Security Practices at Stacker

Stacker was founded on the belief that software shouldn’t dictate how you work—you should dictate how it works. Stacker empowers people to design a near-infinite number of useful apps of their own, without learning to code.

From collaborative strategic planning, to managing global marketing campaigns, to powering the internal team of an organization, Stacker is empowering non-technical workers to rethink decades-old business practices in every industry.

The flexibility of Stacker enables a range of sensitive and mission-critical use cases. As such, we consider **privacy** and **security** to be core functions of our platform, as well as foundational requirements for all new feature development. Earning and keeping the trust of our users is our top priority.

Permission-based access controls

At the heart of Stacker's product offering is our Permissions System, which gives you the ability to restrict access to your data to certain users. This functionality is enforced by our servers to every API request, preventing malicious actors from accessing more information than you have granted access to.

Network and system security

When you use the Stacker service, the transmission of information between your device and our servers is protected using 256-bit TLS encryption. At rest, Stacker encrypts data using AES-256.

Stacker’s servers are located in the EU, in data centers that are SOC 1, SOC 2 and ISO 27001 certified. Stackers data centers have round-the-clock security, automatic fire detection and suppression, fully redundant power systems, and strict controls for physical access.

Application security

Stacker actively monitors ongoing security, performance and availability and runs automated security testing on an ongoing basis. In addition to internal scans, Stacker commissions external penetration tests on a regular basis.

How to report an issue

If you believe you've discovered a security-related issue, contact us at support@stackerhq.com.