VendoCerta

MATERIAŁY VENDOCERTA

Bezpieczeństwo i RODO

Ochrona danych w VendoCercie jest rozłożona po całym produkcie: w tym, jak zapisywana jest historia, kto może zobaczyć który dokument, jak szyfrowany jest rachunek bankowy i czego rola celowo nie może. Ta strona zbiera to w jednym miejscu — łącznie z fragmentami, w których uczciwa odpowiedź brzmi „jeszcze nie”.

5	5	AES-256
ról z rozdziałem uprawnień	reguł, których nie da się obejść	szyfrowanie danych wrażliwych

Wygenerowano: 2026-08-21

vendocerta.com

VENDOCERTA

Sześć pytań, które pada jako pierwsze.

Czy dane mogą zostać u nas?

Tak. VendoCerta instaluje się na infrastrukturze, którą kontrolujecie.

Jak chronione są dane wrażliwe?

AES-256-GCM w spoczynku; odsłonięcie wymaga ponownego hasła i powodu zapisywanego w historii.

Kto ma dostęp do czego?

Role z rzeczywistym rozdziałem uprawnień. Nikt nie zmienia własnej roli.

Czy jest drugi składnik logowania?

Tak, obowiązkowy dla ról z dostępem do danych biznesowych.

Czy jedna osoba może zmienić rachunek bankowy dostawcy?

Nie. Cztery etapy, rozdzielone role, minimum dwie osoby.

Czy historię audytową da się poprawić?

Nie. Brak edycji i usunięcia w interfejsie, w żadnej roli, nawet dla właściciela.

Wpisu nie da się zmienić ani usunąć. Nawet właścicielowi.

Każde zapisane działanie staje się wpisem: logowanie, zmiana statusu dostawcy, decyzja o dokumencie, wysłane zaproszenie, pobrany plik. VendoCerta nie ma nigdzie funkcji edycji ani usunięcia wpisu i nigdy nie nadpisuje istniejącego zdarzenia.

Przed i po, przy każdej zmianie danych

Każdy wpis niesie: kto, co, kiedy — a przy zmianie także to, jak wartości wyglądały po obu stronach.

Odmowy też są zapisywane

Jeśli ktoś próbuje otworzyć coś, do czego nie ma uprawnień, ta próba jest wpisem. Powtarzające się próby są więc widoczne, a nie ciche.

Odfiltrowany widok to link

Filtry trafiają do adresu strony, więc konkretny wycinek historii można przekazać koledze — albo audytorowi — jako adres. Dokładnie tak działa link do historii pojedynczej sprawy.

Własna retencja — i mówimy o tym

Liczba dni u dołu ekranu historii audytowej to nie to samo pole co na ekranie ustawień. Retencja historii audytowej to osobne ustawienie, którego obecnie nie da się zmienić z interfejsu, a zmiana tamtego pola nią nie poruszy.

Jedyna operacja, której produkt odmawia ułatwienia.

Zmiana rachunku dostawcy to cztery etapy i reguła mówiąca, kto może je zakończyć. Wszystko inne w VendoCercie jest projektowane tak, żeby usuwać tarcie; to jest projektowane tak, żeby je zachować.

Szyfrowany od chwili zapisu

Numer rachunku nigdy nie leży w bazie jako zwykły tekst — AES-256-GCM w spoczynku, od momentu zapisania.

Odsłonięcie kosztuje trzy rzeczy

Uprawnienie do danych wrażliwych, ponowne podanie hasła mimo zalogowania i podanie powodu, który trafia do historii. Powód jest zapisywany; numer nigdy. Numer znika z ekranu po 45 sekundach.

Duplikaty są pokazywane, a nie ukrywane

Jeśli ten sam numer rachunku figuruje już przy innym dostawcy, ostrzeżenie trzeba świadomie odrzucić, zanim zatwierdzenie w ogóle stanie się możliwe.

Pięć ról, a ta zaskakująca jest celowa.

Administrator systemu utrzymuje instalację — konfiguracja, diagnostyka, kopie zapasowe — i nie ma żadnego wglądu w dostawców, dokumenty, sprawy ani rachunki bankowe. Dokładne przeciwieństwo administratora biznesowego, który prowadzi stronę dostawców i nie może odtworzyć kopii zapasowej.

