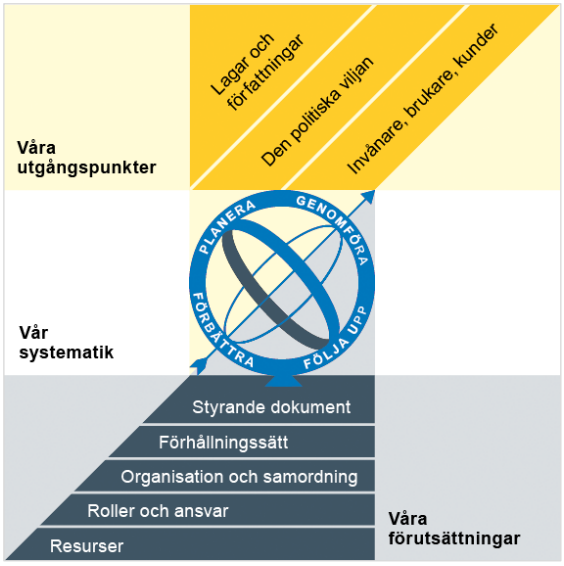
Göteborgs Stad

Försäkrings AB Göta Lejons riktlinje för information- och kommunikationsteknik (IKT)

Reglerande styrande dokument

- Policy
- ► **Riktlinje**
- Regel
- Anvisning
- Rutin
- Instruktion

Göteborgs Stads styrsystem



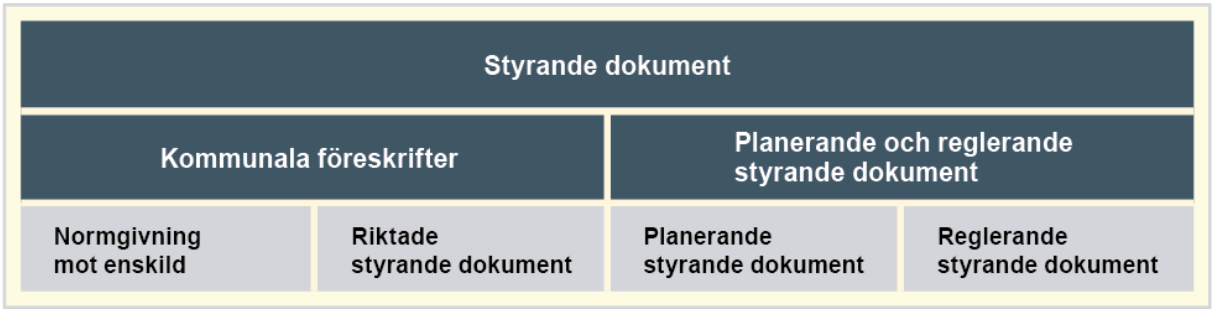
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Styrelse	Försäkrings AB Göta Lejon	0082/24	2024-10-17 § 108
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tillsvidare	2023-11-16	Bolagscontroller

Bilagor:

-

Innehåll

Inledning 4
Syftet med denna riktlinje 4
Vem omfattas av riktlinjen 4
Lagbestämmelser 4
Koppling till andra styrande dokument 4
Riktlinje 5
Strategi för informationssäkerhet 5
Ansvar 6
Styrelse 6
Vd 6
Ansvar för informationssäkerhet 6
Medarbetare 6
Leverantörer 7
Informationssäkerhet och bolagets riskhanteringssystem 7
IT-drift 8
Oberoende funktion för informationssäkerhet, riskhanteringsfunktion 8
Internrevision 8
Tillämpning 8
Fastställande och efterlevnad 9

Inledning

Syftet med denna riktlinje

Syftet med denna riktlinje är att ange bolagets principer och strategi avseende informationssäkerhet så att dessa främjar en effektiv riskhantering. Syftet är att skydda konfidentialitet, riktighet samt tillgänglighet avseende bolagets information. Riktlinjen fastställer även det interna ansvaret för informationssäkerhet inom bolaget.

Riktlinjen utgör Försäkrings AB Göta Lejons strategi för information- och kommunikationsteknik.

Vem omfattas av riktlinjen

Denna riktlinje gäller tillsvidare för hela bolaget samt utlagd verksamhet och verksamhet som utför arbete genom uppdragsavtal.

