Castras ledningssystem för informationssäkerhet

2025-02-12

V 1.7

Informationssäkerhetspolicy

Syfte

Inom Castra Group AB och dess dotterbolag är informationen en nyckelresurs. Vår informationssäkerhetspolicy är fastställd av Castras ledningsgrupp och anger Castras grundläggande synsätt samt viljeinriktning på en övergripande nivå gällande arbetet med informationssäkerhet. Policyn omfattar all information inklusive det stöd som finns för att tillhandhålla information, såsom IT-system, datornät, servrar och arbetsstationer.

Samtliga informationstillgångar som Castra hanterar både internt och externt är av allra högsta betydelse för vår verksamhet. En informationstillgång inkluderar samtlig information som är av värde för Castra, våra kunder och våra samarbetspartners oavsett om de behandlas automatiskt eller manuellt, analogt eller digitalt samt oberoende av dess form eller den miljö den förekommer i. Syftet med denna informationssäkerhetspolicy är att påvisa vår vilja att dessa informationstillgångar behandlas efter våra uppsatta mål och principer. Castras förtroende hos våra medarbetare, samarbetspartners och kunder bygger på att vi hanterar dessa korrekt. All informationshantering ska vara kostnadseffektiv och stödja företagets övergripande mål. Det är därför grundläggande att vi hanterar vår egen, våra kunders, partners och övriga intressenters information på ett säkert och effektivt sätt. Informationssäkerhet innebär för oss att:

Vårt informationssäkerhetsarbete bygger på fyra grundpelare:

- Konfidentialitet: Att information skyddas mot obehörig insyn.
- Riktighet: Att information skyddas mot oönskad förändring eller raderande.
- Tillgänglighet: Att information görs åtkomlig för behörig person vid rätt tillfälle.
- Spårbarhet: Att informationsförändringar går att följa i dess led.

Målbilden för vårt informationssäkerhetsarbete är att:

- Castra skall präglas av en stark informationssäkerhetskultur där vi skyddar vår egen och våra kunders information.
- Castra skall medverka till att sprida en sund informationssäkerhetskultur genom att vara en förebild och ligga i framkant med vårt informationssäkerhetsarbete.

Roller och ansvar

Ansvaret för informationssäkerhetsarbetet ska följa det normala delegerade verksamhetsansvaret på alla nivåer.

Ägare och styrelse: Uttrycker mål och principer genom att fastställa Castras informationssäkerhetspolicy.

Ledningsgrupp: Har det yttersta verksamhetsansvaret inklusive informationssäkerhetsarbetet. Godkänner och fastställer regelverket samt äger och ansvarar för infrastruktur, tjänster, system, applikationer samt tillsätter CISO, informationsägare och systemägare.

IT-ansvarig: Ansvarig för att känna till de IT-säkerhetskrav som finns och att företaget uppfyller dessa. Leder och ansvarar över kontinuitetsplaneringen, revisioner och förbättringsarbetet inom IT samt fattar beslut kring eskaleringar vid incidenter. Arbetar tätt med CISO och leder även arbetet kring drift, IT-säkerhet såväl som behörigheter.

CISO: Ansvarar för att känna till de informationssäkerhetskrav som finns och att företaget uppfyller dessa. Leder arbetet kring riskanalyser, informationsklassificering, styrdokument och rutinerna kopplade till informationssäkerheten. Ansvarar för utbildning av alla medarbetare samt de personer som har tillgång till säkerhetsklassad information som tillhandahålls eller behandlas av Castra samt arbetar tätt tillsammans med IT-ansvarig kring frågor om informationssäkerhet.

Informationsägare: Ansvarar för att förvalta och tillgodose konfidentialitet, riktighet, tillgänglighet och spårbarhet för den information de är utsedda att ansvara för. Arbetet sker utifrån riskbedömning och säkerhetsklassificering av informationsobjekten.

Systemägare: Ansvarar för system som hanterar informationsobjekt och säkerställer att dessa uppfyller krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Verksamhetsansvarig: Vägleder medarbetarna och ansvarar för att de känner till arbetet kring framför allt informationssäkerhet och incidenthanteringen.

Alla medarbetare: Samtliga medarbetare och andra verksamma inom Castra som behandlar informationstillgångar har ett ansvar att hantera information på ett korrekt sätt genom att följa de policy och riktlinjer som organisationen satt upp.

Leverantörer, partners och övriga externa kontakter: Ansvarar för att vara medvetna om de krav Castra ställer på informationssäkerhet och efterleva detta i sina egna organisationer.

Deltar i utvecklingen av informationssäkerhetsarbetet i de fall där de ansvarar för information eller system som ägs eller nyttjas av Castra.

Granskning och revision

Castra bedriver ett kontinuerligt revisionsarbete där ledningssystem och dess vidhängande dokumentation gås igenom och uppdateras löpande, minst en gång per år. Detta för att kunna upprätthålla ett kontinuerligt förbättringsarbete och säkerställa policyns riktighet och kvalitet. Utöver detta sker även förändringar löpande efter uppdatering av standarder, incidenter eller andra förändringar i Castra eller Castras omvärld som påverkar informationssäkerheten. I de fall avsteg behöver göras från beslutade policys och riktlinjer rörande informationssäkerhet så finns det tydliga regler och rutiner för hur tillfälliga avvikelser och undantag ska hanteras samt dokumenteras i incidenthanteringsprocessen. Ett avsteg rapporteras och analyseras alltid som en risk med målsättningen att mitigera avsteget och om möjligt lyfta in det i det ordinarie arbetet.

Denna informationssäkerhetspolicy är aktuell och beslutad av Castras ledningsgrupp och uppdaterades senast den 23 januari 2025.

Relaterade dokument

Informationssäkerhetspolicyn beskriver målbilden för Castra med sitt informationssäkerhetsarbete. Utöver detta dokument finns ytterligare policys och riktlinjer i organisationen som i detalj beskriver regelverk och processer för verksamheten som bidrar till att informationssäkerhetspolicyn ska kunna efterlevas.