Security White Paper

June 2018

Disclaimer

The following is intended to outline product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality. The development, release, and timing of any features or functionality described for Stacks' products remains at the sole discretion of Stacks.

EBSCO | Stacks

Table of Contents

Introduction

This white paper focuses on security specific capabilities and features of Stacks and its products including Stacks, Stacks LITE, Stacks Premium, 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 organizations over the last decade around the globe.

Subscription Service Built for Trust

Stacks' security philosophy is built around the use of industry leading technology and security standards. 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 Content Management System (CMS) and application framework with robust security. Organizations around the world rely on Stacks for websites and mobile applications, testing its security against the most stringent standards and protection against the most critical internet vulnerabilities in the world.

SaaS - Subscription Service

Stacks is a subscription service. This means that we take care of the maintenance behind the scenes so you can focus on what you're passionate about, creating a great experience. One affordable annual license fee guarantees all your integrations will be maintained, software and hardware updates are taken care of and security remains at an industry best.

Shared Security Responsibility Model

The security measures Stacks employs differ from the more traditional on-premises security. Security responsibilities are shared between your organization and Stacks. In this case, Stacks is responsible for securing the underlying infrastructure that supports the subscription service, and you're responsible for anything you put on the cloud such as your website content. This shared security responsibility model can help to increase the level of security in place while reducing your operational burden in many ways.

The amount of security configuration work you have to do varies depending how sensitive your data is. However, there are certain security features—such as individual user accounts and credentials, SSL/TLS for data transmissions, and user activity logging—that you should employ. Additional details regarding these features is outlined below.

Hosting and Performance

Stacks production instances are run on a 99.9% uptime-guaranteed managed host (99.99% uptime available with Stacks Premium). Stacks monitors hardware and network connections for reliability purposes. 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 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. This ensures 99.9% uptime-guaranteed managed host (99.99% uptime available with Stacks Premium). Those looking to locate data in centers located in Canada will be provided with 99% uptime-guaranteed managed host.

Stacks Security Responsibilities

Stacks Inc. is responsible for the infrastructure that runs all of the web and mobile platform services offered and ensuring that this infrastructure is well managed and is secure. These services provide the scalability and flexibility of cloud-based resources with the additional benefit of being managed. For these services, you are required to configure logical access controls and protect your account credentials.

Customer Security Responsibilities

With Stacks, your service is managed meaning you don’t have to worry about maintenance or security updates - Stacks handles that for you. But as with all services, you should protect your Stacks account credentials and set up individual user accounts so that each of your users has their own credentials and you can implement a secure workflow. You are also responsible for the management any third-party application software or utilities you install on the instances.

IT Infrastructure

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 allows 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)

Data Centre Details

Physical and Environmental Security

The data centers employed by Stacks are state of the art, utilize innovative architectural and engineering practices, and are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Access and information is only granted to data centre employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked. All physical access to data centers by data centre employees is logged and audited routinely.

Fire Detection and Suppression

Automatic fire detection and suppression equipment is installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are

conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

Data centres monitor electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Business Continuity Management

Stacks' employs infrastructure that has a high level of availability and deploys resilient IT architecture. The system used is designed to tolerate system or hardware failures with minimal customer impact.

Incident Response

The Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution.

Content Management System CMS and Application Framework

Stacks is built on a proven, stable, and secure CMS and application framework with robust security in mind. Many security problems are prevented entirely by strong coding standards and rigorous review process. Security features include, but are not limited to:

Dedicated Platform Security Team

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.

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, Moderator, Editor, Contributor and User.

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 Memcache, 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.

SESS_

This is a Drupal session cookie used when an authorized user logs in. This only applies to authenticated users and not when someone is browsing the site anonymously.

_ga & _gat

These are both cookies used for Google Analytics.

googletrans

This cookie is set when using the Google Translate functionality to ensure the website is translated into the language selected.

__unam
Used by ShareThis, this plugin is used for social sharing of website content.

has_js
This cookie records whether the browser has enabled JavaScript. This cookie is going to exist for almost all users as Javascript is required to utilize the majority of functions of Stacks.

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.

Support

Stacks is a cloud-based website platform and is sold as a managed service meaning there are no additional staff required for support and maintenance. To ensure you are able to receive help when you need it, Stacks is supported by both EBSCO Customer Support and the Stacks Support Desk.

