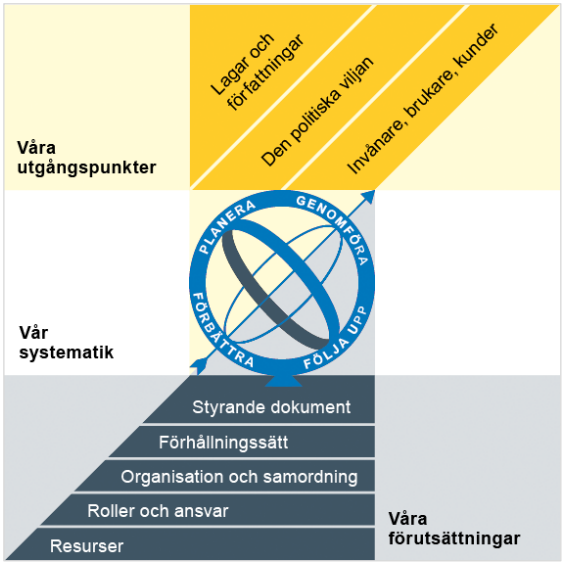
Göteborgs Stad

Försäkrings AB Göta Lejons riktlinje för säkerhet

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



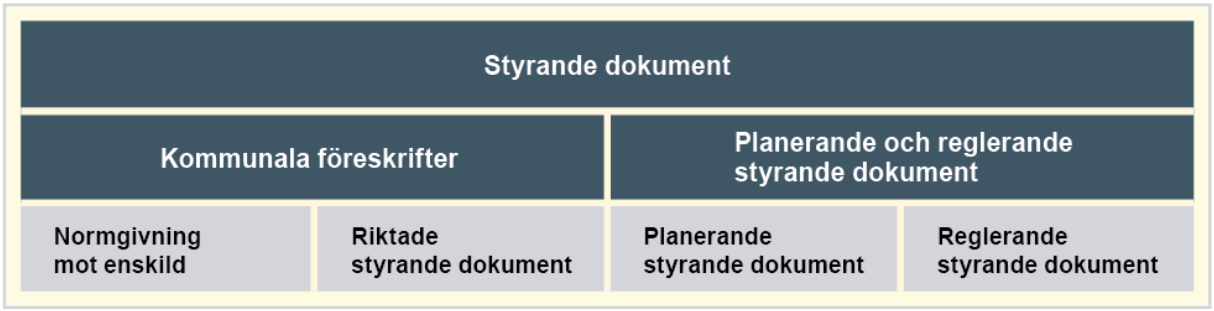
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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	FGL-2025-00123	§ 107 2025-06-12
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	2025-06-02	Säkerhetschef

Bilagor:

Innehåll

Inledning **4**
Syftet med denna riktlinje 4
Vem omfattas av riktlinjen 4
Lagbestämmelser 4
Koppling till andra styrande dokument 4
Riktlinje **6**
Säkerhetsstrategi 6
Riskhantering 6
Ansvar och roller 7
Styrelsen 8
VD 9
Processägare 9
Medarbetare 9
Kontinuitetshantering 9
Fysisk säkerhet 9
Incidenthantering 10
Informationssäkerhet 10
IT-drift 11
Hantering och övervakning, Oberoende funktion för informationssäkerhet 11
Internrevision 11
Leverantörer 12
Tillämpning 12
Fastställande och efterlevnad 12

Inledning

Syftet med denna riktlinje

Syftet med denna riktlinje är att ange bolagets strategi, principer och ansvar avseende Göta Lejons systematiska säkerhetsarbete för att främja en effektiv riskhantering och säkerställa erforderligt skydd rörande bolagets information. Särskild hänsyn är tagen för att säkerställa uppfyllnad av krav utifrån DORA förordningen.

Riktlinjen utgör Försäkrings AB Göta Lejons strategi för säkerhet.

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:

- Dora-förordningen (EU) 2022/2554
- EIOPA-BoS – 20/600: Riktlinjer för säkerhet och företagsstyrning avseende informations och kommunikationsteknik

Koppling till andra styrande dokument

Styrande dokument
Göteborgs stads säkerhetspolicy
Göteborgs stads riktlinje för informationssäkerhet
Göteborgs stads regel för IT användare
Göteborgs stads regler för användande av e-post
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 uppdragsavtal och utlagd verksamhet
Försäkrings AB Göta Lejons riktlinje för hantering och rapportering av händelser av väsentlig betydelse
Försäkrings AB Göta Lejons riktlinje för datakvalité
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 säkerhetsrisker, med särskild vikt på informations- och kommunikationstekniska risker samt informationssäkerhetsrisker, hanteras på lämpligt sätt.

