Stacks

GDPR Processing Procedure

April 2024

Introduction

The Processing Procedures outlined in this document focus on specific security capabilities and features of Stacks Inc. (Stacks) and its products including Stacks, Stacks LITE and Stacks Mobile. Stacks provides secure platform services where customers have effective and manageable security to build trusted and secure web and mobile instances for their users. Stacks has a strong security culture and formal security policies, and its products have been used by enterprises over the last decade around the globe.

Security Features

Ensuring your information is safe and secure is paramount for any organization. Stacks is built to prevent the worst from happening by providing a secure CMS and application framework with robust security. Organizations around the world rely on Stacks for portals and applications, testing its security against the most stringent standards and ensuring protection against the most critical internet vulnerabilities in the world.

PROCEDURE	
What we collect	Username and email of each internal user is only collected. If batch loaded - it is the responsibility of the customer/administrator to have obtained the right to load user data on behalf of user.
What we control Stacks has defined the current sources of personal data as:	• Stacks Internal Users - Stacks has full control of data and is the owner of the data; • Integrated User Details - Stacks integrates data in real time via trusted services provided by other vendors. All security specified protocols are followed. Stacks does not retain this data beyond the session and is not the owner and/or controller of the data; and • Automated individual decision-making including: ○ MailChimp: Stacks Newsletter ○ Microsoft Teams: Stacks product demonstrations and training bookings & online sessions; and ○ Zendesk: Stacks Support Desk.
Processing Procedure (technical)	• Integrated Users ○ Information stored during session only. ○ Displayed to user for purposes of identification to support 'My Account' functionality. ○ Password hashed. • Internal Users ○ Information stored during session Displayed to user for purposes of identification to support 'My Account' functionality. ○ Password hashed. ○ Data stored on the Stacks platform. ○ Data stored as per security protocols outlined in Security White Paper and within internal proprietary security procedure.

Data Processing Details

ACCESS MANAGEMENT	
What is your password policy/standard (e.g. length, complexity, expiration etc.)	Stacks leverages real-time integrations with local SSO systems and thus does not store user passwords beyond the session and uses SHA512 with a salt. Stacks runs the hash through PHP's hash function numerous times to increase the computation cost of generating a password final hash (a security technique called stretching). Stacks internal authentication options employ strong password programs that may be configured on implementation to suit the policies of the customer.
How is your password policy enforced?	Stacks' password policy is technically enforced to require minimum password length and complexity, as well as password history and duration, with configuration specified by the customer.
How many failed login attempts are permitted before the application locks out users? (e.g. Locked out beyond 5 attempts; Locked out after 5 or less attempts; Never locked out, etc.)	Stacks will lock an account after five (5) failed login attempts by default. This may be adjusted on request. Reset options will be presented.

APPLICATION SECURITY	
What type of encryption, if any, is used for password storage?	SHA512 hash with a salt.
Please describe any and all encryption algorithms your application utilizes, and the key sizes employed. Please describe any and all hash functions your application uses.	SSL TLS 1.2/1.3 with 2048-bit encryption. Passwords are stored using a SHA512 with a salt. We run the hash through PHP's hash function numerous times to increase the computation cost of generating a password final hash (a security technique called stretching).

BACKUP AND DISASTER RECOVERY	
What is your backup policy for customer data and supporting systems?	Backups are taken care of by the Stacks team and our response times are as follows: • The Recovery Time Objective (RTO) for Stacks is 6 hours. • The Recovery Point Objective (RPO) for Stacks is 2 hours. These objectives are obtained in part because customers are backed up on the following schedule: • Hourly and retained for seven (7) days. • Daily and retained for two (2) years.
How frequently are backups performed (More than once a day, Weekly, Daily or Monthly)?	Stacks backups are taken hourly and retained for seven (7) days, and daily which are retained for two (2) years.
Do you have a disaster recovery plan? If yes, where are your recovery data centers located and what are the RPO (recovery point objective) and RTO (recovery time objective) for services?	Yes. The Recovery Time Objective (RTO) for Stacks is six (6) hours. The Recovery Point Objective (RPO) for Stacks is two (2) hours.
Can user data be recovered separately from other customer data?	Yes. Each Stacks customer has a dedicated database that contains all their data and configurations.
How long after termination of the business agreement would you keep copies of user data?	No more than 30 days.

