Bezpečnostní politika

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

Bezpečnostní politika aplikace Safety Software (SaaS)

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

1. Účel a rozsah

Tato Bezpečnostní politika stanovuje zásady ochrany informací a dat zpracovávaných v rámci aplikace Safety Software poskytované v modelu Software as a Service (SaaS).

Dokument se týká bezpečnosti uživatelů využívajících aplikaci v rámci služby Safety Software a představuje doplnění Obchodních podmínek a Zásad ochrany osobních údajů.

Politika má informativní charakter a popisuje základní technická a organizační opatření uplatňovaná společností Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polsko (dále jen: „Správce“).

2. Model odpovědnosti

Systém funguje v modelu sdílené odpovědnosti:

1. **Správce (Safety Software)** odpovídá za bezpečnost kódu aplikace, mechanismy přihlašování, autorizace a relací, ochranu dat v aplikační vrstvě, provádění záloh a reakci na bezpečnostní incidenty.

2. **Poskytovatelé infrastruktury a podpůrných služeb** odpovídají za bezpečnost prvků spadajících do rozsahu jimi poskytovaných služeb.

3. **Zákazník** odpovídá za bezpečnost svých zařízení, hesel, identit uživatelů a za správu přístupů ve svém týmu.

3. Zásady bezpečnosti aplikace

1. Přenos dat probíhá výhradně s použitím šifrování TLS.

2. Uživatelské relace jsou zabezpečeny pomocí cookies s atributy **HttpOnly**, **Secure** (pro šifrovaná připojení) a **SameSite**. Po ověření dochází k rotaci identifikátoru relace.

3. Pro relace jsou uplatňovány limity nečinnosti a maximální doby trvání.

4. Požadavky měnící stav systému jsou zabezpečeny tokeny CSRF ověřovanými na straně serveru.

5. Aplikace uplatňuje restriktivní politiku zabezpečení obsahu, včetně mechanismů omezujících spouštění neautorizovaných skriptů a standardních bezpečnostních hlaviček prohlížeče.

6. Jsou uplatňovány mechanismy omezující zneužití, včetně rate limiting a ochrany proti pokusům o přihlášení hrubou silou.

7. Každá operace je prováděna v kontextu uživatele a organizace; neautorizovaný přístup je blokován.

4. Šifrování a ochrana dat

1. Hesla uživatelů jsou ukládána s použitím algoritmu **bcrypt**.

2. Vybraná citlivá data ukládaná v databázi jsou chráněna s použitím modelu obálkového šifrování dat. Kryptografické klíče jsou spravovány odděleně v externím systému správy klíčů.

3. Tam, kde je to odůvodněné, jsou uplatňovány mechanismy omezující expozici dat při zachování funkcí vyhledávání nebo identifikace, bez nutnosti ukládání plných hodnot v otevřené podobě.

5. Zálohování a obnova (BCP/DR)

1. Uplatňujeme vrstvený přístup k zálohám: lokální kopie pro rychlou obnovu a kopie uchovávané mimo primární prostředí.

2. Kopie uchovávané mimo primární prostředí zahrnují obrazy prostředí vytvářené

přírůstkově. Jsou šifrovány, pravidelně validovány a podléhají testům obnovy.

3. Databáze je zabezpečována aplikačně konzistentními kopiemi. Dále jsou udržovány lokální výpisy databáze podporující rychlou obnovu.

4. Integrita kopií je ověřována pomocí kontrolních mechanismů, včetně kontrolních součtů.

5. Proces vytváření kopií je automatizovaný, prováděný denně a podléhá monitoringu úspěšnosti i neúspěšnosti úloh.

6. Pravidelně jsou prováděny testy obnovy dat, zahrnující alespoň obnovu vybraných souborů.

6. Monitoring a upozornění

1. Systém zaznamenává vybrané bezpečnostní události a administrativní operace, zejména související s ověřováním, pokusy o přístup a činností kritických procesů.

2. Jsou uplatňovány mechanismy monitoringu a automatická upozornění na neúspěch úloh, kritické chyby a události, které mohou naznačovat zneužití nebo bezpečnostní incident.

3. Přístup k logům a provozním informacím je omezen na oprávněné osoby.

7. Infrastruktura a udržování bezpečnosti

1. Administrátorský přístup je omezen na oprávněné osoby a zabezpečen mechanismy silného ověřování, včetně ověřování pomocí klíčů.

2. Přímé přihlášení k privilegovanému účtu je vypnuto nebo omezeno v souladu se zásadou minimálních oprávnění.

3. Jsou uplatňovány mechanismy filtrování provozu, ochrany proti pokusům o přístup hrubou silou a monitorování infrastrukturních událostí.

4. Bezpečnostní aktualizace jsou nasazovány pravidelně.

5. Poštovní služby používané pro obsluhu systému jsou zabezpečeny šifrováním přenosu a mechanismy omezujícími zneužití.

8. Dodavatelé a integrace

1. V rozsahu, v jakém systém využívá externí služby nebo podpůrné integrace, výběr řešení zohledňuje bezpečnost dat, zásadu minimalizace a kontrolu rozsahu předávaných informací.

2. Komunikace s externími službami probíhá s použitím šifrovaného přenosu.

9. Hlášení incidentů

Hlášení týkající se bezpečnosti aplikace nebo podezření na incidenty je třeba směřovat na adresu:

office@safetysoftware.eu
Předmět zprávy: SECURITY

Hlášení jsou analyzována v souladu s interním postupem pro řešení incidentů.

10. Soulad a jurisdikce

1. Bezpečnostní opatření jsou navrhována a udržována s ohledem na platné právní předpisy, včetně požadavků **GDPR**, a uznávaných postupů v oblasti bezpečnosti informací.

2. Rozhodným právem je polské právo.

3. V případě rozporu mezi jazykovými verzemi je rozhodující polská verze.

11. Vstup v platnost

Tato verze Zásad bezpečnosti platí od **2026-03-05**.

Aktuální verze dokumentu je publikována v rámci služby Safety Software.

Správce údajů a vlastník systému:
Safety Software Sp. z o.o.
ul. Półłanki 80

30-740 Krakov, Polsko
E-mail: **office@safetysoftware.eu**

Seznam změn

Aktualizace: 2026-03-05

- upřesněny vrstvené záložní kopie a proces obnovy dat (BCP/DR)
- doplněn popis šifrování dat o obálkový model a externí správu klíčů
- rozšířen popis ochrany na úrovni aplikace o relace, CSRF, CSP a mechanismy proti zneužití
- přidána sekce monitorování a upozornění a zjednodušena sekce integrace s externími službami