Som captivebolag med verksamheten begränsad till koncernens egna risker tillämpar bolaget regelverket för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik (IKT) på ett sätt som står i proportion till arten, omfattningen och komplexiteten av bolagets inneboende risker.

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.

Göta Lejon integrerar informationssäkerhetsarbetet i IKT. I detta ingår även dataskydd.

Säkerhetsstrategi

Bolagets strategi för säkerhet grundar sig på den befintliga riskstrategin inom bolagets riskhanteringssystem, dvs att öka sannolikheten för att bolaget ska uppnå de strategiska (verksamhetsnära) målen. Säkerhetsstrategin fastställer en strukturerad och långsiktig inriktning för hur organisationen ska skydda sina tillgångar, säkerställa verksamhetens kontinuitet och bygga en motståndskraftig säkerhetskultur. Effekter av oönskade och oväntade händelser ska minimeras. Säkerhetsstrategin utgör även bolagets IKT-strategi.

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, dagligt arbete eller system och tjänster.

Målet med strategin är att:

- Säkerställa att bolaget efterlever lagar och förordningar samt övergripande krav utifrån tillsynsmyndigheter och Göteborgs Stad.
- Skydda information utifrån konfidentialitet, integritet, tillgänglighet och äkthet
- Förebygga samt ha kapacitet att upptäcka och hantera säkerhetsincidenter
- Etablera en god säkerhetskultur samt stärka medarbetares säkerhetsmedvetenhet och förståelse för individens ansvar

Riskhantering

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

- Identifierade säkerhetsrisker ska tas dokumenteras i bolagets riskregister
- Hantering av säkerhetsrisker ska analyseras, planeras för, följas upp och hanteras i enlighet med bolagets styrande dokument för risk och säkerhet
- Kvarstående säkerhetsrisker ska hanteras i bolagets kontinuitetsplan

- Myndighetssanktioner till följd av otillräcklig intern styrning och kontroll accepteras ej

