Polityka Bezpieczeństwa Portalu ZIELINET

Data Wejścia w Życie: 5 listopada 2025

Wersja: 1.1

1. Wprowadzenie i Cel Polityki

Bezpieczeństwo danych naszych Klientów, Użytkowników i Partnerów jest absolutnym priorytetem dla ZIELINET. Jako integrator ekosystemów wzrostu, rozumiemy, że zaufanie jest fundamentem naszej działalności.

Niniejsza Polityka Bezpieczeństwa opisuje kluczowe środki techniczne, organizacyjne i proceduralne, które wdrożyliśmy w celu ochrony integralności, poufności i dostępności danych przetwarzanych w ramach portalu ZIELINET (obejmującego domeny zielinet.pl, zielinet.eu, zielinet.com oraz domeny administracyjne).

2. Administrator Danych

Administratorem Danych Osobowych przetwarzanych w portalu jest **ZIELINET Wojciech Zieliński** z siedzibą przy Aleja Jana Pawła II 27, 00-867 Warszawa. Wszelkie zapytania dotyczące bezpieczeństwa danych prosimy kierować na adres e-mail: **security@zielinet.com**.

3. Filary Bezpieczeństwa Portalu ZIELINET

Nasze podejście do bezpieczeństwa opiera się na wielowarstwowej strategii (defense-in-depth), obejmującej pięć kluczowych filarów:

3.1. Bezpieczeństwo Danych i Transmisji

- **Szyfrowanie Transmisji:** Cała komunikacja pomiędzy przeglądarką Użytkownika a naszymi serwerami jest szyfrowana przy użyciu silnego protokołu **SSL/TLS**. Dotyczy to zarówno części publicznej portalu, jak i Strefy Klienta oraz Panelu Administracyjnego.
- **Zarządzanie Sekretami:** Wszystkie kluczowe dane dostępowe, klucze API (w tym do integracji z Email Labs, SMSAPI, Google Analytics) oraz poświadczenia bazy danych są zarządzane jako **zmienne środowiskowe (plik .env)**. Są one w pełni odizolowane od bazy kodu źródłowego, co minimalizuje ryzyko ich wycieku.
- **Integralność Danych:** Treści portalu oraz tłumaczenia interfejsu są przechowywane i zarządzane centralnie w bazie danych.

3.2. Bezpieczeństwo Aplikacji (Web Security)

Wdrożyliśmy dedykowane mechanizmy ochrony przed najczęstszymi wektorami ataków na aplikacje webowe:

- **Ochrona przed Stored XSS:** Wszystkie treści wprowadzane przez administratorów i redaktorów, które mają być wyświetlane jako HTML, są poddawane rygorystycznej sanityzacji przy użyciu biblioteki **HTMLPurifier**. Zapobiega to osadzaniu złośliwego kodu (Stored Cross-Site Scripting) w treści portalu.
- **Ochrona przed CSRF:** Wszystkie operacje w Panelu Administracyjnym (np. zmiana ról, edycja treści) są chronione przez dedykowany **serwis tokenów anty-CSRF** (Cross-Site Request Forgery). Każdy formularz musi przesłać unikalny, ważny token, aby akcja została wykonana.
- **Polityka Bezpieczeństwa Treści (CSP):** Wdrożyliśmy nagłówki Content-Security-Policy, aby dodatkowo ograniczyć możliwość wykonywania nieautoryzowanych skryptów.
- **Bezpieczne Zarządzanie Sesją:** Mechanizmy sesji Użytkowników i Administratorów zostały zrefaktoryzowane w celu wyeliminowania konfliktów i zapewnienia bezpiecznego cyklu życia sesji.

3.3. Kontrola Dostępu i Zarządzanie Uprawnieniami

Dostęp do danych jest ściśle reglamentowany zgodnie z zasadą minimalnych uprawnień (least privilege).

