånd genom att simulera taktik, teknik och processer från verkliga situationer.  |
| Sårbarhet | En svaghet, misstänkt fel hos en tillgång eller kontroll som kan utnyttjas genom ett eller flera hot. |

Ändringshistorik

|  |  |  |
| --- | --- | --- |
| Version | Datum för ändring | Beskrivning av ändring |
| 1 |  | Första version |
| 2 |  |  |