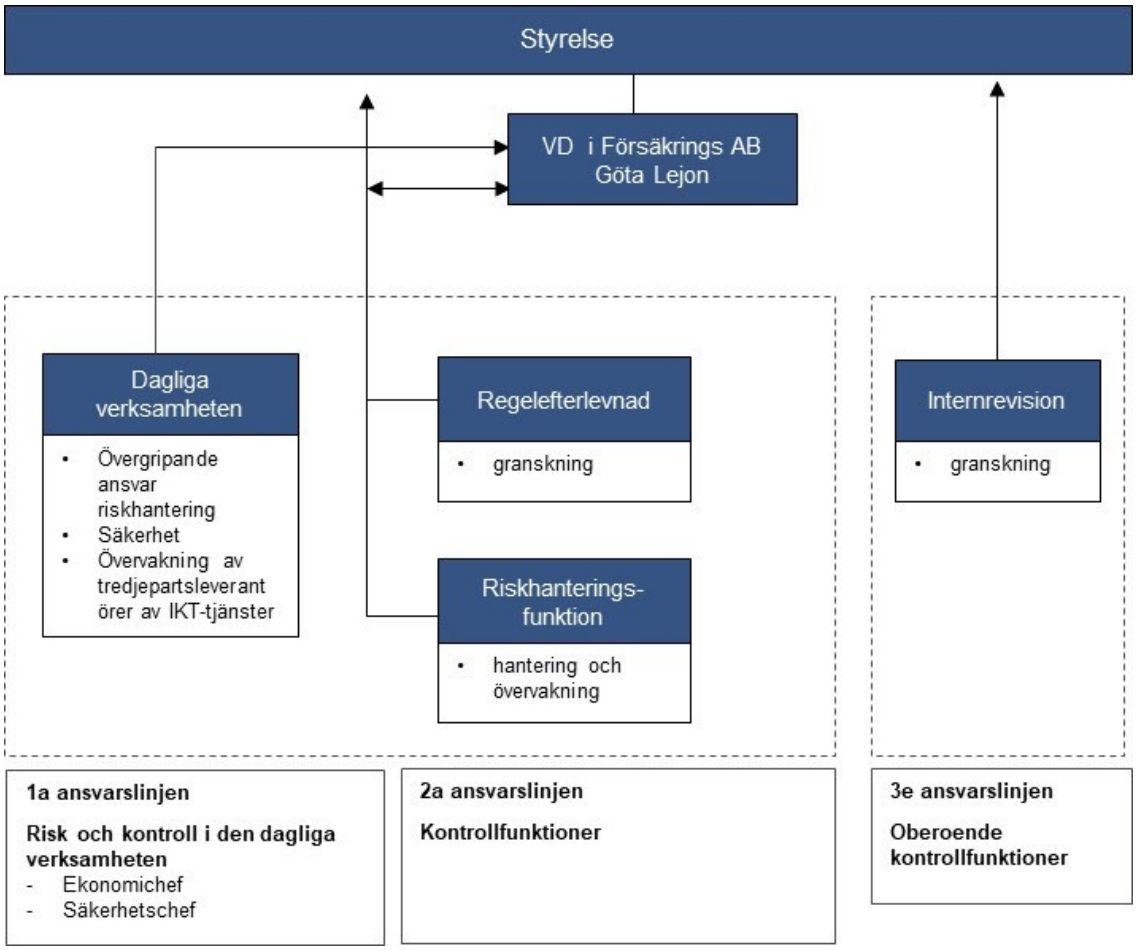
Ansvar och roller

Roller och ansvarsfördelning för säkerhetsarbetet beskrivs i Tabell 1.

Tabell 1: Roller och ansvarsfördelning för säkerhetsarbetet.

Område	Ansvar	Utförare/deltagare
Övergripande ansvar hela riskhanteringsområdet	Ekonomichef	
Rikskommitté	Ekonomichef	Säkerhetschef
Intern riskhantering, inkl. kontinuitetshantering och övervakning av IKT-tredjepartsleverantörer	Ekonomichef	
Intern säkerhet	Säkerhetschef	
Personsäkerhet	Säkerhetschef	Administratör
Fysisk säkerhet	Säkerhetschef	Administratör
Informationssäkerhet, inkl. säkerhetsskydd	Säkerhetschef	Processägare IT
Krisberedskap	Säkerhetschef	

Roller och ansvar avseende IKT och respektive försvarslinje beskrivs i Figur 1. Respektive roll förtydligas ytterligare i avsnitten om Hantering och övervakning, oberoende funktion för informationssäkerhet och internrevision.



Figur 1: Roller och ansvar avseende IKT relaterat till trelinjesmodellen.

Styrelsen

Styrelsen ska se till att bolagets hantering och kontroll av risker är tillfredsställande och har det yttersta ansvaret för bolagets säkerhetsarbete. Detta ansvar inkluderar att tillse att bolaget har en tillräcklig hantering av säkerhet. Styrelsen ansvarar för att sätta riktning, fatta beslut, tilldela resurser och följa upp säkerhetsarbetet samt även upprätta och fastställa bolagets styrande dokument som en del av bolagets affärsstrategi.

Inom säkerhetsområdet omfattar styrelsens ansvar specifikt att:

- Bedöma och förstå säkerhetsrisker på verksamhetsnivå
- Godkänna årliga riskanalyser och riskbedömningar
- Fatta beslut om riskaptit och toleransnivå
- Prioritera och resurssätta säkerhetsinsatser utifrån risk
- Ta del av årliga rapporter om säkerhetsarbetet
- Säkerställa att revisioner och tester genomförs
- Följa upp åtgärder efter incidenter eller avvikelser
- Fastställa relevanta riktlinjer
- Fastställa bolagets IKT-strategi, dvs säkerhetsstrategin

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 säkerhet. Vd ska även tillse att berörda parter/medarbetare har nödvändig kunskap genom lämplig utbildning inom säkerhetsområdena.

Processägare

Ansvarar för att:

- identifiera kritiska processer och risker inom sitt ansvarsområde
- säkerställa att informationsbärare och information är identifierad och att informationen är klassad utifrån bolagets anvisning för informationsklassning
- personal, inhyrda konsulter och kontrakterad tredje part är informerade om relevanta krav på säkerhet samt får tillgång till erforderlig utbildning

Medarbetare

Ansvarar för att:

- säkerställa efterlevnad i det dagliga arbetet och att aktivt ta del av de regler och krav som ställs på individen
- delta i de aktiviteter som beslutas av bolagets säkerhetsansvarig
- delta i hantering av inträffade säkerhetsincidenter
- genomföra obligatoriska utbildningar och säkerhetskampanjer anvisade av Göteborg Stad eller bolaget.