Lagbestämmelser

Denna riktlinje har upprättats i enlighet med EIOPA-BoS – 20/600: Riktlinjer för säkerhet och företagsstyrning avseende informations och kommunikationsteknik.

Koppling till andra styrande dokument

Göteborgs stads regler för användande av e-post
Göteborgs stads regel för IT användare
Göteborgs stads riktlinje för informationssäkerhet
Göteborgs stads säkerhetspolicy
Försäkrings AB Göta Lejons riktlinje för företagsstyrning
Försäkrings AB Göta Lejons riktlinje för riskhantering och intern styrning och kontroll
Försäkrings AB Göta Lejons riktlinje för datakvalité
Försäkrings AB Göta Lejons riktlinje för uppdragsavtal och utlagd verksamhet
Försäkrings AB Göta Lejons riktlinje för hantering och rapportering av händelser av väsentlig betydelse
Försäkrings AB Göta Lejons riktlinje för internrevisionsfunktionen
Försäkrings AB Göta Lejons riktlinje för integritet och dataskydd
Försäkrings AB Göta Lejons kontinuitetsplan
Försäkrings AB Göta Lejons krisledningsplan

Riktlinje

Göta Lejons företagsstyrning och system för riskhantering och intern kontroll ska utformas så att informations- och kommunikationstekniska risker samt informationssäkerhetsrisker hanteras på lämpligt sätt.

Informationssäkerhetsarbetet omfattar alla typer av informationstillgångar som bolaget hanterar, oavsett om de behandlas manuellt eller digitalt och oberoende av vilken i form eller miljö den förekommer.

Informationssäkerhet innebär att bolaget ska skydda informationstillgångar avseende:

- Konfidentialitet, att information inte tillgängliggörs eller avslöjas för obehöriga.
- Riktighet, att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
- Tillgänglighet, att information är tillgänglig och användbar när den behövs.

Som captivebolag med verksamheten begränsad 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.

Göta Lejon integrerar arbetet med informationssäkerhet med arbete inom området informations- och kommunikationsteknik (IKT). I detta ingår även dataskydd.

Strategi för informationssäkerhet

Bolagets strategi för informationssäkerhet grundar sig på den befintliga riskstrategin inom bolagets riskhanteringssystem, dvs att öka sannolikheten för att bolaget ska uppnå de strategiska (verksamhetsnära) målen. Effekter av oönskade och oväntade händelser ska minimeras. Denna strategi gäller all verksamhet bolaget bedriver, oavsett om den utförs internt eller av extern part. Strategin ska alltid beaktas, oavsett om det gäller verksamhetsplanering, organisations- och verksamhetsutveckling eller system och tjänster.

Riskstrategin innebär att informationssäkerhetsarbetet ska bedrivas så att:

- IT-system och information fungerar och utvecklas så att de stödjer genomförandet av affärsstrategin
- Bolagets hantering av egen, kunders, anställdas och övriga intressenters information sker i enlighet med interna och externa regelverk

Bolaget ska därför ständigt sträva efter att uppnå och upprätthålla följande informationssäkerhetsmål:

- Att arbeta i enlighet med regelverk och riktlinjer
- Att ledning och styrelse besitter förmåga att arbeta strategiskt
- Att medarbetare har god kompetens inom informationssäkerhetsområdet

Ansvar

Styrelse

Styrelsen ska se till att bolagets hantering och kontroll av risker är tillfredsställande och har det yttersta ansvaret för bolagets arbete med informationssäkerhet. Styrelsen ansvarar för att upprätta och fastställa bolagets riktlinje för informationssäkerhet som en del av bolagets affärsstrategi. Styrelsen har i denna riktlinje angivit mål och inriktning för bolagets arbete med 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 informationssäkerhet. Vd ska även tillse att berörda parter/medarbetare regelbundet får lämplig utbildning inom informationssäkerhet och säkerhetsrisker.

Ansvar för informationssäkerhet

Bolagets ekonomichef har övergripande ansvar för hela riskhanteringsområdet. Informationssäkerhet är ett åtgärdsområde inom riskhanteringen. För planering, genomförande och uppföljning av informationssäkerhet ansvarar bolagets säkerhetschef. Detta inbegriper att:

- utveckla och förvalta ledningssystem för informationssäkerhet
- utveckla interna regler och säkerhetsåtgärder
- förvalta bolagets register över informationstillgångar
- genomföra riskbedömningar och hotbildsanalyser
- medverka i riskanalyser som berör informationssäkerhet samt uppdatering av riskregister
- uppföljning av informationssäkerhetsarbetet
- utvärdera bolagets informationssäkerhetsarbete

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

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
- genomföra obligatoriska utbildningar och säkerhetskampanjer anvisade av Göteborg Stad eller bolaget.

