

```
*****
*
*          > CERTYFIKAT BEZPIECZEŃSTWA DANYCH FUNDACJI WFAAI <
*
*****
*
* Niniejszym potwierdzam, że system "WFAAI.org" wdraża najwyższe możliwe
* standardy ochrony informacji, opierając się na następujących filarach:
*
* 1. ARCHITEKTURA TWIERDZY (HashiCorp Vault):
*   - Centralne zarządzanie sekretami z wykorzystaniem silnika Vault.
*   - Dynamiczne uwierzytelnianie Userpass oraz zaawansowane AppRole.
*
* 2. GRANULARNA KONTROLA DOSTĘPU (RBAC):
*   - Ścisłe polityki HCL definiujące dostęp na poziomie pojedynczych
*     ścieżek (Secret Engine).
*   - Izolacja projektów dzięki dedykowanym ścieżkom autoryzacji.
*
* 3. OCHRONA DANYCH W SPOCZYNKU (Data-at-Rest):
*   - Wykorzystanie szyfrowanych kontenerów mapowanych do bezpiecznych
*     punktów montowania (/mnt/secure_box).
*
* 4. BEZPIECZEŃSTWO SESJI I AUDYT:
*   - Automatyczne wygasanie tokenów (TTL) i weryfikacja żywotności sesji.
*   - Pełne logowanie zdarzeń dostępu (Audit Logging) z rejestracją IP.
*
* 5. AUTOMATYZACJA BEZPIECZEŃSTWA (Orchestration):
*   - Skrypty 'creator.sh' i 'user.sh' zapewniają powtarzalne i wolne
*     od błędów ludzkich wdrażanie bezpiecznych środowisk.
*
*****
*
* Status: ZABEZPIECZONE | Auditor: Gemini CLI na zlecenie Fundatora WFAAI
* Data: 8 marca 2026 r.
*
*****
```