Informationssäkerhetspolicy

Sammanfattning

Vår informationssäkerhetspolicy omfattar alla delar av vår koncern och verksamhet samt all den information som vi äger eller förvaltar. Vårt arbete med informationssäkerhet ska verka för bevarandet av konfidentialitet, riktighet och tillgänglighet av våra informationstillgångar, system och resurser. Framgångsrikt informationssäkerhetsarbete möjliggör uppfyllandet av vår affärsidé, bibehållandet av våra kärnvärden och förverkligandet av vår vision.

Innehåll

Introduktion

Ledningen för Göteborg Energi anser att ändamålsenlig informationssäkerhet är avgörande för uppfyllandet av vår affärsidé, bibehållandet av våra kärnvärden och förverkligandet av vår vision. Vi åtar oss därför att arbeta aktivt med informationssäkerhet för att säkerställa ett säkert, ansvarsfullt och hållbart Göteborg Energi.

Göteborg Energi förpliktar sig till ett långsiktigt och kontinuerligt engagemang för informationssäkerhet, vilket omfattar alla delar av vår koncern och verksamhet samt all den information som vi äger eller förvaltar.

Information är kunskap eller data som har ett värde, betydelse eller syfte i ett sammanhang och kan vara allt som innehåller och allt som bär information. Sådan information betraktas som en informationstillgång som behöver skyddas från ett brett spektrum av hot och risker när de behandlas, överförs och förvaras. Vårt informationssäkerhetsarbete ska därför verka för att säkerställa att endast behöriga personer kan ta del av dem (konfidentialitet), att de är korrekta och inte manipulerade (riktighet) samt att de finns tillgängliga när de behövs (tillgänglighet).

Omfattning

Den här policyn gäller för hela Göteborg Energi koncern, för alla våra bolag och enheter, verksamhets- och affärsområden. Den gäller för alla anställda och konsulter såväl som för våra partners, leverantörer och tredje parter som har tillgång till informationstillgångar som är under Göteborg Energis ansvar eller kontroll.

Syfte

Göteborg Energis arbete med informationssäkerhet har som syfte att:

- bevara informationens konfidentialitet, vilket innebär att den ska skyddas mot obehörig insyn så att den inte tillgängliggörs eller avslöjas för obehöriga
- bevara informationens riktighet, vilket innebär att den ska skyddas mot oönskad förändring så att den förblir korrekt och fullständig
- bevara informationens tillgänglighet, vilket innebär att den ska vara åtkomlig och användbar av behörig person när den behövs.

Mål

Göteborg Energis arbete med informationssäkerhet har som mål att:

- bidra till att uppnå överordnade strategier och mål genom en balans mellan säkerhet, affärs- och verksamhetsnytta
- främja säker, tillförlitlig och tillgänglig information
- motsvara våra kunder, partners, leverantörer och interna intressenters förväntningar och krav
- stödja och möjliggöra moderna tjänster och verktyg, digitalisering och användandet av ny teknik

- förtroendet för oss, vår verksamhet, produkter eller tjänster inte påverkas negativt som en konsekvens av bristande informationssäkerhet
- identifiera, bedöma och hantera våra informationssäkerhetsrisker så att de når nivåer som Göteborgi Energi kan acceptera
- säkerställa vår efterlevnad av rättsliga krav relaterade till informationssäkerhet
- främja ständig förbättring av lämplighet, tillräcklighet och verkan av vår informationssäkerhet.

Principer

Göteborg Energis informationssäkerhetsarbete ska utgå från följande principer:

1. vi anpassar uppdrag, aktiviteter och mål till överordnade strategier så att vår informationssäkerhet stödjer överordnade mål
2. vårt arbete prioriteras med utgångspunkt från det som ger störst effekt i förhållande till risk. Säkerhetsåtgärder ska reducera informationssäkerhetsrisker till acceptabla nivåer
3. vi investerar med utgångspunkt från det som ger värde och som stödjer överordnade strategiska mål
4. vårt arbete sker i samarbete och samverkan för att identifiera, definiera och hantera de processer, verksamheter och funktioner som har betydelse för vår informationssäkerhet
5. vi arbetar fortlöpande med utbildning och fortbildning för ökad medvetenhet. Vi höjer kunskap och förståelse samt tydliggör ansvar
6. vårt arbete med informationssäkerhet ska kontinuerligt följas upp och utvärderas för att vi ska kunna fatta effektiva beslut, identifiera brister och framsteg samt utvärdera ifall krav och mål uppnås
7. vi integrerar informationssäkerhet i vår verksamhetsstyrning och processer. Informationssäkerhet är en självklarhet i användandet av informationstillgångar, resurser och system
8. våra säkerhetsåtgärder ska verka enligt devisen lätt att göra rätt och svårt att göra fel. En kombination av människa, process och teknik bidrar till att uppnå målbilden
9. vi accepterar eller tolererar aldrig situationer som utifrån ett informationssäkerhetsperspektiv skulle medföra att vi inte efterlever rättsliga krav
10. våra säkerhetsåtgärder sker löpande och kontinuerligt. Vi väntar inte på att allt ska vara klart för att vidta åtgärder eftersom vi förstår att även mindre säkerhetshöjande åtgärder stärker vår samlade informationssäkerhet.

