STERA DATASÄKERHETSPOLICY

Denna policy beskriver målet med och riktlinjerna för Stera-koncernens (”Stera”) datasäkerhetspolicy samt ansvar och organisation.

I denna policy innebär datasäkerhet att säkerställa datans sekretess, integritet och användbarhet, oavsett hur den presenteras. Denna policy definierar de grundläggande kraven på datasäkerhet och skapar ett underlag för planering och genomförande av aktiviteter i enlighet med policyn. För att stödja genomförandet av policyn utarbetas även mer detaljerade riktlinjer för datasäkerhetens olika delområden.

Datasäkerhet förverkligas och utvecklas på ett riskorienterat sätt med lämpliga och kostnadseffektiva lösningar. Stera-koncernens ledningsgrupp för dataadministration utvärderar årligen datasäkerhetspolicyns lämplighet.

Datasäkerhetspolicyn är, tillsammans med Steras värden, riskhanterings-, säkerhets- och dataskyddspolicyer, en viktig del av god förvaltning i Stera.

Målet med datasäkerhetspolicyn

Det primära målet med datasäkerhet är att under alla omständigheter säkerställa kontinuiteten i den verksamhet som Stera-koncernen ansvarar för. Målmedveten och effektiv datasäkerhet möjliggör IKT-lösningarnas användbarhet relaterade till Steras verksamhet, integriteten hos data som används i processer och tjänster samt sekretess under alla omständigheter i alla verksamhetsländer. Denna policy lägger grunden för att säkerställa säkerheten för Stera-koncernens informationssystem och databehandling.

Hos Stera är säkrandet av kunduppgifter och data som produceras och behandlas av andra digitala funktioner en väsentlig del av den ansvarsfulla verksamhet som både våra kunder och våra partner kräver av Stera. Digitaliseringens framväxt gör att datasäkerhet i allt högre grad regleras genom lagstiftning. Varje medarbetare i Stera-koncernens alla verksamhetsländer måste följa datasäkerhetspolicyn, dess kompletterande principer och instruktioner samt tillämplig lagstiftning.

Implementering av datasäkerhet

Riskbedömning

Datasäkerhetsrisker bedöms och analyseras regelbundet utifrån deras affärspåverkan. Man måste också utarbeta en riskbedömning under utformningsfasen av nya system och i samband med stora förändringar som påverkar verksamhetens kritiska områden.

Klassificering av datahantering

Stera använder en datahanteringsklassificering där man beskriver klassificering av data och betydelsen av data för verksamheten, samt tar hänsyn till åtkomsträttigheter.

Behandling av personuppgifter

Datasäkerhetspolicyn och -riktlinjerna beskriver hur personuppgifter behandlas hos Stera.

Datasäkerhetskrav

Steras datasäkerhetskrav bestämmer den lägsta nivå av datasäkerhet som krävs av företagets avtalspartner. Vid behov kan man även fastställa en tillräcklig nivå av datasäkerhet genom revisioner.

Utbildning i datasäkerhet

Stera vidtar regelbundet en mängd olika åtgärder för att förbättra medvetenheten om datasäkerhet hos medarbetare. Dessa omfattar exempelvis utbildningar online, simuleringar av bluffmeddelanden och nyheter på intranätet. Dessutom anordnas riktad datasäkerhetsutbildning för utvalda målgrupper. Utbildningarna planeras delvis i samarbete med HR-teamet. Komplettering av medarbetares kompetensmatriser i nödvändiga delar och datasäkerhet beaktas i framtida utbildningsplaner.

Kontroll och uppföljning

För att förbättra och upprätthålla datasäkerhetsnivån krävs systematisk och kontinuerlig automatisk kontroll av hur informationssystemen fungerar. Enligt lag har personer som bedriver kontroll tystnadsplikt om de data de behandlar i sitt arbete.

Datasäkerhetsläget rapporteras i samband med normal intern kontroll samt vid interna och externa revisioner. Den tekniska datasäkerheten utvärderas kontinuerligt och separata säkerhetsrevisioner genomförs i de viktigaste miljöerna.

Hantering av datasäkerhetsintrång

Stera har rutiner och tjänster för att upptäcka datasäkerhetsintrång. Eventuella datasäkerhetsöverträdelser behandlas av dataadministrationen och rapporteras till koncernens ledningsgrupp.

Datasäkerhetsbrott

Ett datasäkerhetsbrott definieras som en aktivitet som bryter mot datasäkerhetspolicyn och -riktlinjerna.

Ansvar och organisation

Datasäkerhetspolicyn godkänns av Stera-koncernens ledningsgrupp.

Datasäkerhetspolicyn omfattar verksamheten hos Steras företag i alla länder där Stera är verksamt. Steras personal måste följa policyn. Steras företag och enheter ansvarar för att policyn och nödvändiga resurser implementeras i den egna verksamheten.

VD ansvarar för att Stera har en välfungerande datasäkerhet som en del av riskhanteringssystemet. VD genomför datasäkerhet med hjälp av koncernens dataadministration. Dataadministrationen behandlar och övervakar koncernens datasäkerhetsrisker och genomförandet av riskhanteringsåtgärder samt rapporterar om dessa till koncernledningen.

Ansvaret för att implementera datasäkerhet ligger på medlemmarna i koncernens ledningsgrupp. Dataadministrationen koordinerar och utvecklar datasäkerhetsprocesser, ansvarar för praktiskt genomförande tillsammans med tjänsteleverantörer, ansvarar för rapportering och utför, tillsammans med affärsfunktioner och gemensamma funktioner, identifiering av datasäkerhetsrisker och fastställande av ledningsåtgärder. Varje Stera-medarbetare måste kunna identifiera och reagera på datasäkerhetsrelaterade risker som påverkar hans eller hennes eget arbete eller koncernen i allmänhet. Utbildningarnas omfattning och inriktning följs upp i samarbete med Steras eget HR-team.

Styrning av datasäkerhet

BCP-verksamhetsmodellen fungerar som en mekanism för styrning av datasäkerhet och där datasäkerhet har sin egen del. I enlighet med sin arbetsordning övervakar och utvärderar Stera-koncernens ledningsgrupp bland annat hur effektiv Steras interna kontroll, internrevision och BCP-verksamhetsmodell är. Koncernens ledningsgrupp hanterar koncernens främsta datasäkerhetsrisker tillsammans med IT-teamet.

Ikraftträdande

Godkänd av Stera-koncernens ledningsgrupp, Åbo 12.12.2022.