Incident Response

Stacks incident response is split into two (2) categories: automated and alerted. The Stacks Automated Response System constantly monitors Stacks instances and alerts the appropriate personnel if and when action is needed for maintenance and reliability. If a site is unresponsive, an alert is sent to multiple personnel to immediately address the issue.

The Stacks Alerted Response System allows end-users such as technical staff to submit an alert. If an organization is reporting difficulty accessing services, they can communicate through the Stacks ticketing system whereby the issue will be diagnosed and resolved with frequent updates communicated.

Data Process FAQ

What is your password policy/standard (e.g. length, complexity, expiration etc)?

Stacks leverages real-time integrations with local Single Sign-on (SSO) systems and thus does not store user passwords beyond the user session with a SHA512 salted hash. Stacks runs the hash through PHP 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 often are your infrastructure (non-application) administrative passwords audited against your policy? (e.g. Once in 3 Months, 3- 12 Months, Never, etc)?

Yearly on average, but may be conducted periodically as well.

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.

Once a user is locked out, will the account automatically unlock after a set period of time? If yes, how long?

Stacks accounts will not automatically unlock after a period of time. The administrator will need to reset the account's password by using the 'Forgot Your Password" link on the login page, or by contacting Stacks Support for assistance.

Do you maintain and review your customer, your employee and administrator access logs? If yes, how long are the logs retained?

Only active user sessions are retained within the application. Server side logs are reviewed as necessary. We do not log sessions for integrated but do track admin content changes with moderation feature.

How would users authenticate to your environment? e.g. one factor (user id and password) or multi factor authentication (user id, password, secure token, digital certificates, Kerberos etc.)?

Stacks offers a variety of methods for authenticating users, including one and multifactor authentication, integrated and non-integrated options, as outlined below:

- IP Address
- User ID and Password
- Active Directory/LDAP Authentication
- OpenAthens Authentication
- Shibboleth Authentication
- HTTPS Authentication

Sites may select the best method to meet their user-authentication needs, and sites can use the Stacks Dashboard to set up their method of authentication.

Can any third party (your service providers) access user data, and if so, how? How do they comply with your security requirements and controls?

Stacks will only provide access to data with affiliates and third parties (e.g., Contractors) involved in carrying out services if they similarly safeguard this information, consistent with the Stacks' Privacy Policy.

Does the policy require that access controls are in place to ensure that persons only have the minimal privileges they require on all applications, operating systems, databases, and network devices?

Yes. Stacks employs several security measures to ensure proper role-based access to information.

Please explain your process of provisioning and deprovisioning administrative access?

Processes and technology are in place to ensure that appropriate changes are made within 24 hours of personnel changes, however it is Stacks' policy that due to proprietary and confidential information as it relates to our security and contingency protocols, we cannot provide further detail surrounding our strategies and capabilities.

Describe your application account provisioning and deprovisioning process?

Stacks internal username/password accounts are created by library administrators via the Stacks Dashboard. Using the 'Create New User' feature, administrators can create a username that is unique to the system and a secure password. A unique email must also be provided. Integrated authentication methods qualify the user in real time and only store the data for the duration of the session.

How is the need for an account validated?

Initial accounts are created by Stacks staff. Additional accounts are created/controlled by the customer or facilitated via integrations with customer authentication systems.

Does the application support multiple roles or authorization levels of access?

Stacks accounts can be created with different levels of access to content. Usernames/passwords are assigned to a particular User and each User can contain unique profiles and content. Users can only access content enabled in their role that the username/password is assigned to.

What protocols will be used for data access and data movement between the various parts of the system, internally and/or externally?

The data that pertains to EBSCO services is fully mirrored across redundant data centers, sent through our dedicated fiber, so it is secure – not encrypted. Stacks provides encryption for data in transit with SSL TLS 1.2/1.3 with 2048 bit encryption.

Who manages and is responsible for these roles (i.e. the customer, the vendor, no roles exist, etc.)?

The customer.

How are application user passwords stored?

Stacks internal user passwords are stored using a salted SHA512 hash. Integrated authentication methods do not require Stacks to store password at all beyond the session.

What type of encryption, if any, is used for password storage?