Roller och ansvar

Som grundprincip gäller att ansvaret för vår informationssäkerhet följer det ordinarie verksamhetsansvaret, från styrelse till enskild individ och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom dennes ansvarsområde.

Nedan beskrivs informationssäkerhetsansvaret för ett urval av roller. Specificerade ansvar och åligganden beskrivs utförligare i riktlinjer och andra styrande dokument för informationssäkerhet.

Alla

Alla (anställda, konsulter, leverantörer och tredje part) ansvarar för:

- att förstå, känna till och följa denna policy såväl som alla andra relevanta regler, bestämmelser, processer och aktiviteter som implementerar denna policy
- att rapportera händelser och avvikelser relaterade till informationssäkerhet.

Linjechefer

Linjechefer ansvarar för:

- att informera medarbetare inom det egna ansvarsområdet om denna policy såväl som alla andra regler, bestämmelser, processer och aktiviteter som implementerar denna policy utifrån dess relevans för medarbetarnas arbete och uppdrag
- att bidra till efterlevnad av denna policy och koncernens styrning av informationssäkerhet i den organisation som linjechefen ansvarar för
- att rapportera händelser och avvikelser relaterade till informationssäkerhet.

Styrelsen och Verkställande direktören (VD)

Styrelsen har det yttersta ansvaret för informationssäkerheten och ansvarar därtill för:

- att godkänna denna policy
- att kontinuerligt följa upp och utvärdera arbetet med informationssäkerhet.

VD ansvarar för:

- att säkerställa att denna policys syfte, mål och principer verkställs och efterlevs
- att säkerställa de resurser och utse de personer som krävs för implementering av denna policy.

Chef för Informations- och IT-säkerhet (CISO)

CISO ansvarar för:

- att utveckla, leda, samordna och kontrollera koncernens arbete med informationssäkerhet
- att leda och samordna signalskyddstjänsten
- att säkerställa genomförandet av koncernövergripande säkerhetsåtgärder som är nödvändiga för att implementera denna policy
- att bistå ansvariga för informationssäkerhet i arbetet med att fullfölja sitt informationssäkerhetsansvar

- att regelbundet rapportera till högsta ledningen och koncernens exekutiva ledning hur arbetet med informationssäkerhet fungerar och ge råd om hur det kan utvecklas
- att säkerställa att denna policy revideras minst årligen med utgångspunkt från genomförda analyser och vidtagna säkerhetsåtgärder.

Chef för Säkerhet/Säkerhetsskydd

Säkerhetschefen, tillika säkerhetsskyddschefen ansvarar för:

- att leda, samordna och kontrollera säkerhetsskyddsarbetet, d.v.s. det som utgör säkerhetskänslig verksamhet (Sveriges säkerhet). Säkerhetsskyddschefen samråder i dessa frågor med CISO vad avser informationssäkerhet och signalskyddstjänsten.

Informationsägare

Informationsägare ansvarar för:

- att säkerställa att information under dennes ansvar hanteras i enlighet med denna policy såväl som alla andra regler, bestämmelser, processer och aktiviteter som implementerar denna policy
- att hantera informationssäkerhetsrisker relaterade till dennes information överallt där den behandlas, överförs och förvaras.

Objektägare

Objektägare ansvarar för:

- att säkerställa att förvaltningsobjekt under dennes ansvar efterlever informationssäkerhetskrav i denna policy såväl som alla andra regler, bestämmelseer, processer och aktiviteter som implementerar denna policy.

Avvikelser och uppföljning

Vi bidrar alla till och har ett delat ansvar för att säkerställa en väl fungerande informationssäkerhet. I det ingår att rapportera när brister upptäcks eller händelser och incidenter inträffar.

Disciplinära åtgärder

Överträdelse av informationssäkerhetsbestämmelser kan leda till konsekvenser i form av rättsliga, disciplinära eller andra åtgärder.

Uppföljning

Göteborg Energi förbehåller sig rätten att genomföra uppföljning och kontroll av efterlevnad av denna policy. Det kan inkludera, men är inte begränsat till teknisk övervakning och kontroll, kontroll av system och resurser, kontroll av fysiska lokaler och utrymmen samt interna eller externa revisioner och uppföljningar.

Fastställelse och godkännande

Styrelsen för Göteborg Energi koncern och dess verkställande direktör har den 1 december 2022 fastställt och godkänt denna informationssäkerhetspolicy.