- **Role Użytkowników:** System opiera się na predefiniowanych rolach (np. Superadministrator, Administrator, Redaktor, Klient).
- **Granularne Uprawnienia:** Zamiast polegać wyłącznie na rolach, wdrożyliśmy system **granularnych uprawnień** (np. manage_roles, edit_legal_docs, manage_all_users). Pozwala to na precyzyjne nadawanie i odbieranie dostępu do poszczególnych funkcji.
- **Segregacja Obowiązków (SoD):** Zgodnie z najlepszymi praktykami, rola "Administrator" ma ograniczone możliwości: nie może zarządzać innymi Administratorami ani Superadministratorem, ani zmieniać własnych uprawnień. Pełnię uprawnień posiada wyłącznie rola "Superadministrator".
- **Nadpisywanie Uprawnień:** System umożliwia ręczne nadpisywanie (dodawanie lub odbieranie) konkretnych uprawnień dla poszczególnych użytkowników, niezależnie od ich roli.

3.4. Bezpieczeństwo Infrastruktury i Środowiska

- **Hosting:** Korzystamy z usług renomowanego dostawcy hostingu (OVH), który zapewnia bezpieczeństwo fizyczne i sieciowe infrastruktury serwerowej.

- **Separacja Domen (Isolation):** Zaimplementowaliśmy kluczową separację środowisk. Portal publiczny (zielinet.pl) oraz Panel Administracyjny (admin.zielinet.pl) działają na **oddzielnych subdomenach** i posiadają **oddzielne katalogi główne (DocumentRoot)**. Takie rozwiązanie znacząco utrudnia próby eskalacji uprawnień lub ataki typu *path traversal* z części publicznej do administracyjnej.
- **Monitoring i Logowanie:** Aplikacja wykorzystuje system logowania zgodny z PSR-3 (Monolog) do rejestrowania kluczowych zdarzeń systemowych i błędów, co wspiera szybką diagnostykę i reagowanie na incydenty.

3.5. Bezpieczeństwo Procesu Rozwoju Oprogramowania (DevSecOps)

Bezpieczeństwo jest integralną częścią naszego cyklu rozwoju oprogramowania (SDLC).

- **Prywatne Repozytorium Kodu:** Cały kod źródłowy portalu jest przechowywany w **prywatnym repozytorium Git**.
- **Wymuszony Code Review:** Wszelkie zmiany w kodzie muszą być wprowadzane poprzez **Pull Requesty** i poddane **weryfikacji (code review)** przez innego członka zespołu przed scaleniem z główną gałęzią produkcyjną (main).
- **Testowanie Automatyczne:** Utrzymujemy stabilny pakiet testów automatycznych (PHPUnit), który jest uruchamiany w celu weryfikacji nowych funkcji i zapobiegania błędom regresji.

4. Program Ujawniania Podatności (Vulnerability Disclosure)

Jesteśmy otwarci na współpracę ze społecznością badaczy bezpieczeństwa. Jeśli odkryłeś potencjalną lukę w bezpieczeństwie naszego portalu, zachęcamy do jej odpowiedzialnego ujawnienia (Responsible Disclosure).

Prosimy o kontakt pod adresem e-mail: **security@zielinet.com**, abyśmy mogli jak najszybciej zweryfikować zgłoszenie i podjąć odpowiednie kroki. W ramach podziękowania za pomoc w utrzymaniu bezpieczeństwa naszych Użytkowników, prowadzimy publiczną listę podziękowań na stronie "Podziękowania dla Badaczy Bezpieczeństwa".

5. Postanowienia Końcowe

Niniejsza Polityka Bezpieczeństwa jest dokumentem żywym i podlega regularnym przeglądom oraz aktualizacjom w miarę rozwoju technologicznego portalu i ewolucji otoczenia. Wszystkie zmiany będą publikowane na tej stronie i wersjonowane, zgodnie z naszym ogólnym systemem zarządzania dokumentami prawnymi.