SHA512 hash with a salt.

Are Web Services used in your implementation? If so, what security controls have been implemented to secure them?

Stacks integrations often use web services and are limited in security by the service employed.

Describe the process for doing security-specific Quality Assurance testing for the application? (For example, testing of authentication, authorization and accounting functions, as well as any other activity designed to validate the security architecture.)

Stacks exercises strict quality control and inspection in every aspect of performance so that the end product conforms to the intent of the specifications. Stacks is regularly assessed by Stacks for compliance to these terms and policies. Stacks also has a structured software development lifecycle methodology. Stacks' testing includes functional, stress, load, security, negative and ad-hoc testing. The culmination of the testing cycle is the creation of the Software Release Order – a signed document signifying that testing is complete and all stakeholders approve of deployment.

Do you perform any vulnerability assessments of applications, for the explicit purposes of finding and remediating security vulnerabilities? (For example web code reviews including (CGI, Java), use of and tampering with hidden fields, Cookie or parameter poisoning or hijacking, URL parameter tampering; Variable checking within application code; Buffer overflows within application code; Cross site scripting; SQL Injection.)

Yes. Stacks performs exhaustive internal testing to ensure the security of our system and information. Testing is conducted prior to releasing software, as well as periodic penetration testing independent of software releases, not only on the layers of protection put in place, but across the data lifecycle. Stacks does not share test dates or results.

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 the PHP hash function numerous times to increase the computation cost of generating a password final hash (a security technique called stretching).

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:

- Every two hours 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 backup are taken every two hours and retained for serven (7) days, and daily which are retained for two (2) years.

Do you perform verification testing of backups? If yes, how often?

Yes, monthly where applicable. For customer facing applications we rely on multiple live data centers and site to site replication backup and redundancy. We also have many automated tools that monitor the performance of live sites and backups along with other scheduled tasks.

Where do you store backups? (Internally, 3rd Party, Both)

It is Stacks' policy that due to proprietary and confidential information as it relates to our resiliency and contingency strategies, we do not provide detail surrounding our strategies and capabilities.

Are backups encrypted?

Yes, the data that pertains to Stacks services is fully mirrored across our redundant data centers, so it is secure. Backups are encrypted using a strong industry standard cipher.

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 of their data and configurations.

How long after termination of the business agreement would you keep copies of user data?

No more than 30 days unless otherwise requested.

Who in your organization will have access to user data residing in backup media? How do you ensure that access to back-up media is appropriately secured?

Stacks considers backup data with the highest security procedures, with only senior personnel having access.

How is your environment designed to segregate users data from other customers' data?

Each customer is given a dedicated instance in our redundant cloud environment. Each customer therefore also has a dedicated database and file system.

How do you ensure that users data cannot be accessed by other customer?

Stacks instances are not connected.

Do you encrypt the data at rest or apply other technologies to ensure data confidentiality? If encryption is used, please provide details of the tool and algorithm used.

Data at rest is not encrypted, but is hosted in a secure environment and facilitates several options for content protection at a very granular level.

In what countries do you transfer, store, and backup users data?

Stacks instances can be hosted in Australia, Canada, Europe (Denmark, Germany), India, Singapore, United States, United Kingdom (Ireland and London).

At any point would users data be transmitted or stored outside of the originating country (i.e. US data stored in China/India, data is collected in the EU and stored and backed up in a US facility, etc.)?

No

How do you ensure security of data in transmission from user to and within your environment? Do you use any encryption standards? If yes, what encryption strength is used?

Stacks has developed and implemented several policies surrounding the protection of data. See our Security Whitepaper. Stacks uses SSL TLS 1.2/1.3 with 2048 bit encryption.

What is your data retention standard?

We have internal Data Categorization and Retention policies based on industry standards and best practices.

What processes and mechanisms have been implemented for secure disposal and removal of data (in the case of termination of contract, faulty hardware replacements, system

decommissioning, component upgrades, etc.) from all storage media? What audit trails are maintained and how is a user notified?

Stacks has mature termination procedures. Additional communications or logs may be requested in advance.

Describe your process for monitoring access to PII data and incident response to potential breach of the data.

