Środki techniczne i organizacyjne CarSpaIQ

CarSpaIQ · wersja 1.8.0 · obowiązuje od 20 września 2026 r.

1. Zakres i zasada doboru zabezpieczeń

Ten załącznik opisuje środki techniczne i organizacyjne stosowane przez SZCZERBOWSKI PIOTR TALITHA dla CarSpaIQ w wersji 1.8.0. Środki są dobierane do ryzyka, zakresu usługi i aktualnego stanu wiedzy zgodnie z art. 32 RODO. Nie stanowią obietnicy absolutnego bezpieczeństwa ani gwarantowanego SLA; są regularnie przeglądane i mogą być zastępowane środkami co najmniej równoważnymi.

2. Tożsamość, dostęp i rozdzielenie obowiązków

- indywidualne konta, silne hasła i weryfikacja e-mail; MFA jest zalecane użytkownikom organizacji i obowiązkowe dla operatorów platformy;
- role platformowe są fizycznie oddzielone od ról organizacji;
- autoryzacja serwerowa i najmniejsze uprawnienia dla użytkowników, procesów i baz;
- sesje mogą być przeglądane i unieważniane, a wrażliwe akcje wymagają świeżego uwierzytelnienia;
- dostęp administracyjny jest ograniczony, uwierzytelniany kluczem i docelowo prowadzony przez prywatną sieć administracyjną;
- osoby dopuszczone do danych są związane poufnością i otrzymują dostęp tylko w niezbędnym zakresie.

3. Izolacja organizacji i integralność danych

- każdy rekord klienta ma jawnego właściciela tenantowego, a relacje chronią composite FK i constraints;
- brak kontekstu organizacji powoduje odmowę zamiast globalnego fallbacku;
- policies, capabilities, kontrolery, joby, eksporty, pliki i cache ponownie weryfikują właściciela;
- negatywne testy Tenant A/Tenant B oraz uprawnień są częścią bramki release;
- istotne dowody prawne, wiadomości, snapshoty, próby providerów i audyt mają ochronę append-only lub integralności.

4. Szyfrowanie i sekrety

- ruch publiczny i połączenia SMTP używają TLS, a połączenia bazodanowe są uwierzytelnione i szyfrowane;
- wybrane pola PII są szyfrowane per tenant osobnym kluczem danych i wiązane z kontekstem kryptograficznym;

- klucze danych są przechowywane wyłącznie w opakowanej postaci; sekret środowiskowy pozostaje poza repozytorium;
- blind indexy umożliwiają ograniczone wyszukiwanie bez przechowywania jawnych identyfikatorów pomocniczych;
- sekrety runtime, bazy, Redis, backupu i dostępu administracyjnego są odseparowane od innych produktów oraz od kodu.

5. Prywatne pliki i bezpieczne uploady

- media są przechowywane poza publicznym docrootem w prywatnych, tenantowych ścieżkach;
- upload ma limity typu i rozmiaru, magic/MIME validation, kwarantannę i skan antymalware;
- obrazy przechodzą decode/re-encode i usunięcie zbędnych metadanych, w tym EXIF/GPS;
- pobranie wymaga bieżącej autoryzacji lub krótkotrwałej, podpisanej capability;
- integralność exact obiektu jest sprawdzana przez wersję, liczbę bajtów i SHA-256.

6. Operacje, logowanie i podatności

- produkcyjne wydania są immutable, wskazują exact commit i przechodzą testy, analizę statyczną, build oraz skan zależności/obrazów;
- migracje są forward-only, a konto aplikacji nie ma uprawnień DDL;
- logi i metryki używają correlation ID oraz centralnego scrubbera; nie zapisują celowo treści wiadomości, recipientów ani sekretów;
- zdarzenia bezpieczeństwa i wrażliwe operacje mają audyt odporny na zwykłe nadpisanie;
- aktualizacje, zależności i sygnatury antymalware podlegają kontrolowanemu utrzymaniu.

7. Dostępność, backup i odtworzenie

- baza, media i bezpieczna konfiguracja są objęte szyfrowanym, odseparowanym backupem z manifestem SHA-256;
- backup ma ograniczony dostęp, kontrolowaną retencję do 90 dni i test odtworzenia do izolowanego celu;
- kolejki, scheduler i workery mają ograniczone retry, lease, idempotentne outboxy i monitoring stanu;
- health checki obejmują aplikację, bazę, Redis, kolejki, scheduler, storage i skaner plików;
- bieżąca alfa nie jest środowiskiem HA; awaria fizycznej roli może powodować przerwę do odtworzenia.

8. Incydenty, ciągłość i usuwanie

Proces obejmuje ograniczenie dostępu, zabezpieczenie dowodów, ocenę zakresu i ryzyka, naprawę, odtworzenie, komunikację z administratorem oraz wnioski po zdarzeniu. Dane są usuwane lub anonimizowane po ustaniu celu i podstawy, z uwzględnieniem legal hold oraz cyklu szyfrowanych

kopii. Szczegóły zgłoszenia naruszenia wynikają z DPA, a wyjścia z osobnego załącznika.

9. Przegląd i kontakt

Istotne osłabienie zabezpieczeń albo nowa kategoria przetwarzania wymaga oceny ryzyka i aktualizacji pakietu. Pytania, dowody zgodności i uzgodnienie audytu: biuro@talitha.pl.