Politica de Securitate

Safety Software | Aktualizacja: 03.09.2026 | https://safetysoftware.eu

Politica de securitate a aplicației Safety Software (SaaS)

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

1. Scop și domeniu de aplicare

Prezenta Politică de securitate stabilește regulile de protecție a informațiilor și datelor prelucrate în cadrul aplicației Safety Software pusă la dispoziție în modelul Software as a Service (SaaS).

Documentul se referă la securitatea utilizatorilor care folosesc aplicația în serviciul Safety Software și constituie o completare a Regulamentului și a Politicii de confidențialitate.

Politica are caracter informativ și descrie măsurile tehnice și organizatorice de bază aplicate de Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polonia (denumit în continuare: „Administratorul”).

2. Modelul de responsabilitate

Sistemul funcționează într-un model de responsabilitate partajată:

1. **Administratorul (Safety Software)** este responsabil pentru securitatea codului aplicației, mecanismele de autentificare, autorizare și sesiune, protecția datelor la nivelul aplicației, efectuarea copiilor de rezervă și reacția la incidente de securitate.

2. **Furnizorii de infrastructură și servicii auxiliare** sunt responsabili pentru securitatea elementelor care se încadrează în sfera serviciilor prestate de aceștia.

3. **Clientul** este responsabil pentru securitatea dispozitivelor sale, a parolelor, a identităților utilizatorilor și pentru gestionarea accesului în cadrul echipei sale.

3. Principiile de securitate ale aplicației

1. Transmiterea datelor are loc exclusiv cu utilizarea criptării TLS.

2. Sesiunile utilizatorilor sunt securizate prin utilizarea cookie-urilor cu atributele **HttpOnly**, **Secure** (pentru conexiuni criptate) și **SameSite**. După autentificare are loc rotația identificatorului de sesiune.

3. Pentru sesiuni se aplică limite de inactivitate și ale duratei maxime.

4. Cererile care modifică starea sistemului sunt protejate cu token-uri CSRF verificate pe partea de server.

5. Aplicația utilizează o politică restrictivă de securitate a conținutului, inclusiv mecanisme care limitează executarea scripturilor neautorizate și antete standard de securitate ale browserului.

6. Sunt utilizate mecanisme care limitează abuzurile, inclusiv rate limiting și protecție împotriva încercărilor de autentificare prin forță brută.

7. Fiecare operațiune este executată în contextul utilizatorului și al organizației; accesul neautorizat este blocat.

4. Criptarea și protecția datelor

1. Parolele utilizatorilor sunt stocate utilizând algoritmul **bcrypt**.

2. Anumite date sensibile stocate în baza de date sunt protejate utilizând modelul de criptare în plic (envelope) a datelor. Cheile criptografice sunt administrate separat într-un sistem extern de management al cheilor.

3. Acolo unde este justificat, sunt utilizate mecanisme care limitează expunerea datelor, păstrând funcțiile de căutare sau identificare, fără a fi necesară stocarea valorilor complete în formă necriptată.

5. Backup și restaurare (BCP/DR)

1. Aplicăm o abordare stratificată a copiilor de rezervă: copii locale pentru restaurare rapidă și copii stocate în afara mediului principal.

2. Copiile stocate în afara mediului principal includ imagini ale mediului realizate incremental. Acestea sunt criptate, validate regulat și supuse testelor de restaurare.

3. Baza de date este protejată prin copii consistente la nivel de aplicație. În plus, sunt menținute dump-uri locale ale bazei de date care sprijină restaurarea rapidă.

4. Integritatea copiilor este verificată utilizând mecanisme de control, inclusiv sume de control.

5. Procesul de efectuare a copiilor este automatizat, se execută zilnic și este monitorizat în ceea ce privește reușita și eșecul sarcinilor.

6. Sunt efectuate periodic teste de restaurare a datelor, incluzând cel puțin restaurarea unor fișiere selectate.

6. Monitorizare și alerte

1. Sistemul înregistrează evenimente de securitate selectate și operațiuni administrative, în special cele legate de autentificare, încercări de acces și funcționarea proceselor critice.

2. Sunt utilizate mecanisme de monitorizare și alerte automate privind eșecul sarcinilor, erori critice și evenimente care pot indica un abuz sau un incident de securitate.

3. Accesul la loguri și la informațiile operaționale este limitat la persoanele autorizate.

7. Infrastructura și menținerea securității

1. Accesul administrativ este limitat la persoanele autorizate și protejat prin mecanisme de autentificare puternică, inclusiv autentificare cu chei.

2. Autentificarea directă pe contul privilegiat este dezactivată sau limitată conform principiului privilegiilor minime.

3. Sunt utilizate mecanisme de filtrare a traficului, protecție împotriva încercărilor de acces prin forță brută și monitorizare a evenimentelor de infrastructură.

4. Actualizările de securitate sunt implementate regulat.

5. Serviciile de e-mail utilizate pentru operarea sistemului sunt protejate prin criptarea transmisiei și mecanisme care limitează abuzurile.

8. Furnizori și integrări

1. În măsura în care sistemul utilizează servicii externe sau integrări auxiliare, selecția soluțiilor ia în considerare securitatea datelor, principiul minimizării și controlul domeniului informațiilor transmise.

2. Comunicarea cu serviciile externe are loc utilizând transmisie criptată.

9. Raportarea incidentelor

Raportările privind securitatea aplicației sau suspiciunile de incidente trebuie transmise la adresa:

office@safetysoftware.eu
Subiectul mesajului: SECURITY

Raportările sunt analizate conform procedurii interne de gestionare a incidentelor.

10. Conformitate și jurisdicție

1. Măsurile de securitate sunt proiectate și menținute având în vedere dispozițiile legale aplicabile, inclusiv cerințele **GDPR**, precum și practicile recunoscute de securitate a informațiilor.

2. Legea aplicabilă este legea poloneză.

3. În cazul unor discrepanțe între versiunile lingvistice, versiunea poloneză este cea determinantă.

11. Intrarea în vigoare

Această versiune a Politicii de Securitate este în vigoare din data de **2026-03-05**.

Versiunea curentă a documentului este publicată în serviciul Safety Software.

Administratorul datelor și proprietarul sistemului:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Cracovia, Polonia
E-mail: **office@safetysoftware.eu**

Istoricul modificărilor

Actualizare: 2026-03-05

- au fost precizate copiile de rezervă stratificate și procesul de restaurare a datelor (BCP/DR)
- a fost completată descrierea criptării datelor cu modelul „envelope” și gestionarea externă a cheilor
- a fost extinsă descrierea protecției la nivel de aplicație cu sesiuni, CSRF, CSP și mecanisme anti-abuz
- a fost adăugată secțiunea de monitorizare și alerte și a fost simplificată secțiunea de integrare cu servicii externe