finexer

Dashboard

Security at Finexer

Security is at the heart of what we do. Protecting your data is, therefore, our number one priority.

If you believe you've discovered a bug, or encountered any security-related issues, please get in touch at security@finexer.com or here. We will respond as quickly as possible to your report. We request that you not publicly disclose the issue until it has been addressed by Finexer.

Robust, Reliable, Safe, and Secure

We regularly install ongoing security updates and patches on our servers.
We never expose sensitive financial data once captured on our end. Sensitive data gets

masked or removed from transactions and logs.
We regularly use our automation tests to ensure that the software continues to perform properly.
We apply industry-standard coding guidelines, including OWASP recommendations for all development of the software including public website and API.

Encryption

Finexer uses Advanced Encryption Standard (AES). All sensitive data is encrypted with AES-256 and stored in isolated environment. This data store doesn't share credentials with another services and cannot be connected to via the internet. In addition, we practice consistent key rotation.

HTTPS and HSTS

HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of data between

the user's device and the internet site. Finexer forces HTTPS for all services using TLS (SSL), including our APIs, public website and the Dashboard. We also use HSTS to ensure browsers interact with Finexer only over HTTPS. This will force browsers to prevent requests from being sent through insecure connection (HTTP).

Two-factor authentication

This is authentication based on the use of two or more elements categorised as knowledge (i.e., something only the user knows), possession (i.e., something only the user possesses), and inherence (i.e., something the user is).
Your first layer of protection is your password. Two-factor authentication adds a second layer of protection - on Finexer, a unique verification code that changes every time you sign in. When enabled, internal team members will have to enter an authentication token from their mobile device prior to gaining

access to their account.

> We highly recommend to use this option.

Strong customer authentication (SCA)

One of the major implications of PSD2 is the focus on improving security in the payments space by emphasising strong customer authentication. An important element of SCA is two-factor authentication. Most consumers are aware of this even if they don't know it by that name. It's for those situations where inputting the username and password by themselves aren't considered secure enough, so additional steps are required. Obvious examples of such an approach are additional questions that only a consumer would know, such as "what's my mother's maiden name?" New approaches to two-factor authentication are emerging e.g., biometric recognition or fingerprint activation.