Kontinuitetshantering

Kontinuitetshantering avser den planering som behövs för att hantera och minimera negativa konsekvenser då avbrott sker i den dagliga verksamheten. Syftet är att säkerställa tillgång till kritiska resurser och funktioner för att upprätthålla prioriterad verksamhet vid störningar och kriser. Planerna ska regelbundet testas och uppdateras. Ekonomichef ansvarar för att kontinuitetsplaner är framtagna för bolagets kritiska processer och att beroenden är utredda och har nödvändiga åtgärder planerade.

Kontinuitetsplaneringen ska utgå från risk och konsekvensanalys där identifierade processer, system och resurser bedöms utifrån tidskritiska återställningskrav samt interna och externa beroenden. Det ska finnas upprättade kontinuitetsplaner för prioriterade funktioner samt återställningsplaner för kritiska och viktiga IT-system. Nödvändiga rutiner för kommunikation och kriskommunikation ska upprättas, både internt och externt. Planer ska testas årligen och lärdomar ska återföras genom uppdaterade planer.

Fysisk säkerhet

Med fysisk säkerhet avses skydd för verksamhetens personal, lokaler, informationstillgångar och utrustning från skadegörelse, brand, stöld, obehörig åtkomst samt andra fysiska hot. Säkerhetsåtgärder ska definieras oavsett om det gäller bolagets egna lokaler eller tjänsteleverantörer. Åtgärder ska

dokumenteras och genomföras för att skydda lokaler, datacenter och känsliga områden från obehörigt tillträde med hjälp av passerkort, nycklar eller kodlås. Tillträde ska endast beviljas till behörig personal och besökare ska registreras i reception, bära besöksbricka och ha en följeslagare i skyddade områden.

Åtkomst ges efter principen minsta möjliga behörighet och bör granskas regelbundet. Skyddade områden som kan vara känsliga är ex. serverrum, nätverksskåp eller teknikrum och dessa bör skyddas med ex. larm, kameraövervakning eller brandklassade dörrar. Alla lokaler ska ha brandskydd enligt gällande lagar och förordningar.

Incidenthantering

Bolaget ska säkerställa att säkerhetsincidenter hanteras snabbt, korrekt och spårbart för att minimera skador på verksamheten, information och infrastruktur. Alla incidenter ska rapporteras omgående och dessa ska bedömas utifrån allvarlighet, påverkan (verksamhet, information, system) samt om incidenten rör utpekad kritiskt/viktigt system eller personuppgifter. Säkerhetsincidenter ska hanteras enligt bolagets styrande dokument avseende incidenthantering.

Informationssäkerhet

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

Göta Lejon 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. Detta inkluderar även äkthet, i form av säkerställande av sändare och mottagare.
- Tillgänglighet, att information är tillgänglig och användbar när den behövs.

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.

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

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

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.

Hantering och övervakning, Oberoende funktion för informationssäkerhet

I enlighet med Dora-förordningen, Artikel 6:4 samt EIOPA-BoS – 20/600 ska bolaget ska ha en oberoende funktion eller person för hantering och övervakning av informationssäkerhet. Riskhanteringsfunktionen ansvarar för att identifiera och bedöma risker kopplade 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

I enlighet med Dora-förordningen Artikel 6:6 ska området för IKT och informationssäkerhet ingå som i internrevisionens granskningsplan med lämplig frekvens, (se också riktlinje för internrevision).

Leverantörer

Bolaget ska tillse att relevanta krav för tjänster och system uppfylls även när dessa utförs av extern part. Säkerhetskraven ska beaktas i leverantörsrelationer och införande av nya system. Detta gäller även idrifttagande av nya moduler inom befintliga system eller då större förändring sker exempelvis genom uppdatering till nya versioner.

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. Samtliga arrangemang med tredjepartsleverantörer av IKT-tjänster ska årligen sammanställas och övervakas avseende riskexponering och relevant dokumentation. Ansvarig för detta är ekonomichef

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. Det ska även säkerställas att Göta Lejon har möjlighet att rapportera nödvändig information som ska levereras till Finansinspektionens informationsregister.

Ovanstående krav gäller även vid hantering av tredjepartsleverantörer.

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 utlagd 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.