EmbedPolicy – Tekniske og organisatoriske sikkerhedsforanstaltninger

Version: 0.1
Status: Foreløbig sikkerhedsbeskrivelse
Dokumentejer: Beezy365 A/S

1. Formål

Dette dokument beskriver EmbedPolicys overordnede tilgang til tekniske og organisatoriske sikkerhedsforanstaltninger.

Formålet er at understøtte en passende beskyttelse af personoplysninger og en stabil og sikker drift af løsningen.

Dokumentet indgår i leverandørens sikkerhedsdokumentation og skal læses sammen med databehandleraftalen og risikovurderingen.

2. Systemarkitektur og kundeadskillelse

EmbedPolicy er udviklet som en webbaseret SaaS-løsning.

Systemet anvender en arkitektur med særskilte databaser for de enkelte kunder.

Denne opdeling er valgt for at understøtte adskillelse af kundernes oplysninger og begrænse risikoen for utilsigtet adgang mellem kunder.

Den faktiske isolation skal løbende verificeres gennem teknisk kontrol og test.

3. Adgangsstyring

EmbedPolicy anvender brugerkonti og rollebaseret adgangsstyring.

Adgang til administrative funktioner og oplysninger skal begrænses til autoriserede brugere med et relevant arbejdsbetinget behov.

Følgende forhold indgår i sikkerhedskontrollen:

- Oprettelse og nedlæggelse af brugere.
- Tildeling og ændring af adgangsrettigheder.
- Begrænsning af privilegerede rettigheder.
- Sikker autentifikation.
- Krav til multifaktorautentifikation, hvor dette er fastlagt i databehandleraftalen.

Den konkrete implementering og håndhævelse af multifaktorautentifikation skal verificeres.

4. Kommunikation og datatransmission

Kommunikation mellem brugere og EmbedPolicy foregår via HTTPS.

Krypteret kommunikation anvendes til at beskytte data under overførsel.

Relevante sikkerhedsindstillinger for servere, certifikater og eksterne integrationer indgår i den tekniske kontrol.

5. Versionsstyring og publicering

EmbedPolicy understøtter versionsstyring af privatlivspolitikker.

Dette gør det muligt at adskille arbejdet med indhold fra den offentliggjorte version.

Publiceringsprocessen skal understøtte, at ændringer kan kontrolleres inden offentliggørelse, og at tidligere versioner kan identificeres.

Rettighedskontrol, ændringshistorik og muligheder for genopretning skal indgå i sikkerhedstests.

6. Backup og gendannelse

Der skal foreligge procedurer for sikkerhedskopiering og gendannelse af relevante system- og kundedata.

Procedurerne skal omfatte:

- Backupfrekvens.
- Opbevaring og adgangsbeskyttelse.
- Kontrol af backup.
- Test af gendannelse.
- Håndtering af fejl og datatab.

Konkrete backupintervaller, opbevaringsperioder og gendannelsestider dokumenteres efter verificering af driftsopsætningen.

7. Logning og hændelseshåndtering

Relevante system- og sikkerhedshændelser skal kunne undersøges.

Der skal være procedurer for registrering, vurdering og håndtering af sikkerhedshændelser.

Ved brud på persondatasikkerheden skal Beezy365 A/S bistå kunden i overensstemmelse med databehandleraftalen og gældende databeskyttelsesregler.

Logningens omfang, opbevaringsperiode og adgangsbeskyttelse skal dokumenteres.

8. Vedligeholdelse og sårbarheder

EmbedPolicy vedligeholdes med henblik på at begrænse kendte sikkerhedssårbarheder.

Dette omfatter relevant vedligeholdelse af applikationskode, softwareafhængigheder, servermiljø og integrationer.

Der arbejdes med at etablere og dokumentere en fast procedure for sikkerhedsopdateringer, sårbarhedskontrol og test.

9. Organisatoriske foranstaltninger

Beezy365 A/S har ansvaret for at fastlægge og vedligeholde relevante organisatoriske sikkerhedsprocedurer.

Dette omfatter blandt andet:

- Adgang til produktionsmiljøet.
- Håndtering af sikkerhedshændelser.
- Kontrol med underdatabehandlere.
- Ændringsstyring.
- Risikovurdering.
- Løbende dokumentation og opfølgning.

10. Dokumentation og kontrol

Sikkerhedsforanstaltningerne skal løbende vurderes i forhold til de identificerede risici og kravene i databehandleraftalen.

Dokumentationen opdateres, når kontroller er verificeret, eller der sker væsentlige ændringer i systemet.

Dokumentstatus: Foreløbig beskrivelse. Dokumentet indeholder både kendte arkitekturforhold og kontrolområder, hvor implementering og dokumentation endnu skal verificeres. Det udgør ikke en uafhængig sikkerhedserklæring.