Dokumenty

Polityka bezpieczeństwa

Jak chronimy dane, co robimy przy incydencie i jak zgłosić podatność.

Dokument nie ma jeszcze uzupełnionych danych rejestrowych operatora. Do czasu ich uzupełnienia traktuj go jako projekt, nie jako wiążącą umowę.

Kto świadczy usługę

Podmiot | DO UZUPEŁNIENIA
Adres | DO UZUPEŁNIENIA
NIP | DO UZUPEŁNIENIA
REGON | DO UZUPEŁNIENIA
Rejestr | DO UZUPEŁNIENIA
Serwis | elogowanie.pl
Kontakt | kontakt@elogowanie.pl

Wersja dokumentu z dnia 2026-09-08.

Szyfrowanie

- Cały ruch po HTTPS z HSTS. Certyfikaty odnawiane automatycznie.
- Hasła jako skrót argon2id (19 MiB pamięci, 2 iteracje). Nie da się ich odwrócić i nie znamy Twojego hasła.
- Tokeny sesji, kody jednorazowe i tokeny weryfikacji trzymamy jako SHA-256. Wyciek bazy nie pozwala przejąć trwającej sesji.
- Sekrety TOTP, sekrety klientów OAuth i numery telefonu szyfrujemy AES-256-GCM kluczem z konfiguracji, poza bazą.
- Poczta wychodząca przez STARTTLS z weryfikacją certyfikatu odbiorcy.

Kontrola dostępu

- Logowanie ma dwa składniki. Samo hasło nigdy nie wydaje sesji, także w oknie zgody OAuth.
- Passkeys (WebAuthn) jako alternatywa dla hasła. Klucz prywatny nie opuszcza urządzenia użytkownika.
- Sesje mają limit bezczynności i limit bezwzględny. Zmiana hasła unieważnia pozostałe urządzenia i sesje w oknie OAuth.
- Każde zapytanie API jest ograniczone do jednej firmy. Zasób innej firmy zwraca 404, nie 403, żeby nie potwierdzać istnienia cudzych danych.
- Proces aplikacji działa jako zwykły użytkownik, nie root. Baza słucha wyłącznie na pętli zwrotnej.
- Rola serwera pocztowego widzi tylko widok aliasów. Nie ma dostępu do kont ani do haseł.

Ograniczanie nadużyć

- Limity trwałe w bazie, liczone atomowo, po adresie IP, koncie, organizacji, numerze telefonu i kluczu API.
- Rosnąca blokada po kolejnych nieudanych próbach, przechowywana niezależnie od okna czasowego.
- Turnstile przy rejestracji, logowaniu i resecie hasła. Token sprawdzamy po stronie serwera, razem z akcją i domeną.
- Wysyłka SMS ograniczona do wybranych kierunków, z limitem segmentów i szablonem

bez adresów stron.

- Adresy webhooków rozwiązujemy przed połączeniem i odrzucamy te wskazujące do sieci prywatnych. Nie podążamy za przekierowaniami.

Przechowywanie i kasowanie

- Zdjęcie dokumentu kasujemy zaraz po analizie, także przy nieudanej próbie. Znacznik zapisujemy dopiero po potwierdzeniu, że pliku nie ma.
- Wynik weryfikacji zerujemy po 30 dniach.
- Log dostarczeń webhooków kasujemy po 30 dniach.
- Pliki bez wiersza w bazie sprząta zamiatarka po godzinie.
- Log audytowy nie zawiera treści, haseł, kluczy ani danych osobowych.

Kopie zapasowe

- Kopia bazy codziennie i przed każdą migracją schematu.
- Kopie trzymamy 30 dni.
- Materiał weryfikacyjny nie trafia do kopii, bo w chwili wykonania kopii już go nie ma.
- Odtworzenie ćwiczymy przy każdej większej zmianie schematu.

Procedura incydentu

- Zgłoszenie trafia na security@elogowanie.pl i jest potwierdzane w ciągu 24 godzin.
- Odcinamy dostęp albo wyłączamy funkcję, jeżeli to ogranicza szkodę.
- Ustalamy zakres: co, kiedy i czyich danych dotyczy.
- Naruszenie ochrony danych zgłaszamy Prezesowi UODO w ciągu 72 godzin od stwierdzenia.
- Osoby, których dotyczy wysokie ryzyko, informujemy bez zbędnej zwłoki, prostym językiem i z konkretną radą.
- Po zamknięciu sprawy publikujemy podsumowanie w historii zmian .

Zgłaszanie podatności

Pisz na security@elogowanie.pl . Nie mamy programu bug bounty i nie płacimy za zgłoszenia, ale odpowiadamy na każde i podajemy, co z nim zrobiliśmy.

- Testuj wyłącznie na własnym koncie i własnych danych.
- Nie prowadź testów obciążeniowych bez wcześniejszego uzgodnienia.
- Nie ujawniaj podatności publicznie, zanim jej nie naprawimy albo nie miną 90 dni.
- Zgłoszenie zgodne z tymi zasadami nie jest naruszeniem regulaminu i nie skończy się zawiadomieniem.

Czego jeszcze nie ma

Piszemy o tym wprost, bo brak takiej sekcji zwykle znaczy, że ktoś ją przemilczał.

- Nie mamy certyfikacji ISO 27001 ani SOC 2.
- Nie mamy niezależnego audytu bezpieczeństwa przeprowadzonego przez firmę zewnętrzną.
- Nie mamy jeszcze wykrywania prezentacji przy weryfikacji dokumentu (zdjęcie ekranu, wydruk, maska).
- Nie mamy zapasowego ośrodka. Awaria całego serwera oznacza przerwę do czasu odtworzenia z kopii.

Wersja z dnia 2026-09-08.