FIREkit безпека

FAQ

Чи мої дані захищені?

Так, ваші дані надійно захищені з FIREkit. Ми використовуємо дата-центри Microsoft Azure та MongoDB Atlas, які дотримуються суворих галузевих стандартів ISO 27001 та SOC. Наші заходи безпеки включають міцні протоколи аутентифікації через Auth0, передову мережеву безпеку з файєрволами та техніки анонімізації даних для захисту вашої конфіденційності.

Чи продає FIREkit мою інформацію?

Ваша безпека та захист ваших даних є нашим пріоритетом. Ми ніколи не продамо, не опублікуємо та не поділимося вашими даними з третіми сторонами.

Що робити, якщо сервери FIREkit будуть зламані?

По-перше, ми не зберігаємо жодних чутливих даних та радимо вам не вводити ваші імена, картки, рахунки тощо. Якщо сервери FIREkit будуть зламані, ваші чутливі дані будуть абсолютно безпечними.
По-друге, всі ваші дані в додатку зашифровані під час зберігання та анонімізовані на наших серверах. Таким чином, навіть якщо хтось зламає систему та отримає доступ до резервної копії бази даних, він не зможе розшифрувати дані або асоціювати їх з реальною особою.

Режим захисту приватності

Не хвилюйтеся, за замовчуванням при логіні у нас включений прихований режим, який дозволяє безпечно використовувати сервіс у громадських місцях без ризику розкриття чутливих даних.

Чи втрачу я свої дані, якщо залишу FIREkit?

Ви можете експортувати свої дані в будь-який час, що забезпечує контроль над вашою інформацією. Ви можете створювати резервні копії своїх даних та безпечно передавати їх на іншу платформу.

Що, якщо я хочу все стерти?

Ви маєте можливість повністю видалити свій профіль і всі пов'язані з ним дані з додатку. Це дає вам змогу впевнено покинути платформу, гарантуючи, що ваша особиста інформація буде назавжди стерта. Незалежно від причин — чи то особисті

обставини, зміна інтересів, або просто бажання вийти з платформи — ви можете бути спокійні за свою конфіденційність та безпеку.

Коли я видаляю свої дані, чи можна їх відновити з резервної копії?

Коли ви видаляєте свій обліковий запис, ми відразу ж видаляємо всі ваші дані з нашої основної бази даних. Ми зберігаємо ротаційні резервні копії протягом 30 днів. Ваші дані будуть видалені з резервної копії у наступному циклі очищення резервної копії.

Оцінки безпеки та відповідність стандартам

Дата-центри

Фізична інфраструктура FIREkit розміщена та управляється в захищених дата-центрах Microsoft з використанням хмарного провайдера **Microsoft Azure**. Microsoft постійно управляє ризиками та проходить повторні оцінки для забезпечення відповідності галузевим стандартам. Сертифікати дата-центру Azure:

- ISO 27001, 27017, 27018 та 27701
- SOC 1, SOC 2

Додаткова інформація: документація про відповідність стандартам Azure

Інфраструктура бази даних FIREkit розміщена та управляється дата-центрами **MongoDB Atlas**. MongoDB вділяє увагу забезпеченню безпеки та захисту ваших даних за допомогою передових технічних та організаційних заходів безпеки, численних регуляторних деталей і відповідності стандартам, а також зростаючим наборам різноманітних атестацій та сертифікатів. Атестації та сертифікати MongoDB Atlas:

- ISO 27001, 27017, 27018 та 27701
- SOC
- CSA STAR,
- PCI DSS
- HIPAA, GDPR, VPAT, HITRUST, IRAP, TX-RAMP

Додаткова інформація: довідковий центр MongoDB

Аутентифікація

Інфраструктура аутентифікації FIREkit розміщена та управляється **Auth0** (Okta). Auth0 підтримує та відповідає вимогам багатьох структур та сертифікацій відповідності:

- ISO27001, ISO27018
- SOC 2 Type II
- HIPAA BAA

- Gold CSA STAR
- PCI DSS
- GDPR

Додаткова інформація: безпека Auth0

Платежі

Ми використовуємо процесор платежів, відповідний PCI, **Fondy** для шифрування та обробки платежів кредитними картками. Fondy має сертифікацію PCI DSS рівня 1 та PSD2.

Мережева безпека

Файєрволи

Файєрволи є важливими для контролю доступу з зовнішніх мереж і всередині внутрішніх систем. Доступ блокується за замовчуванням, і дозволяються лише необхідні порти та протоколи для ведення бізнесу. Системи класифіковані в групи безпеки файєрволів відповідно до їх функцій, що забезпечує обмежений доступ до необхідних портів та протоколів, знижуючи потенційні ризики.

Безпека даних

ДАНІ ПІД ЧАС ПЕРЕДАЧІ

Дані під час передачі відносяться до даних, які переміщуються між різними пристроями або мережами. Для забезпечення безпеки та конфіденційності ваших даних під час передачі FIREkit використовує стандартні протоколи шифрування, такі як TLS (Transport Layer Security), для шифрування даних, що переміщуються між вашим пристроєм та нашими серверами. Це шифрування запобігає несанкціонованому доступу або перехопленню ваших даних зловмисниками під час передачі.

ДАНІ ПРИ ЗБЕРІГАННІ

Дані при зберіганні стосуються даних, які зберігаються на диску або інших носіях, коли вони не передаються активно. FIREkit використовує міцні заходи шифрування для захисту ваших даних, коли вони зберігаються в наших базах даних. Наприклад, наш провайдер інфраструктури баз даних MongoDB Atlas використовує шифрування всього тома (диска) для захисту всіх даних при зберіганні, включаючи дані кластерів та резервні копії. Це шифрування забезпечує, що навіть якщо несанкціонований доступ буде отримано до фізичних носіїв даних, дані залишаться зашифрованими та незчитуваними без відповідних ключів дешифрування.

АНОНІМІЗАЦІЯ

Ваші облікові дані керуються соціальними логінами Auth0. Це дозволяє вам покладатися на стандарти безпеки цих провайдерів, включаючи багатофакторну аутентифікацію (що настійно рекомендується). Усі токени, передані додатку FIREkit, повністю анонімізовані, тому їх не можна простежити до окремих користувачів. Це забезпечує конфіденційність та безпеку користувачів під час взаємодії з додатком FIREkit.

РЕЗЕРВНІ КОПІЇ

Автоматичні резервні копії (щомісяця, щотижня, щодня) дозволяють нам швидко відновлювати ваші дані у разі втрати даних. Ці резервні копії також зашифровані.

Контакт

Якщо ви помітили зловживання, неправомірне використання / експлуатацію або ж стали жертвою інциденту з вашим обліковим записом, будь ласка, повідомте нас за адресою security@firekit.space.