ENDPOINT AND SERVER SECURITY	
Please describe your patch deployment and implementation process (including timelines for implementation and how they are prioritized). Does the process differ for critical and non-critical patches?	Backups are taken care of by the Stacks team and our response times are Stacks operates on a continuous deployment model with weekly releases including but not limited to security and non-security related patches, updates, enhancements, and bug fixes. These releases do not interfere with user or administrator access or performance with our redundant cloud infrastructure. Hot fixes (critical patches) may be applied in a matter of minutes if required.
Please describe the hardware/OS platform (including virtual machine platforms) you have deployed in your environment.	The IT infrastructure that Stacks provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including: • SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70) • SOC 2 • SOC 3 • FISMA, DIACAP, and FedRAMP • DOD CSM Levels 1-5 • PCI DSS Level 1 • ISO 9001 / ISO 27001 • ITAR • FIPS 140-2 • MTCS Level 3 In addition, the flexibility and control allow customers to deploy solutions that meet several industry-specific standards, including: • Criminal Justice Information Services (CJIS) • Cloud Security Alliance (CSA) • Family Educational Rights and Privacy Act (FERPA) • Health Insurance Portability and Accountability Act (HIPAA) • Motion Picture Association of America (MPAA)

ENDPOINT AND SERVER SECURITY (CONTINUED)	
Have you deployed host-based firewalls, antivirus software, and/or host intrusion detection/prevention systems? Please provide details.	Stacks employs a host of Security protocols and systems, including but not limited to: Preventing XSS, CSRF, and other malicious data entry. Stacks ensures that data is validated and scrubbed before entry in the database. The system tests that user-entered data--and even the form fields themselves--match prescribed, expected formats and values. Tokens are injected into each form as it is generated, to protect against potential CSRF attacks. Database abstraction layer performs additional security checks on data as it is written to and retrieved from the database. Brute Force Detection - Stacks protects against brute-force password attacks by limiting the number of login attempts from a single IP address over a predefined period of time. Failed login attempts are logged and visible via the administrative interface. Stacks can also be configured to allow administrators to ban individual IP addresses and address ranges. Mitigating Denial of Service (DoS) Attacks - Stacks' extensible cache layer comes pre-configured with basic page, JavaScript, and CSS caches. The system supports deep integration with performance technologies such as Memcached, Redis, Varnish, and many popular CDN services. Individual components of Stacks are typically cached as well, and granular expiry is a common feature. This multi-layered cache architecture is extremely resistant to high volumes of traffic and allows for high-traffic websites. Addresses OWASP Top 10 Risks - Security feature address all the Open Web Application Security Project's top ten security risks, a list of the most commonly seen risks in practice. Cookies / User Data - The Stacks platform has session and cookie data is set to expire after three (3) hours. The following provides a listing of the primary cookies that the Stacks platform uses. • Authenticated users will have a timestamp of their visit recorded in the website logs under their user profile. • Protective Block - Our hosting service has a protective blocking feature that, under certain circumstances, restricts access to web sites with security vulnerabilities. We use this partial blocking method to prevent exploitation of known security vulnerabilities. The protective block is meant for high impact, low complexity attacks.
Do you regularly perform vulnerability assessment on your production environment? If yes, what is the frequency of vulnerability assessments?	The Stacks platform is backed by a platform security team consisting of dozens of experts from around the world which are employed to validate and respond to security issues pertaining to the platform employed by Stacks. Stacks maintains a database of signatures of known security vulnerabilities. We analyze the code of your application: When we release new code Regularly when new vulnerabilities are added to our database If a vulnerability deemed as critical is detected, our automated systems decline the release for development websites, we run complete blocks, and the error message gives us detailed information about the vulnerability. Unblocking is automated upon resolution of the security risk. The block is removed soon after a customer applies a security upgrade and removes the vulnerability.

