Beveiligingsbeleid

<?xml encoding="utf-8" ?>

Beveiligingsbeleid van de Safety Software-applicatie (SaaS)

ID: SE-2026-V2
Update: 2026-03-05

1. Doel en reikwijdte

Dit Beveiligingsbeleid bepaalt de regels voor de bescherming van informatie en gegevens die worden verwerkt binnen de Safety Software-applicatie die wordt aangeboden volgens het Software as a Service (SaaS)-model.

Het document heeft betrekking op de beveiliging van gebruikers die de applicatie in de Safety Software-dienst gebruiken en vormt een aanvulling op de Algemene Voorwaarden en het Privacybeleid.

Het beleid heeft een informatief karakter en beschrijft de basis technische en organisatorische maatregelen die worden toegepast door Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polen (hierna: „Beheerder”).

2. Verantwoordelijkheidsmodel

Het systeem werkt volgens een model van gedeelde verantwoordelijkheid:

1. **Beheerder (Safety Software)** is verantwoordelijk voor de beveiliging van de applicatiecode, inlog-, autorisatie- en sessiemechanismen, gegevensbescherming op applicatielaag, het maken van back-ups en het reageren op beveiligingsincidenten.

2. **Leveranciers van infrastructuur en ondersteunende diensten** zijn verantwoordelijk voor de beveiliging van elementen die binnen de reikwijdte van de door hen geleverde diensten vallen.

3. **Klant** is verantwoordelijk voor de beveiliging van zijn apparaten, wachtwoorden, gebruikersidentiteiten en het beheren van toegangen binnen zijn team.

3. Regels voor applicatiebeveiliging

1. Gegevensoverdracht vindt uitsluitend plaats met gebruik van TLS-versleuteling.

2. Gebruikerssessies worden beveiligd met cookies met de attributen **HttpOnly**, **Secure** (voor versleutelde verbindingen) en **SameSite**. Na authenticatie vindt rotatie van de sessie-id plaats.

3. Voor sessies worden limieten voor inactiviteit en maximale duur toegepast.

4. Verzoeken die de toestand van het systeem wijzigen, worden beveiligd met CSRF-tokens die aan de serverzijde worden geverifieerd.

5. De applicatie hanteert een restrictief content security policy, inclusief mechanismen die het uitvoeren van niet-geautoriseerde scripts beperken en standaard browserbeveiligingsheaders.

6. Er worden mechanismen toegepast die misbruik beperken, waaronder rate limiting en bescherming tegen brute-force inlogpogingen.

7. Elke operatie wordt uitgevoerd in de context van de gebruiker en de organisatie; niet-geautoriseerde toegang wordt geblokkeerd.

4. Versleuteling en gegevensbescherming

1. Wachtwoorden van gebruikers worden opgeslagen met gebruik van het **bcrypt**-algoritme.

2. Geselecteerde gevoelige gegevens die in de database worden opgeslagen, worden beschermd met gebruik van een envelope-encryptiemodel. Cryptografische sleutels worden afzonderlijk beheerd in een extern sleutelbeheersysteem.

3. Waar dit gerechtvaardigd is, worden mechanismen toegepast die de blootstelling van gegevens beperken met behoud van zoek- of identificatiefuncties, zonder dat het noodzakelijk is volledige waarden in leesbare vorm op te slaan.

5. Back-up en herstel (BCP/DR)

1. Wij hanteren een gelaagde aanpak voor back-ups: lokale kopieën voor snel herstel en kopieën die buiten de primaire omgeving worden opgeslagen.

2. Kopieën die buiten de primaire omgeving worden opgeslagen omvatten incrementeel uitgevoerde omgevingsimages. Deze zijn versleuteld, worden regelmatig gevalideerd en vallen onder hersteltests.

3. De database wordt beveiligd met applicatieconsistentie-back-ups. Daarnaast worden lokale database-dumps onderhouden ter ondersteuning van snel herstel.

4. De integriteit van de back-ups wordt geverifieerd met controlemechanismen, waaronder checksums.

5. Het back-upproces is geautomatiseerd, wordt dagelijks uitgevoerd en valt onder monitoring van het slagen en falen van taken.

6. Er worden regelmatig tests voor gegevensherstel uitgevoerd, die ten minste het herstellen van geselecteerde bestanden omvatten.

6. Monitoring en alerts

1. Het systeem registreert geselecteerde beveiligingsgebeurtenissen en administratieve handelingen, met name die welke verband houden met authenticatie, toegangspogingen en het functioneren van kritieke processen.

2. Er worden monitoringsmechanismen en automatische alerts toegepast bij het falen van taken, kritieke fouten en gebeurtenissen die kunnen wijzen op misbruik of een beveiligingsincident.

3. Toegang tot logs en operationele informatie is beperkt tot bevoegde personen.

7. Infrastructuur en instandhouding van beveiliging

1. Administratieve toegang is beperkt tot bevoegde personen en beveiligd met sterke authenticatiemechanismen, waaronder authenticatie met sleutels.

2. Direct inloggen op een geprivilegieerde account is uitgeschakeld of beperkt overeenkomstig het principe van minimale privileges.

3. Er worden mechanismen toegepast voor verkeersfiltering, bescherming tegen brute-force toegangspogingen en monitoring van infrastructuurgebeurtenissen.

4. Beveiligingsupdates worden regelmatig doorgevoerd.

5. E-maildiensten die worden gebruikt voor de werking van het systeem zijn beveiligd met versleuteling van de transmissie en mechanismen die misbruik beperken.

8. Leveranciers en integraties

1. Voor zover het systeem gebruikmaakt van externe diensten of ondersteunende integraties, houdt de keuze van oplossingen rekening met gegevensbeveiliging, het minimalisatiebeginsel en controle over de reikwijdte van de doorgegeven informatie.

2. Communicatie met externe diensten vindt plaats met gebruik van versleutelde transmissie.

9. Incidentmelding

Meldingen met betrekking tot de beveiliging van de applicatie of vermoedens van incidenten dienen te worden gericht aan het adres:

office@safetysoftware.eu
Onderwerp van het bericht: SECURITY

Meldingen worden geanalyseerd overeenkomstig de interne incidentafhandelingsprocedure.

10. Naleving en rechtsmacht

1. Beveiligingsmaatregelen worden ontworpen en onderhouden met inachtneming van de toepasselijke wettelijke bepalingen, waaronder de vereisten van de **AVG**, en erkende praktijken voor informatiebeveiliging.

2. Het toepasselijke recht is het Poolse recht.

3. In geval van verschillen tussen taalversies is de Poolse versie beslissend.

11. Inwerkingtreding

Deze versie van het Veiligheidsbeleid geldt vanaf **2026-03-05**.

De actuele versie van het document wordt gepubliceerd in de Safety Software-service.

Verwerkingsverantwoordelijke en eigenaar van het systeem:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polen
E-mail: **office@safetysoftware.eu**

Wijzigingslog

Update: 2026-03-05

- gelaagde back-ups en het proces voor gegevensherstel (BCP/DR) verduidelijkt
- de beschrijving van gegevensversleuteling aangevuld met het envelopmodel en extern sleutelbeheer
- de beschrijving van applicatiebeveiliging uitgebreid met sessies, CSRF, CSP en anti-misbruikmechanismen
- een sectie monitoring en alerts toegevoegd en de sectie integratie met externe diensten vereenvoudigd