Informationssäkerhetspolicy

1. Bakgrund och syfte

Att hantera information är grunden till Eviras verksamhet. Att information hanteras korrekt är av betydelse för förtroende inom bolaget samt externt för kunder och samarbetspartners. Syftet med denna policy är att påvisa vårt åtagande att hantera information på ett adekvat sätt.

Informationssäkerhet kan sammanfattas i följande fyra kravområden:

- Tillgänglighet: att information finns tillgänglig vid behov för behöriga användare
- Korrekthet: att information skyddas från inkorrekt förändring eller borttagning
- Konfidentialitet: att information endast finns tillgänglig för behöriga användare
- Spårbarhet: att åtkomst och ändringar av konfidentiell information ska vara spårbar

Med fastställandet av denna policy åtar sig Evira att följa tillämpliga krav rörande informationssäkerhet och ansvarsförhållanden.

2. Omfattning

Denna policy gäller för all information som hanteras av verksamheten, oavsett format, inklusive men inte begränsat till, elektronisk, tryckt och muntlig information. Policyn gäller för alla anställda, konsulter, leverantörer och andra eventuella parter som hanterar information.

3. Riktlinjer och principer

Evira åtar sig:

- att fortlöpande arbeta med kunskapsutveckling om hur informationssäkerhet upprättas och säkerställs inom verksamheten,
- att vid behov ta hjälp av extern expertis,
- att hantera information som känslig om inte annat anges,
- att fortlöpande utvärdera och bedöma hot och risker,
- att arbeta förebyggande mot hot och risker för att förebygga oönskade effekter,
- att arbeta med informationssäkerhet som en naturlig och integrerad del i verksamhetens rutiner och
- att ledningssystem, säkerhetsåtgärder och krishanteringsplaner återkommande revideras och uppdateras.

4. Ansvar

Ansvaret för att upprätthålla Eviras arbete med informationssäkerhet ska följa verksamhetens normala strukturer. Medarbetare har ett individuellt ansvar att lyfta potentiella brister eller risker som uppdagas.

Om avvikelser sker eller undantag görs från denna policy eller övriga rutiner för informationssäkerhet ska dessa rapporteras till närmaste chef och rapporteras vidare till ledningsgruppen. Allvarliga överträdelser rapporteras till lämpligt skyddsorgan eller myndighet.

5. Uppföljning & revision

Denna policy och övriga rutiner för informationssäkerhet ska granskas och uppdateras årligen eller om betydande förändringar sker inom Evira eller i omvärlden. Granskningen syftar till att säkerställa policyns relevans och riktighet men också för att säkerställa att det finns en genomgående medvetenhet om policyn och övriga rutiner inom organisationen.

6. Informationssäkerhetspolicyns giltighet

Policyn fastställdes av Eviras ledningsgrupp och ägare 2023-07-03 och gäller till och med 2026-02-28.