STACK ACCESS & SPEND
STACKOON

June 2023

Information Security and Data Privacy

Stackoon Corp.

16192 Coastal Highway,
Lewes, DE 19958

Infrastructure and Security

Cloud Infrastructure Security

Stackoon platform is hosted on AWS cloud servers and inherits the physical security and SLAs of the largest cloud services provider. We also enforce strict employee data handling policies, including limiting the administrator access to our production environment to just the CTO. Separate access controls are also applied at each layer of infrastructure via detailed IAM policies. All application and user access logs are stored centrally and monitored, and are ready to be provided for external security and privacy audits.

Data Encryption and Hashing

We are paying specific attention to data security. All passwords and auth credentials are hashed and salted, all data in transit is 256-bit encrypted, all sensitive data is also encrypted at rest. Spending data from financial institutions is obtained through our partners - Plaid.com and GoCardless.com (ex Nordigen.com) - who only allow client requests using strong TLS protocols and ciphers. Additionally, all communication with financial institutions is transmitted over encrypted tunnels and all client communication utilizes cryptographically hashed headers and timestamps to verify authenticity.

Active Threat Monitoring

Stackoon uses industry-best logging & monitoring systems on both infrastructure and application levels. We use Mezmo (ex LogDNA) and NewRelic for centralized logging and continuous monitoring across the entire stack to detect and contain indicators of compromise such as account takeover attacks, password bruteforce, or stolen credentials in real-time. This allows us to get a live and in-depth view of the network, infrastructure, applications and end-user experience. End-user auditable logs of key activities within a workspace can be provided upon request.

Privacy and Account Controls

Information Privacy

Stackoon doesn’t require any Personally Identifiable Information (PII) except the name and email of a user. Any and all data that flows into a user account is treated as private, and is never shared with anyone else without the user's explicit permission. The user retains ownership of all the data that flows into the user account and can choose to delete all or parts of it at any time by sending the request to support@stackoon.io.

Data Handling

As a company that handles data of sensitive and confidential nature, we are fully aware of its custodial obligations. We have built a development process that requires minimal manual intervention, is constantly monitored, allows rapid response to issues, and encourages efficient software testing. We extensively utilize multiple staging and sandbox environments with mock data, while the production data is isolated and containerized. While we make sure every one of our employees understands their personal role in keeping your data safe from security compromises and data breaches, we additionally require every employee with even partial privileges to our production environment to sign NDAs and confidentiality agreements.

Access Controls

Users are provided with full control of their data, including the ability to delete a particular app, payment method (bank account) or the entire workspace they created. Stackoon allows admin users to grant different permissions and access levels to their users so they control how the data in their workspace is shared with the team.