Polityka Bezpieczeństwa

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

Polityka Bezpieczeństwa Aplikacji Safety Software (SaaS)

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

1. Cel i zakres

Niniejsza Polityka Bezpieczeństwa określa zasady ochrony informacji i danych przetwarzanych w ramach aplikacji Safety Software udostępnianej w modelu Software as a Service (SaaS).

Dokument dotyczy bezpieczeństwa użytkowników korzystających z aplikacji w serwisie Safety Software i stanowi uzupełnienie Regulaminu oraz Polityki Prywatności.

Polityka ma charakter informacyjny i opisuje podstawowe środki techniczne i organizacyjne stosowane przez Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polska (dalej: „Administrator”).

2. Model odpowiedzialności

System działa w modelu współdzielonej odpowiedzialności:

1. **Administrator (Safety Software)** odpowiada za bezpieczeństwo kodu aplikacji, mechanizmy logowania, autoryzacji i sesji, ochronę danych w warstwie aplikacyjnej, wykonywanie kopii zapasowych oraz reagowanie na incydenty bezpieczeństwa.

2. **Dostawcy infrastruktury i usług pomocniczych** odpowiadają za bezpieczeństwo elementów pozostających w zakresie świadczonych przez nich usług.

3. **Klient** odpowiada za bezpieczeństwo swoich urządzeń, haseł, tożsamości użytkowników oraz zarządzanie dostępami w swoim zespole.

3. Zasady bezpieczeństwa aplikacji

1. Transmisja danych odbywa się wyłącznie z użyciem szyfrowania TLS.

2. Sesje użytkowników zabezpieczone są przy użyciu ciasteczek z atrybutami **HttpOnly**, **Secure** (dla połączeń szyfrowanych) oraz **SameSite**. Po uwierzytelnieniu następuje rotacja identyfikatora sesji.

3. Dla sesji stosowane są limity bezczynności oraz maksymalnego czasu trwania.

4. Żądania zmieniające stan systemu zabezpieczone są tokenami CSRF weryfikowanymi po stronie serwera.

5. Aplikacja stosuje restrykcyjną politykę bezpieczeństwa treści, w tym mechanizmy ograniczające wykonywanie nieautoryzowanych skryptów oraz standardowe nagłówki bezpieczeństwa przeglądarki.

6. Stosowane są mechanizmy ograniczające nadużycia, w tym rate limiting oraz ochrona przed próbami siłowego logowania.

7. Każda operacja wykonywana jest w kontekście użytkownika i organizacji; nieautoryzowany dostęp jest blokowany.

4. Szyfrowanie i ochrona danych

1. Hasła użytkowników przechowywane są z użyciem algorytmu **bcrypt**.

2. Wybrane dane wrażliwe przechowywane w bazie są chronione z użyciem modelu kopertowego szyfrowania danych. Klucze kryptograficzne są zarządzane oddzielnie w zewnętrznym systemie zarządzania kluczami.

3. Tam, gdzie jest to uzasadnione, stosowane są mechanizmy ograniczające ekspozycję danych przy zachowaniu funkcji wyszukiwania lub identyfikacji, bez konieczności przechowywania pełnych wartości w postaci jawnej.

5. Backup i odtwarzanie (BCP/DR)

1. Stosujemy warstwowe podejście do kopii zapasowych: lokalne kopie dla szybkiego odtworzenia oraz kopie przechowywane poza podstawowym środowiskiem.

2. Kopie przechowywane poza podstawowym środowiskiem obejmują obrazy środowiska wykonywane przyrostowo. Są one szyfrowane, regularnie walidowane i objęte testami odtwarzania.

3. Baza danych jest zabezpieczana kopiami spójnymi aplikacyjnie. Dodatkowo utrzymywane są lokalne zrzuty bazy wspierające szybkie odtworzenie.

4. Integralność kopii jest weryfikowana przy użyciu mechanizmów kontrolnych, w tym sum kontrolnych.

5. Proces wykonywania kopii jest zautomatyzowany, wykonywany codziennie i objęty monitoringiem powodzenia oraz niepowodzenia zadań.

6. Regularnie przeprowadzane są testy odtwarzania danych, obejmujące co najmniej odtworzenie wybranych plików.

6. Monitorowanie i alerty

1. System rejestruje wybrane zdarzenia bezpieczeństwa oraz operacje administracyjne, w szczególności związane z uwierzytelnianiem, próbami dostępu i działaniem procesów krytycznych.

2. Stosowane są mechanizmy monitorowania oraz automatyczne alerty o niepowodzeniu zadań, błędach krytycznych i zdarzeniach mogących wskazywać na nadużycie lub incydent bezpieczeństwa.

3. Dostęp do logów i informacji operacyjnych jest ograniczony do osób upoważnionych.

7. Infrastruktura i utrzymanie bezpieczeństwa

1. Dostęp administracyjny jest ograniczony do upoważnionych osób i zabezpieczony

mechanizmami silnego uwierzytelniania, w tym uwierzytelnianiem kluczami.

2. Bezpośrednie logowanie na konto uprzywilejowane jest wyłączone lub ograniczone zgodnie z zasadą minimalnych uprawnień.

3. Stosowane są mechanizmy filtrowania ruchu, ochrony przed próbami siłowego dostępu oraz monitorowania zdarzeń infrastrukturalnych.

4. Aktualizacje bezpieczeństwa są wdrażane regularnie.

5. Usługi pocztowe wykorzystywane do obsługi systemu są zabezpieczone szyfrowaniem transmisji oraz mechanizmami ograniczającymi nadużycia.

8. Dostawcy i integracje

1. W zakresie, w jakim system korzysta z usług zewnętrznych lub integracji pomocniczych, dobór rozwiązań uwzględnia bezpieczeństwo danych, zasadę minimalizacji oraz kontrolę zakresu przekazywanych informacji.

2. Komunikacja z usługami zewnętrznymi odbywa się z użyciem szyfrowanej transmisji.

9. Zgłaszanie incydentów

Zgłoszenia dotyczące bezpieczeństwa aplikacji lub podejrzenia incydentów należy kierować na adres:

office@safetysoftware.eu
Temat wiadomości: SECURITY

Zgłoszenia są analizowane zgodnie z wewnętrzną procedurą obsługi incydentów.

10. Zgodność i jurysdykcja

1. Środki bezpieczeństwa są projektowane i utrzymywane z uwzględnieniem obowiązujących przepisów prawa, w tym wymagań **RODO**, oraz uznanych praktyk bezpieczeństwa informacji.

2. Prawem właściwym jest prawo polskie.

3. W przypadku rozbieżności między wersjami językowymi rozstrzygająca jest wersja polska.

11. Wejście w życie

Niniejsza wersja Polityki Bezpieczeństwa obowiązuje od dnia **2026-03-05**.

Aktualna wersja dokumentu jest publikowana w serwisie Safety Software.

Administrator danych i właściciel systemu:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polska
E-mail: **office@safetysoftware.eu**

Changelog

Aktualizacja: 2026-03-05

- doprecyzowano warstwowe kopie zapasowe oraz proces odtwarzania danych (BCP/DR)
- uzupełniono opis szyfrowania danych o model kopertowy i zewnętrzne zarządzanie kluczami
- rozszerzono opis ochrony aplikacyjnej o sesje, CSRF, CSP i mechanizmy anty-nadużyciowe
- dodano sekcję monitorowania i alertów oraz uproszczono sekcję integracji z usługami zewnętrznymi