UPRAWNIENIE	WŁAŚCICIEL	ADMINISTRATOR BIZNESOWY	ADMINISTRATOR SYSTEMU	RECENZENT	OBSERWATOR
Widzi dostawców i dokumenty	✓	✓	–	✓	✓
Dodaje i edytuje dostawców	✓	✓	–	–	–
Sprawdza dokumenty i decyduje o zatwierdzeniu	✓	✓	–	✓	–
Widzi dokumenty wrażliwe (dane do płatności)	✓	✓	–	–	–
Zarządza użytkownikami i rolami	✓	✓	✓	–	–
Odtwarza kopię zapasową	✓	–	–	–	–

Reguły, których żadna rola nie obejdzie

- Nikt — łącznie z właścicielem — nie może zmienić własnej roli.
- Administrator nie może utworzyć ani zdegradować konta z rolą właściciela.
- Ostatniego konta właściciela nie da się zdegradować ani wyłączyć, więc firma nigdy nie zostaje bez nikogo z pełnymi uprawnieniami.
- Uwierzytelnianie dwuskładnikowe jest obowiązkowe i nie do pominięcia dla właściciela, administratora biznesowego, administratora systemu i recenzenta. Obserwator może je włączyć, ale nie musi.
- Nieudane logowanie nigdy nie mówi, czy błędny był adres, czy hasło, więc ekranu nie da się użyć do sprawdzenia, czy dane konto istnieje.

Co jest przechowywane, kto może to sięgnąć i jak długo.

Dokumenty wrażliwe wymagają osobnego uprawnienia

Zwykłe dokumenty dostawcy widzi każdy, kto ma dostęp do jego karty. Dokumenty oznaczone jako wrażliwe — głównie związane z płatnościami — wymagają dodatkowego uprawnienia, co w praktyce oznacza wyłącznie właściciela i administratora. Próba otwarcia bez niego kończy się odmową, a odmowa jest zapisywana.

Pliki nigdy nie mają stałego adresu

Pobranie idzie przez podpisany cyfrowo link ważny kilka minut i związany z Waszą firmą. Otwarcie go z innego kontekstu nic nie da. Każde pobranie pliku wrażliwego jest audytowane osobno.

Retencja: domyślnie siedem lat

Ustawienie dokumentów i retencji ma domyślnie 2555 dni, zgodnie z typowymi wymogami audytu zakupowego, i można je zmienić w każdej chwili. Uczciwie: dziś zapisuje ono Waszą politykę i będzie napędzać przyszłe porządki — nic nie jest kasowane automatycznie tylko dlatego, że termin minął.

Zaproszenia wygasają, a ponowne wysłanie unieważnia

Link z zaproszeniem to jednorazowy, losowy token o ograniczonym czasie życia, domyślnie tydzień. Wysłanie nowego zaproszenia natychmiast unieważnia poprzednie, nawet jeśli ktoś je otworzył — i obecnie to jedyny sposób odcięcia linku; nie ma osobnego przycisku unieważnienia.

Dane bankowe zaszyfrowane w spoczynku

AES-256-GCM od chwili zapisu. Podany powód odsłonięcia numeru trafia do historii audytowej; sam numer nigdy.

Raport dla wsparcia bez danych

Zakładka diagnostyki w centrum systemu tworzy raport dla wsparcia technicznego zawierający wersje, liczniki i zamaskowane linie logów — nigdy treści dokumentów, danych bankowych ani danych osobowych dostawców.

Pytania, które audytor przysyła jako pierwsze.

Czy VendoCerta to usługa chmurowa, której powierzamy dane?

Nie. Instaluje się na maszynie, którą kontrolujecie. PostgreSQL, magazyn plików i podgląd poczty działają jako przenośne binaria wewnątrz folderu projektu — nic nie jest instalowane w Windows, bez praw administratora, Docker opcjonalnie. Internet potrzebny jest przy pierwszym uruchomieniu, żeby pobrać te usługi; potem instalacja jest Wasza.

Czy dostaniemy dokumentację techniczną wykraczającą poza tę stronę?

Tak. Instalacja zawiera model bezpieczeństwa i model zagrożeń jako dokumenty w repozytorium — te same źródła, z których powstała ta strona. Poproście osobę utrzymującą Waszą instalację albo nas przez formularz demo, zaznaczając, że to na potrzeby przeglądu bezpieczeństwa.

Do czego ma dostęp asystent AI?

Wyłącznie do tego, co osoba pytająca i tak może zobaczyć, i nigdy nie wykonuje działania bez jej wyraźnego potwierdzenia — uprawnienia są sprawdzane ponownie w momencie kliknięcia, wobec osoby, która klika. Nie może zatwierdzić, odrzucić ani zawiesić dostawcy, nie może zmienić roli i nie może niczego usunąć.

Czy reset hasła pozwala ominąć uwierzytelnianie dwuskładnikowe?

Nie. Dla ról, w których drugi składnik jest obowiązkowy, jest obowiązkowy na każdej drodze do konta, także po resecie.

Gdzie trafiają maile w trakcie pilotażu?

Do lokalnej skrzynki podglądowej na samej instalacji, a nie do prawdziwych odbiorców — więc pilotaż nie może przypadkiem napisać do dostawcy. Zakładka instalacji w centrum systemu mówi, z której skrzynki dana instalacja faktycznie korzysta.