Środki techniczne i organizacyjne ClockIt

Wersja 2026-10-26-B2B-04.

Załącznik B do umowy powierzenia przetwarzania danych.

1 Organizacja ochrony

Za wykonanie zobowiązań Operatora odpowiada Patryk Pławski, kontakt@clockit.pl. Dostęp do danych jest przyznawany do konkretnego zadania osobom upoważnionym i związanym poufnością. Uprawnienia są ograniczane po zmianie zadania i odbierane po ustaniu potrzeby. Klient zarządza dostępem własnych użytkowników, a Operator dostępem administracyjnym do infrastruktury i wsparcia.

Środki dobiera się do ryzyka i zmienia wraz z architekturą, kategoriami danych i zagrożeniami. Zmiana nie może obniżać uzgodnionej ochrony bez odpowiednich środków zastępczych. Operator dokumentuje istotne decyzje, incydenty, wymagane upoważnienia i działania zaradcze. Klient może uzyskać informacje i skontrolować wykonanie zgodnie z umową powierzenia.

2 Uwierzytelnianie i role

Konta są przypisane do organizacji i ról, a w odpowiednich funkcjach również oddziałów lub rozmów. Operator zapewnia kontrolę dostępu po stronie serwera dla chronionych operacji oraz oddzielenie danych organizacji. Dostęp do kartotek, płac i dokumentów nieobecności wymaga właściwego uprawnienia. Samo ukrycie elementu interfejsu nie jest wystarczającą kontrolą dostępu.

Stałe hasła są przechowywane jako skróty bcrypt. Minimalna długość wynosi 8 znaków; użytkownik powinien stosować unikalne hasło i chronić pocztę. Administrator rejestrujący firmę otrzymuje startowe hasło ważne 24 godziny i zmienia je przy pierwszym logowaniu. Zaproszony pracownik ustawia własne hasło przez link. Procedura odzyskania wykorzystuje hasło tymczasowe ważne 15 minut i wymaga zmiany. Krótkotrwałe hasła są treścią wiadomości e-mail i wymagają ochrony skrzynki; nie są stałym hasłem przechowywanym w postaci jawnej w bazie użytkowników.

Dla ról administracyjnych, kierownika i grafika działa domyślna konfiguracja TOTP 2FA. Użytkownik może wyłączyć ją wyłącznie dla własnego konta po weryfikacji hasła i kodu lub dozwolonej metody odzyskania. Operator platformy podlega obowiązkowemu 2FA. Zapamiętane urządzenie jest honorowane najwyżej 30 dni, z możliwością wcześniejszego unieważnienia przy zmianie zabezpieczeń. Reset 2FA wymaga sprawdzenia uprawnienia, a sama znajomość adresu e-mail nie wystarcza.

3 Sesje, transmisja i dane przechowywane

Usługa korzysta z HTTPS i weryfikacji certyfikatów przy połączeniach wymagających ochrony. Tokeny, hasła, klucze i sekrety nie są przeznaczone do publikacji w repozytoriach, logach lub materiałach pomocy. Klucze produkcyjne są zarządzane oddzielnie od kodu, z ograniczonym dostępem i możliwością wymiany po ujawnieniu.

Wybrane wrażliwe pola, sekrety TOTP, przejściowa kolejka wysyłki haseł i dokumenty nieobecności są chronione szyfrowaniem AES-256-GCM w odpowiednich ścieżkach usługi. Kopie bazy są dodatkowo szyfrowane przed wysłaniem do magazynu B2. Nie oznacza to szyfrowania całego telefonu lub całej komunikacji metodą end-to-end. Treści muszą być odczytywane w systemie w zakresie koniecznym do wykonania uprawnionej funkcji.

Panel korzysta z localStorage dla tokenu sesji i dowodu zaufania urządzenia. Ich ważność sprawdza serwer. Wylogowanie usuwa właściwy token sesji, lecz nie musi usuwać dowodu zaufania. Na telefonie wybrane dane uwierzytelniania i klucze korzystają z systemowego bezpiecznego magazynu; dane oczekujące na synchronizację są ograniczone do potrzeb aplikacji. Pobrane pliki i eksporty wymagają również ochrony przez Klienta.

