

МАТЕРІАЛИ VENDOCERTA

Безпека та захист даних

Захист даних у VendoCerta розподілений по всьому продукту: як записується історія, хто може бачити який документ, як шифрується банківський рахунок, і чого роль навмисно не може робити. Ця сторінка збирає все це в одному місці.

5

ролей із розділенням
повноважень

5

правил, які не обійти

AES-256

шифрування чутливих
даних

Шість запитань, які виникають найперше.

Чи можуть дані залишатися у нас?

Так. VendoCerta встановлюється на інфраструктурі, яку контролюєте ви.

Як захищені чутливі дані?

AES-256-GCM у стані спокою; розкриття вимагає повторного введення пароля та причини, яка записується в історію.

Хто має доступ до чого?

Ролі з реальним розподілом повноважень. Ніхто не змінює власну роль.

Чи є другий фактор входу?

Так, обов'язковий для ролей із доступом до бізнес-даних.

Чи може одна людина змінити банківський рахунок постачальника?

Ні. Чотири етапи, розділені ролі, щонайменше дві людини.

Чи можна виправити журнал аудиту?

Ні. Немає функції редагування чи видалення в інтерфейсі, у жодній ролі, навіть для власника.

Запис не можна змінити чи видалити. Навіть власнику.

Кожна збережена дія стає записом: вхід у систему, зміна статусу постачальника, рішення щодо документа, надіслане запрошення, завантажений файл. У VendoCerta ніде немає функції редагування чи видалення запису, і вона ніколи не перезаписує наявну подію.

До і після, при кожній зміні даних

Кожен запис містить: хто, що, коли — а при зміні також те, якими значення були з обох боків.

Відмови теж записуються

Якщо хтось намагається відкрити те, на що не має прав, ця спроба стає записом. Тож повторювані спроби видно, а не приховано.

Відфільтрований перегляд — це посилання

Фільтри потрапляють в адресу сторінки, тож конкретний фрагмент історії можна передати колезі — чи аудитору — як адресу.

Власна ретенція — і ми говоримо про це відкрито

Кількість днів унизу екрана журналу аудиту — не те саме поле, що на екрані налаштувань. Ретенція журналу аудиту — окреме налаштування, яке наразі не можна змінити з інтерфейсу, і зміна іншого поля на неї не впливає.

Єдина операція, полегшення якої продукт відмовляється надавати.

Зміна банківського рахунку постачальника складається з чотирьох етапів і правила про те, хто може їх завершити. Усе інше у VendoCerta спроектовано так, щоб усувати тертя; це спроектовано так, щоб його зберігати.

Зашифровано з моменту збереження

Номер рахунку ніколи не зберігається у відкритому вигляді в базі даних — AES-256-GCM у стані спокою, з моменту збереження.

Розкриття коштує трьох речей

Право на чутливі дані, повторне введення пароля попри активний вхід, і причина, яка потрапляє в історію. Причина зберігається; номер — ніколи. Номер зникає з екрана через 45 секунд.

Дублікати показуються, а не приховуються

Якщо той самий номер рахунку вже фігурує в іншого постачальника, попередження потрібно свідомо відхилити, перш ніж затвердження взагалі стане можливим.

П'ять ролей, і та, що дивує, — навмисна.

Системний адміністратор підтримує встановлення справним — конфігурація, діагностика, резервні копії — і не має жодного доступу до постачальників, документів, справ чи банківських рахунків. Пряма протилежність бізнес-адміністратора, який веде сторону постачальників і не може відновити резервну копію.

МОЖЛИВІСТЬ	ВЛАСНИК	БІЗНЕС-АДМІНІСТРАТОР	СИСТЕМНИЙ АДМІНІСТРАТОР	ПЕРЕВІРЯЮЧИЙ	СПОСТЕРІГАЧ
Бачить постачальників і документи	✓	✓	—	✓	✓
Додає та редагує постачальників	✓	✓	—	—	—
Перевіряє документи та вирішує щодо затвердження	✓	✓	—	✓	—
Бачить чутливі документи (платіжні дані)	✓	✓	—	—	—
Керує користувачами та ролями	✓	✓	✓	—	—
Відновлює резервну копію	✓	—	—	—	—

Правила, які жодна роль не може обійти

- Ніхто — включно з власником — не може змінити власну роль.
- Адміністратор не може створити чи понизити обліковий запис із роллю власника.
- Останній обліковий запис власника не можна понизити чи вимкнути, тож компанія ніколи не залишається без нікого з повними правами.

