Politik for informationssikkerhed

Opdateret den 13. maj 2026

Formål og ambition

Informationssikkerhed er fundamentet for **FAKTURASERVICE A/S**. Vores kunder betror os deres mest kritiske regnskabs- og fakturadata, og vi er bevidste om vores ansvar for at beskytte disse data mod tab, misbrug og uautoriseret adgang.

Vores ambition er at opretholde et sikkerhedsniveau, der gør os til en troværdig partner for både private virksomheder og offentlige myndigheder, samt at sikre vores fortsatte adgang til kritiske infrastrukturer som PEPPOL og Nemhandel.

Overordnede sikkerhedsmål

For at styre vores indsats har ledelsen fastlagt følgende hovedmål:

- **Certificering:** Vi vil opnå og vedligeholde en ISO/IEC 27001:2022-certificering senest 1. juli 2027.
- **Tilgængelighed:** Vores SaaS-løsninger, Onlineregnskab.dk og Fakturaservice.dk, skal være tilgængelige og stabile for vores kunder.
- **Integritet og fortrolighed:** Vi beskytter kundedata og e-dokumenter mod uautoriserede ændringer og sikrer, at kun de rette personer har adgang.
- **Compliance:** Vi efterlever gældende lovgivning, herunder bogføringsloven og GDPR, samt de specifikke krav fra Erhvervsstyrelsen og OpenPeppol.

Strategi og arbejdsmetode

Vores tilgang til sikkerhed er risikobaseret. Det betyder, at vi prioriterer vores ressourcer der, hvor risikoen for vores forretning og vores kunder er størst.

- **NorthGRC** er vores centrale "sandhedskilde" og værktøj til at styre risici, kontroller og dokumentation.
- Sikkerhed skal være en naturlig del af vores daglige drift og softwareudvikling, ikke en separat administrativ byrde.
- Vi forpligter os til løbende forbedring af vores ledelsessystem for informationssikkerhed (ISMS).

Roller og ansvar

- **Ledelsen** har det overordnede ansvar for informationssikkerheden og sikrer, at de nødvendige ressourcer er til rådighed.
- **Informationssikkerhedschefen** koordinerer det daglige arbejde og opfølgning i NorthGRC.
- **Alle medarbejdere** har et ansvar for at efterleve politikker og procedurer samt rapportere eventuelle sikkerhedshændelser eller svagheder.

Revision og opfølgning

Denne politik gennemgås mindst én gang årligt af ledelsen eller ved væsentlige ændringer i virksomhedens risikobillede eller forretningsmodel. Politikken er tilgængelig for alle medarbejdere og relevante interessenter.