4 Pliki i udostępnianie

Operator ogranicza dopuszczalne typy i rozmiary plików według dokumentu 03 oraz zapewnia kontrolę przesyłania i udostępniania odpowiednią do ich charakteru. Dane nie są przeznaczone do publicznego udostępnienia wyłącznie na podstawie nazwy pliku lub roli w innej organizacji. Klient przekazuje dokumenty kadrowe i informacje zdrowotne właściwą ścieżką, ogranicza adresatów i nie zastępuje jej publikacją w ogólnym kanale.

Nowe pliki w obsługiwanych ścieżkach czatu i dokumentów mogą być przechowywane w PostgreSQL; starsze media mogą korzystać z zewnętrznego magazynu. Usuwanie obejmuje rekord oraz powiązany obiekt u właściwego dostawcy. Klient chroni kopie pobrane na urządzenia i wysłane poza ClockIt; Operator nie usuwa ich z cudzej skrzynki lub dysku przez usunięcie rekordu w aplikacji.

5 Kopie i odtwarzanie

Proces kopii PostgreSQL jest uruchamiany przez GitHub Actions według harmonogramu czterech wykonań dziennie. Zrzut jest szyfrowany AES-256-GCM, przekazywany do prywatnego B2 i weryfikowany w procesie kopii. Sygnał wykonania służy kontroli terminowości w Healthchecks.io. Harmonogram zewnętrznego wykonawcy nie jest gwarancją uruchomienia dokładnie co sześć godzin ani samodzielną gwarancją RPO.

Kopia bazy obejmuje rekordy i zapisane w niej bajty załączników. Nie obejmuje automatycznie zewnętrznych obiektów Cloudinary, kluczy aplikacji i sekretów. Operator zapewnia ochronę danych w przyjętym zakresie także dla pozostałych miejsc ich przechowywania oraz oddzielne zabezpieczenie materiału potrzebnego do odtworzenia. Dostęp do magazynu i kluczy jest ograniczony do upoważnionych osób.

Kopie chroni Object Lock z okresem 30 dni. Nie służą do zwykłego udostępniania danych usuniętych z produkcji. Cykl usuwania i granicę dalszego przechowania określa dokument 08. Operator kontroluje powodzenie kopii, reaguje na brak wykonania, okresowo sprawdza odtwarzanie i dokumentuje wynik, w tym zakres plików i rekordów. Po odtworzeniu ponownie wykonuje zapisane dyspozycje usunięcia i ograniczenia. Umowa nie określa odrębnej gwarancji godzinowej czasu odtworzenia ani procentowej dostępności.

6 Utrzymanie i wsparcie

Operator aktualizuje istotne zależności i zabezpieczenia z uwzględnieniem ryzyka, sprawdza uprawnienia i walidację przy zmianach oraz oddziela testy od niepotrzebnego użycia danych produkcyjnych. Próbki do pomocy są minimalizowane. Nie przesyła się pełnej bazy do narzędzia konsultanta lub testowego tylko z powodu wygody. Udostępnienie wymaga właściwej podstawy i ochrony.

Zgłoszenia obsługuje kontakt@clockit.pl. Wsparcie nie prosi o stałe hasło, sekret TOTP ani kody odzyskiwania. W razie potrzeby dostępu do danych Operator określa zadanie i osoby uprawnione. Rutynowe logi są ograniczone do danych potrzebnych do działania i bezpieczeństwa; nie służą jako magazyn haseł i pełnych załączników.

7 Incydenty i przegląd skuteczności

Po wykryciu zagrożenia Operator ogranicza jego skutki, zabezpiecza dowody, ustala zakres i przyczynę oraz wdraża środki zaradcze. Naruszenie powierzonych danych zgłasza bez zbędnej zwłoki, najpóźniej w ciągu 24 godzin od stwierdzenia, zgodnie z umową powierzenia. Nie czeka na zakończenie całego dochodzenia, aby przekazać pierwszą informację.

Przegląd ochrony obejmuje kontrolę uprawnień, dostępu do plików, aktualizacji, kopii, usuwania i ryzyka transferów. Operator udostępnia Klientowi potrzebną dokumentację w ramach audytu, z ochroną innych klientów i tajemnic bezpieczeństwa. Klient odpowiada za zabezpieczenie urządzeń, wyłączanie nieaktualnych kont i zgodne z prawem wykorzystanie funkcji w organizacji.