- Двофакторна автентифікація обов'язкова і без можливості пропустити для власника, бізнес-адміністратора, системного адміністратора та перевіряючого. Спостерігач може її увімкнути, але не зобов'язаний.
- Невдалий вхід ніколи не повідомляє, чи була неправильною адреса, чи пароль, тож екран не можна використати для перевірки існування облікового запису.

Що зберігається, хто може отримати доступ і як довго.

Чутливі документи вимагають окремого права

Звичайні документи постачальника бачить кожен, хто має доступ до його картки. Документи, позначені як чутливі — переважно пов'язані з платежами — вимагають додаткового права, що на практиці означає лише власника та адміністратора. Спроба без нього завершується відмовою, і відмова записується.

Файли ніколи не мають постійної адреси

Завантаження відбувається через цифровий підписаний лінк, дійсний кілька хвилин і прив'язаний до вашої компанії. Відкриття його з іншого контексту нічого не дасть. Кожне завантаження чутливого файлу аудитується окремо.

Ретенція: сім років за замовчуванням

Налаштування документів і ретенції за замовчуванням становить 2555 днів, відповідно до типових вимог аудиту закупівель, і його можна змінити будь-коли. Чесно кажучи: сьогодні воно фіксує вашу політику і керуватиме майбутнім прибиранням — нічого не видаляється автоматично лише тому, що минув термін.

Запрошення закінчуються, а повторне надсилання їх скасовує

Посилання-запрошення — це випадковий токен з обмеженим терміном дії, за замовчуванням тиждень — навмисно не одноразовий, щоб постачальник міг повернутися до незавершеної форми тим самим посиланням. Надсилання нового запрошення миттєво скасовує попереднє, навіть якщо його вже відкрили — наразі це єдиний спосіб відрізати посилання; окремої кнопки скасування немає.

Банківські дані зашифровані в стані спокою

AES-256-GCM з моменту збереження. Вказана причина розкриття номера потрапляє в журнал аудиту; сам номер — ніколи.

Звіт для підтримки без даних

Вкладка діагностики в центрі системи створює звіт для технічної підтримки з версіями, лічильниками та замаскованими рядками журналу — ніколи зі вмістом документів, банківськими даними чи персональними даними постачальників.

Питання, які аудитор ставить найперше.

Чи є VendoCerta хмарним сервісом, якому ми довіряємо дані?

Ні. Встановлення відбувається на машині, яку контролюєте ви. PostgreSQL, сховище файлів і попередній перегляд пошти працюють як портативні бінарні файли всередині папки проєкту — нічого не встановлюється на рівні Windows, без прав адміністратора, Docker — за бажанням. Інтернет потрібен лише при першому запуску для завантаження цих служб; після цього встановлення належить вам.

Чи отримуємо ми технічну документацію окрім цієї сторінки?

Так. Встановлення містить модель безпеки та модель загроз як документи в репозиторії — ті самі джерела, з яких з'явилася ця сторінка. Запитайте про них у людини, яка обслуговує ваше встановлення, або в нас через форму демо, зазначивши, що це для перевірки безпеки.

До чого має доступ ШІ-асистент?

Лише до того, що особа, яка запитує, і так може побачити, і ніколи не виконує дію без її явного підтвердження — права перевіряються повторно в момент кліку, щодо особи, яка клікає. Він не може затвердити, відхилити чи призупинити постачальника, не може змінити роль і не може нічого видалити.

Чи скидання пароля дозволяє обійти двофакторну автентифікацію?

Ні. Для ролей, де другий фактор обов'язковий, він обов'язковий на будь-якому шляху до облікового запису, включно з шляхом після скидання.

Куди надходять листи під час пілоту?

У локальну поштову скриньку попереднього перегляду на самому встановленні, а не реальним отримувачам — тож пілот не може випадково написати постачальнику. Вкладка встановлення в центрі системи показує, яку скриньку насправді використовує конкретне встановлення.