Leverantörer

Bolaget ska tillse att relevanta krav för tjänster och system uppfylls även när dessa utförs av extern part.

Informationssäkerhet ska beaktas i leverantörsrelationer och införande av nya system. Detta gäller även idrifttagande av nya moduler inom befintliga system.

Bolagets riktlinje för utlagd verksamhet förtydligar vilka regelverk som ska beaktas vid upprättande och uppföljning av avtal.

Verksamhet som inte utförs på uppdragsavtal ska kravställas och följas upp utifrån det Göta Lejon anser nödvändigt för att bolagets information ska hanteras säkert.

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 etcetera.

Ovanstående krav gäller även vid hantering av tredjepartsleverantörer.

Informationssäkerhet och bolagets riskhanteringssystem

Göta Lejon följer Göteborgs stads metod för säker informationshantering. Arbetet ska bedrivas systematiskt och långsiktigt och innehålla följande delar:

- Informationsklassificering
- Riskanalys
- Vidtagande av säkerhetsåtgärder
- Uppföljning

Bolaget ska tillse att det finns en uppdaterad förteckning över informationstillgångar enligt Göteborgs stads riktlinje för informationssäkerhet.

Bolaget ska ha uppdaterade processbeskrivningar som tillsammans med förteckningen över informationstillgångar utgör ett underlag för att kunna bedöma informationssäkerhetsrisker och hur informationssäkerhetsarbetet bedrivs på ett lämpligt sätt.

Hantering av informationssäkerhet och säkerhetsrisker ska vara en del av bolagets allmänna riskhanteringssystem och riskhanteringsprocess som finns beskrivet i bolagets riktlinje för riskhantering. I enlighet med bolagets riskstrategi gäller följande toleranser avseende informationssäkerhet och säkerhetsrisker:

- identifierade kvarstående avbrottsrisker ska hanteras i bolagets kontinuitetsplan
- myndighetssanktioner till följd av otillräcklig intern styrning och kontroll accepteras ej.

Informationssäkerhetsrisker ska inkluderas i bolagets riskregister som tas fram av bolaget tillsammans med funktionen för riskhantering.

Incidenter ska hanteras enligt bolagets incidenthantering.

IT-drift

Bolagets IT-drift utförs av Intraservice som därför ansvarar för att Göta Lejons IT har de säkerhetsåtgärder, rutiner och funktioner som krävs för att säkerställa en tillräckligt hög säkerhetsnivå i enlighet med externa och interna krav. Verksamheten bedrivs på uppdragsavtal och följs upp av Göta Lejon i enlighet med riktlinje för utlagd verksamhet.

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 informationssäkerhet. Särskilt när det kommer till informationssäkerhet samt IKT-risker ska riskhanteringsfunktionen:

- utgöra ett stöd till bolagets ledning i samband med fastställande och upprätthållande av bolagets informationssäkerhetsarbete
- 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 informationssäkerhetsriktlinjer
- samordna granskningar av operativa incidenter eller säkerhetsincidenter och rapportera granskningar till bolagets ledning och vd.

De närmare reglerna för funktionen finns i riktlinjer för riskhanteringsfunktionen.

Internrevision

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

Tillämpning

Denna riktlinje reglerar all informationsbehandling oavsett driftsmiljö och gäller oavsett om behandlingen sker internt eller hos en tjänsteleverantör av outsourcad verksamhet.

Riktlinjen ska göras tillgänglig 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 denna riktlinje, ska stadens 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.

Fastställande och efterlevnad

Denna riktlinje fastställs av styrelsen och träder i kraft dagen för beslut. Riktlinjen ska årligen fastställas av styrelsen även om inga ändringar beslutas. Ansvarig för uppdatering av riktlinjen är vd.

Alla medarbetare ansvarar för att denna riktlinje följs. Chefer i organisationen säkerställer att riktlinjen efterlevs och att kunskap om innehållet finns inom gruppen.