Politika bezpečnosti

Safety Software | Aktualizacja: 17.12.2025 | https://safetysoftware.eu

Politika bezpečnosti aplikácie Safety Software (SaaS)

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

1. Účel a rozsah

Táto Politika bezpečnosti stanovuje zásady ochrany informácií a údajov spracúvaných v rámci aplikácie Safety Software poskytovanej v modeli Software as a Service (SaaS).

Dokument sa týka bezpečnosti používateľov využívajúcich aplikáciu v službe Safety Software a predstavuje doplnenie Podmienok používania a Zásad ochrany súkromia.

Politika má informačný charakter a opisuje základné technické a organizačné opatrenia uplatňované spoločnosťou Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Poľsko (ďalej len „Správca”).

2. Model zodpovednosti

Systém funguje v modeli zdieľanej zodpovednosti:

1. **Správca (Safety Software)** zodpovedá za bezpečnosť kódu aplikácie, mechanizmy prihlásenia, autorizácie a relácií, ochranu údajov v aplikačnej vrstve, vykonávanie záloh a reakciu na bezpečnostné incidenty.

2. **Poskytovatelia infraštruktúry a podporných služieb** zodpovedajú za bezpečnosť prvkov, ktoré spadajú do rozsahu nimi poskytovaných služieb.

3. **Zákazník** zodpovedá za bezpečnosť svojich zariadení, hesiel, identít používateľov a za riadenie prístupov vo svojom tíme.

3. Zásady bezpečnosti aplikácie

1. Prenos údajov prebieha výlučne s použitím šifrovania TLS.

2. Používateľské relácie sú zabezpečené pomocou cookies s atribútmi **HttpOnly**, **Secure** (pre šifrované spojenia) a **SameSite**. Po overení sa vykoná rotácia identifikátora relácie.

3. Pre relácie sa uplatňujú limity nečinnosti a maximálneho trvania.

4. Požiadavky meniace stav systému sú zabezpečené tokenmi CSRF overovanými na strane servera.

5. Aplikácia uplatňuje reštriktívnu politiku bezpečnosti obsahu, vrátane mechanizmov obmedzujúcich vykonávanie neautorizovaných skriptov a štandardných bezpečnostných hlavičiek prehliadača.

6. Uplatňujú sa mechanizmy obmedzujúce zneužitie, vrátane rate limiting a ochrany pred pokusmi o hrubou silou pri prihlasovaní.

7. Každá operácia sa vykonáva v kontexte používateľa a organizácie; neautorizovaný prístup je blokovaný.

4. Šifrovanie a ochrana údajov

1. Heslá používateľov sa ukladajú s použitím algoritmu **bcrypt**.

2. Vybrané citlivé údaje uložené v databáze sú chránené pomocou modelu obálkového šifrovania údajov. Kryptografické kľúče sú spravované oddelene v externom systéme správy kľúčov.

3. Tam, kde je to opodstatnené, sa používajú mechanizmy obmedzujúce expozíciu údajov pri zachovaní funkcií vyhľadávania alebo identifikácie, bez potreby uchovávania plných hodnôt v otvorenej forme.

5. Zálohovanie a obnova (BCP/DR)

1. Uplatňujeme vrstvený prístup k zálohovaniu: lokálne kópie na rýchlu obnovu a kópie uchovávané mimo primárneho prostredia.

2. Kópie uchovávané mimo primárneho prostredia zahŕňajú obrazy prostredia

vykonávané prírastkovo. Sú šifrované, pravidelne validované a podliehajú testom obnovy.

3. Databáza je zabezpečená aplikačne konzistentnými kópiami. Dodatočne sa udržiavajú lokálne databázové dumpy podporujúce rýchlu obnovu.

4. Integrita kópií sa overuje pomocou kontrolných mechanizmov, vrátane kontrolných súčtov.

5. Proces vytvárania kópií je automatizovaný, vykonáva sa denne a je monitorovaný z hľadiska úspešnosti aj neúspešnosti úloh.

6. Pravidelne sa vykonávajú testy obnovy údajov, zahŕňajúce minimálne obnovu vybraných súborov.

6. Monitorovanie a upozornenia

1. Systém zaznamenáva vybrané bezpečnostné udalosti a administratívne operácie, najmä súvisiace s overovaním, pokusmi o prístup a fungovaním kritických procesov.

2. Uplatňujú sa mechanizmy monitorovania a automatické upozornenia na zlyhanie úloh, kritické chyby a udalosti, ktoré môžu naznačovať zneužitie alebo bezpečnostný incident.

3. Prístup k logom a prevádzkovým informáciám je obmedzený na oprávnené osoby.

7. Infraštruktúra a udržiavanie bezpečnosti

1. Administrátorský prístup je obmedzený na oprávnené osoby a zabezpečený mechanizmami silného overovania, vrátane overovania pomocou kľúčov.

2. Priame prihlásenie na privilegovaný účet je vypnuté alebo obmedzené v súlade so zásadou minimálnych oprávnení.

3. Uplatňujú sa mechanizmy filtrovania prevádzky, ochrany pred pokusmi o prístup hrubou silou a monitorovania infraštruktúrnych udalostí.

4. Bezpečnostné aktualizácie sa zavádzajú pravidelne.

5. Poštové služby využívané na obsluhu systému sú zabezpečené šifrovaním prenosu a mechanizmami obmedzujúcimi zneužitie.

8. Dodávatelia a integrácie

1. V rozsahu, v akom systém využíva externé služby alebo podporné integrácie, výber riešení zohľadňuje bezpečnosť údajov, zásadu minimalizácie a kontrolu rozsahu odovzdávaných informácií.

2. Komunikácia s externými službami prebieha s použitím šifrovanej transmisie.

9. Nahlasovanie incidentov

Oznámenia týkajúce sa bezpečnosti aplikácie alebo podozrenia na incidenty smerujte na adresu:

office@safetysoftware.eu
Predmet správy: SECURITY

Oznámenia sa analyzujú v súlade s interným postupom riešenia incidentov.

10. Súlad a jurisdikcia

1. Bezpečnostné opatrenia sú navrhované a udržiavané s ohľadom na platné právne predpisy, vrátane požiadaviek **GDPR**, a uznávaných postupov bezpečnosti informácií.

2. Rozhodným právom je poľské právo.

3. V prípade rozporov medzi jazykovými verziami je rozhodujúca poľská verzia.

11. Nadobudnutie účinnosti

Táto verzia Bezpečnostnej politiky je účinná od **2026-03-05**.

Aktuálna verzia dokumentu je zverejnená v službe Safety Software.

Správca údajov a vlastník systému:

Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Poľsko
E-mail: **office@safetysoftware.eu**

Zoznam zmien

Aktualizácia: 2026-03-05

- spresnili sa vrstvené zálohy a proces obnovy dát (BCP/DR)
- doplnil sa opis šifrovania dát o obálkový model a externú správu kľúčov
- rozšíril sa opis aplikačnej ochrany o relácie, CSRF, CSP a mechanizmy proti zneužitiu
- pridala sa sekcia monitorovania a alertov a zjednodušila sa sekcia integrácie s externými službami