# SelfStir Data Center & Network Security

## PHYSICAL SECURITY

### Facilities

SelfStir service providers physical infrastructure is hosted and managed within Liquid Web's secure data centers and utilizes the Cloud Sites technology. Liquid Web continually manages risk and undergoes recurring assessments to ensure compliance according to the industry's standards. Liquid Web's data center operations have been accredited under:

- SOC 2 SSAE 16 Compliant and SOC 3
- PCI DDS Version 3.2.1
- HIPAA Compliant
- EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework

https://www.liquidweb.com/about-us/policies/certifications/

### On-site Security

SelfStir utilizes SSAE-16 Compliant data centers managed by Liquid Web. Liquid Web data centers are 24/7/365 Manned Facilities, with CCTV Security Cameras Covering Inside, Outside and All Entrances of Data Centers, Site Entrances Controlled By Electronic Perimeter Access Card System, Sites Remotely Monitored By 3rd Party Security Company, Entrances Secured by Mantraps with Interlocking Doors and are SSAE-16 & HIPAA Compliant, Safe Harbor Certified

https://www.liquidweb.com/about-us/data-centers/us-central/

### Location

SelfStir service providers data centers are located in Lansing, MI, United States.

## NETWORK SECURITY

### Protection

All firewalls infrastructure and management is provided by our service providers: sucuri.net and Liquid Web.

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to the ports and protocols required for a system's specific function in order to mitigate risk. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.



SelfStir Limited
Station House I Connaught Road I Brookwood I Woking I Surrey I GU24 OER I UK

### Vulnerability Scanning

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Our service provider utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

### Penetration Testing and Vulnerability Assessments

Third party security testing of our service provider is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team.

### Security Incident Event and Response

In the event of a security incident, our engineers are called in to gather extensive logs from critical host systems and analyze them to respond to the incident in the most appropriately way possible.

Gathering and analyzing log information is critical for troubleshooting and investigating issues. Our service provider allows us to analyze three main log types: system, application, and API logs.

### DDoS Mitigation

Our service providers infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

### Logical Access

Access to the SelfStir Production Network is restricted by an explicit need- to-know basis. It utilizes least privilege, is frequently audited, and is closely controlled by our Engineering Team. Employees accessing the SelfStir Production Network are required to use multiple factors of authentication.

## ENCRYPTION

### Encryption in Transit

Communications between you and SelfStir servers are encrypted via industry best-practices (HTTPS).

### Encryption at Rest

SelfStir supports encryption of customer data at rest.



SelfStir Limited
Station House I Connaught Road I Brookwood I Woking I Surrey I GU24 OER I UK

## AVAILABILITY & CONTINUITY

### Uptime
SelfStir availability has been 99.99% since 2013 and is continuously monitored.

### Redundancy
SelfStir service clustering and network redundancies eliminate single point of failure.

### Disaster Recovery
Our service provider's platform automatically restores customer applications and databases in the case of an outage. The provider's platform is designed to dynamically deploy applications within its cloud, monitor for failures, and recover failed platform components including customer applications and databases. We also maintain 3 months of application and database backups for each client on CodeGuard; in the event the client wishes to restore the data back to a specific date.

# Application Security

## SECURE DEVELOPMENT (SDLC)

### Framework Security Controls
We utilize framework security controls to limit exposure to OWASP Top 10 security flaws. These include inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.

### QA
Our QA department reviews and tests our code base. Application engineers on staff identify, test, and triage security vulnerabilities in code.

### Separate Environments
Testing and staging environments are separated from the production environment. No actual customer data is used in the development or test environments. Each customer has their own database with separate credentials hosted on dedicated database servers.

## APPLICATION VULNERABILITIES

### Static Code Analysis
Our source code repositories hosted on Assembla are continuously scanned for security issues via our integrated static analysis tooling.



SelfStir Limited
Station House I Connaught Road I Brookwood I Woking I Surrey I GU24 OER I UK

### Penetration Testing and Vulnerability Assessments

Third party security testing of our application is performed by independent and reputable security consulting firms on an annual basis or after a major update. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team. The SelfStir engineering and QA team use Qualys on an ongoing basis to carry out WAS vulnerability assessments for newly exposed vulnerabilities in the industry.

# Product Security Features

## SECURE DEVELOPMENT (SDLC)

### Authentication Options

SelfStir supports SAML SSO. Single sign-on (SSO) allows you to authenticate users in your own systems without requiring them to enter additional login credentials for SelfStir access.

### Secure Credential Storage

SelfStir follows secure credential storage best practices by never storing passwords in human readable format.

### API Security & Authentication

SelfStir API is SSL-only and you must be a verified user to make API requests. You can authorize against the API using API token.

## ADDITIONAL PRODUCT SECURITY FEATURES

### Access Privileges & Roles

Access to data within the SelfStir application is governed by access rights, and can be configured to define access privileges. SelfStir has various permission levels for organization (member and admin, member and moderator) and SelfStir users (user, coach).

### Transmission Security

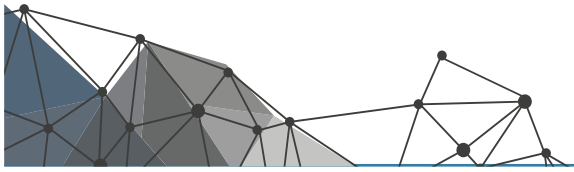
All communications with SelfStir service provider servers are encrypted using industry standard HTTPS. This ensures that all traffic between you and SelfStir is secure during transit.

# Additional Security Methodologies

## SECURITY AWARENESS

### Policies

SelfStir maintains a set of security policies covering a range of topics. These policies are shared with, and made available to all employees and contractors with access to SelfStir information assets.





SelfStir Limited
Station House I Connaught Road I Brookwood I Woking I Surrey I GU24 OER I UK

### Training

All new employees attend a Security Awareness Training, and the Engineering Team provides security awareness updates via e-mail, Slack posts, and in presentations during internal events.

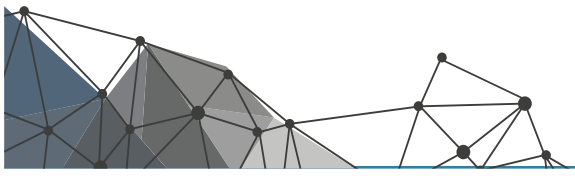
## EMPLOYEE VETTING

### Background Checks

SelfStir performs background checks on all new employees in accordance with local laws. The background check includes Criminal, Education, and Employment verification.

### Confidentiality Agreements

All new hires are screened through the internal hiring process and are required to sign Non-Disclosure and Confidentiality agreements.





SelfStir Limited
Station House I Connaught Road I Brookwood I Woking I Surrey I GU24 OER I UK