**ZIELINET Portal Security Policy**

Effective Date: November 5, 2025

Version: 1.1

**1. Introduction and Policy Objective**

The security of our Clients', Users', and Partners' data is an absolute priority for ZIELINET. As an integrator of growth ecosystems, we understand that trust is the foundation of our business.

This Security Policy describes the key technical, organizational, and procedural measures we have implemented to protect the integrity, confidentiality, and availability of data processed within the ZIELINET portal (covering the zielinet.pl, zielinet.eu, zielinet.com domains, and administrative domains).

**2. Data Administrator**

The Administrator of Personal Data processed in the portal is **ZIELINET Wojciech Zieliński**, headquartered at Aleja Jana Pawła II 27, 00-867 Warszawa. All inquiries regarding data security should be directed to the email address: **security@zielinet.com**.

**3. Pillars of ZIELINET Portal Security**

Our approach to security is based on a multi-layered (defense-in-depth) strategy, encompassing five key pillars:

**3.1. Data and Transmission Security**

- **Transmission Encryption:** All communication between the User's browser and our servers is encrypted using a strong **SSL/TLS** protocol. This applies to the public part of the portal, the Client Zone, and the Administrative Panel.
- **Secret Management:** All critical access credentials, API keys (including for integrations with Email Labs, SMSAPI, Google Analytics), and database credentials are managed as **environment variables (.env file)**. They are fully isolated from the source code base, minimizing the risk of leakage.
- **Data Integrity:** Portal content and interface translations are stored and managed centrally in the database.

**3.2. Application Security (Web Security)**

We have implemented dedicated mechanisms to protect against the most common web application attack vectors:

- **Protection against Stored XSS:** All content entered by administrators and editors, intended to be displayed as HTML, undergoes rigorous sanitization using the **HTMLPurifier** library. This prevents the embedding of malicious code (Stored Cross-Site Scripting) within the portal's content.
- **CSRF Protection:** All operations in the Administrative Panel (e.g., changing roles, editing content) are protected by a dedicated **anti-CSRF token service** (Cross-Site Request Forgery). Every form must submit a unique, valid token for the action to be executed.
- **Content Security Policy (CSP):** We have implemented Content-Security-Policy headers to further restrict the execution of unauthorized scripts.
- **Secure Session Management:** The session mechanisms for Users and Administrators have been refactored to eliminate conflicts and ensure a secure session lifecycle.

### 3.3. Access Control and Permissions Management

Access to data is strictly regulated according to the principle of least privilege.

- **User Roles:** The system is based on predefined roles (e.g., Superadministrator, Administrator, Editor, Client).
- **Granular Permissions:** Instead of relying solely on roles, we have implemented a system of **granular permissions** (e.g., manage_roles, edit_legal_docs, manage_all_users). This allows for precise granting and revoking of access to specific functions.
- **Segregation of Duties (SoD):** In line with best practices, the "Administrator" role has limited capabilities: it cannot manage other Administrators or the Superadministrator, nor can it change its own permissions. Only the "Superadministrator" role has full privileges.
- **Permission Overrides:** The system allows for the manual overriding (adding or revoking) of specific permissions for individual users, regardless of their assigned role.

### 3.4. Infrastructure and Environment Security

- **Hosting:** We use the services of a reputable hosting provider (OVH), which ensures the physical and network security of the server infrastructure.
- **Domain Separation (Isolation):** We have implemented crucial environment separation. The public portal (zielinet.pl) and the Administrative Panel (admin.zielinet.pl) operate on **separate subdomains** and have **separate home directories (DocumentRoot)**. This solution significantly hinders attempts at

privilege escalation or *path traversal* attacks from the public section to the administrative section.

- **Monitoring and Logging:** The application uses a PSR-3 compliant logging system (Monolog) to record key system events and errors, supporting rapid diagnostics and incident response.

**3.5. Secure Software Development Lifecycle (DevSecOps)**

Security is an integral part of our software development lifecycle (SDLC).

- **Private Code Repository:** All of the portal's source code is stored in a **private Git repository**.
- **Enforced Code Review:** All code changes must be introduced via **Pull Requests** and undergo **verification (code review)** by another team member before being merged into the main production branch (main).
- **Automated Testing:** We maintain a stable suite of automated tests (PHPUnit) that is run to verify new features and prevent regression errors.

**4. Vulnerability Disclosure Program**

We are open to collaboration with the security researcher community. If you have discovered a potential security vulnerability in our portal, we encourage you to disclose it responsibly (Responsible Disclosure).

Please contact us at the email address: **security@zielinet.com**, so we can verify the report as quickly as possible and take appropriate action. As a token of our appreciation for helping to maintain the security of our Users, we maintain a public acknowledgment list on the "Security Researcher Acknowledgements" page.

**5. Final Provisions**

This Security Policy is a living document and is subject to regular reviews and updates in line with the portal's technological development and the evolving threat landscape. All changes will be published on this page and versioned, in accordance with our general legal document management system.