Appendix A - General Data Information

Performance and Hosting

Stacks production instances are run on a 99.9% uptime-guaranteed managed host with 24/7 support. The managed host also monitors hardware and network connections for reliability purposes. 99.99% uptime is available with Stacks Premium.

Stacks utilizes a cloud environment to maintain a high degree of security while integrating all recommended information security standards as defined by ISO 27001. This includes the following:

- Enforces the use of highly secure RSA keys for server access and encryption;
- Maintains centralized logging of all servers;
- Regularly patches servers and applications;
- Enforces the use of firewalls and server monitoring; and
- Follows the openSCAP security guidelines for all servers not on our managed host.

Data Sovereignty

Stacks provides organizations with the ability to maintain data sovereignty by having data centers and servers located in the United States and Europe. More details can be found in the Stacks Security White Paper.

Secure Access

Stacks supports salted hash passwords with stretching applied (multiple hashes) for native Stacks users such as Staff users stored in the database. Third-party authenticated users such as ILS authenticated patrons are supported by a salted hash encryption method. Stacks also supports a variety of password policies such as minimum length, complexity, or expiration. Industry standard authentication practices are also supported including SSL and 2-factor authentication.

Granular User Access Control

Stacks provides a hierarchical role structure which is designed to support all levels of staff. Intricate moderation rules such as requiring proofing and approval before publishing with email notifications, ensures safe and responsible workflows within your organization. Administrators can control who can see and who can modify every part of the site including menu links and features that can be automatically hidden from users who do not have appropriate access. For example, a user role could be created that allows a user to create and update content, but not publish or delete it--permissions reserved for the editor role--while administrative settings are reserved for a separate role entirely. These roles can be further refined by individual organizations post implementation as necessary. Default roles include Administrator, Booking Manager, Event Manager, Contributor, Editor, and Moderator.

Preventing XSS, CSRF, and other malicious data entry

Stacks ensures that data is validated and scrubbed before entry in the database. The system tests that user-entered data--and even the form fields themselves--match prescribed, expected formats and values. Tokens are injected into each form as it is generated, to protect against potential CSRF attacks. Database abstraction layer performs additional security checks on data as it is written to and retrieved from the database.

Brute Force Detection

Stacks protects against brute-force password attacks by limiting the number of login attempts from a single IP address over a predefined period of time. Failed login attempts are logged and visible via the administrative interface. Stacks can also be configured to allow administrators to ban individual IP addresses and address ranges.

Mitigating Denial of Service (DoS) Attacks

Stacks' extensible cache layer comes pre-configured with basic page, JavaScript, and CSS caches. The system supports deep integration with performance technologies such as Memcached, Redis, Varnish, and many popular CDN services. Individual components of Stacks are typically cached as well, and granular expiry is a common feature. This multi-layered cache architecture is extremely resistant to high volumes of traffic and allows for high-traffic websites.

Addresses OWASP Top 10 Risks

Security feature address all of the Open Web Application Security Project's top ten security risks, a list of the most commonly seen risks in practice.

Cookies / User Data

The Stacks platform has session and cookie data is set to expire after three (3) hours. The following provides a listing of the primary cookies that the Stacks platform uses. Authenticated users will have a timestamp of their visit recorded in the website logs under their user profile.

Protective Block

Our hosting service has a protective blocking feature that, under certain circumstances, restricts access to web sites with security vulnerabilities. We use this partial blocking method to prevent exploitation of known security vulnerabilities. The protective block is meant for high impact, low complexity attacks.

Additional Information

Further information can be found in the Stacks Security White Paper and Technical Data Sheet located here https://hub.stacks4libraries.com/hc/en-us/articles/16125757273371-Security-Whitepaper