Users of Stacks are not typically known to us as individuals. Stacks does not require the use of personal information in order for users to access or use Stacks. Institutions may choose an authentication method that could link to personal user information; however, neither of these is a requirement for using Stacks. Users may voluntarily submit customer-generated forms with personal information such personal information might include name, email address, telephone number, etc. Under no circumstances will Stacks sell this information, and we will only enable access to it with affiliates and third parties (e.g., contractors) involved in carrying out services and partner services, if they similarly safeguard this information, consistent with the Stacks Privacy Policy.

Do you have hardening guidelines (security configurations) for systems (virtual and physical)?

Yes

How are changes to the configuration managed? Do changes to host configurations go through security?

Stacks utilizes a mature change control methodology for all systems, applications, and devices. Security-related changes are reviewed and approved by Information 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?

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.

Are your systems current on security patches?

Yes.

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 Memcache, 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.

Do you regularly perform vulnerability assessment on your production environment? If yes, what is the frequency of vulnerability assessments?

Dedicated Platform Security Team

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.

Are logs generated for security relevant activities? If yes, how are these logs analyzed (near real-time vs. manual)

Yes, console near real-time.

Are all logs retained? Please explain how long are they retained for and what are the security controls around log integrity?

Logs are retained as required based on our internal data retention standards. Logs are secured by commercial logging device security controls.

Please explain the network security architecture of your hosting environment. Include details on placement of routers, firewall placement, network zoning, change review/management, firewall rule processes (creation/deletion/modification), and VLAN implementation from a security perspective.

Stacks production instances are run on a 99.9% uptime-guaranteed managed host (99.99% uptime available with Stacks Premium). Stacks monitors hardware and network connections for reliability purposes. 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 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.

Do you install firewalls to protect your production environment from external threats?

Yes.

How do you secure your firewall?

Firewalls are protected in accordance with our security policy for critical systems (secure access, role based access, network segmentation, etc).

What is the process for creation/deletion/modification of firewall rules?

Firewall rules follow our Change Management process. All rules are approved by dedicated Information Security personnel.

Is your hosting environment where user data resides (including all databases) separate from your corporate internal network?

Yes.

Do you have a network IDS, IPS implemented? Please provide details. Describe the process of monitoring IDS/IPS and support procedures.

Yes, console based, near real time. IPS updates are both scheduled and on demand with a review process prior to implementation.

Do you perform regular network vulnerability testing? If so, who performs the testing (internal or external party), when was the last scan performed?

Stacks performs vulnerability testing internally on an ongoing basis both automated and manual as per our information security policies.

List the physical security controls managing access to systems and networks housing or processing user data.

The data centers employed by Stacks are state of the art, utilize innovative architectural and engineering practices, and are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Do you have any non-company owned/managed systems or devices that connect to your network? If not, how do you monitor and detect that?

No.

Who, other than authorized IT personnel, has unescorted (physical) access to IT infrastructure? (For example, cleaners, managers, 'physical security' staff, contractors, consultants, vendors, etc.)

No one.

What kind of physical security mechanisms are in place to monitor access of these personnel?

Access and information is only granted to data centre employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked. All physical access to data centers by data center employees is logged and audited routinely.

What procedures or policies are in place to ensure that environmental issues do not cause an interruption to service? Prevention from fire, earthquake, flooding ,and failure of environmental control systems?

Fire Detection and Suppression

Automatic fire detection and suppression equipment is installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical

infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

Data centers monitor electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Is this service, application, etc. SSAE 16, ISO-27001, PCI DSS, Safe Harbor, etc. certified? If so please list these certifications, dates last certified, and provide supporting documentation or links.

Stacks does not hold any industry certification, but does use a combination of multi-industry security best practices from ISO, SANS, NIST, and CIS with its security policies and practices to protect customers and provide confidentiality, integrity, security, and availability of its services and data.

Do you have an Information Security Policy? If yes, when were these polices last updated? How do you ensure compliance to these policies?

Yes, Stacks has a documented Information Security program and policies that follow industry best practices and processes.

How do you ensure compliance to these policies?

All employees are governed by a comprehensive employment agreement, strong confidentiality clauses and mature human resources policies and procedures.

What security and privacy education programs are provided to anyone with access to user data?

Stacks is committed to continuing professional development with an emphasis on data privacy as a vendor specializing in information management verticals with new opportunities as technologies advance.