Salsa Labs Security

Salsa Labs, Inc. (“Salsa”) employs IT best practices for its information security strategy and has achieved PCI DSS 3.2 Level 1 annual certifications since 2013, which requires a third-party Qualified Security Assessor (QSA) to conduct an audit and certify.

Salsa’s IT security strategy is organized in the categories below:

- **Customer Privacy and Data Protection.**

    - Salsa values transparency and privacy. We make sure our customer data is protected. The following link explains our privacy policy. https://www.salsalabs.com/privacy-policy

    - Salsa labs follow EU consumer data protection regulations. https://help.salsalabs.com/hc/en-us/articles/360004772754-What-is-GDPR-

    We make sure we follow industry standards to protect customers’ data from unauthorized use or loss. For that reason, various controls are in place some of which include.

    - Offsite backups are being done and restored on a regular basis to validate.
    - Best practice secure drive destruction/data disposal methods are used via 3rd party services.
    - Only authorized agents with limited permission from specific locations are allowed to access customer data in order to support customer requests.
    - Best in class encryption and hashing algorithms are being used to encrypt all data and communication channels including password, SSL certificates, and sensitive data.
    - Specific data archival and retention policies are applied to ensure historical changes are recorded in case they are needed and data removal is done at service termination.

- **Operational Security.**
    - Industry best in class secure facilities are used for colocation and cloud services.
    - Salsa’s operation team along with third-party 24x7 SOC operations monitor Salsa’s production infrastructure to protect from cyber-attacks.
    - Salsa maintains both WAF, IDS to minimize attack vectors.
    - Regular scans and tests are being performed by internal ITSEC and third party SOC against both internal and external environments to identify and resolve any security weaknesses.
    - Only authorized employees can gain access to production services and data via 2-Factor, Role-based Access-Control, and only from a specific location via limited permission, and their activities are being logged.
    - All required inbound and outbound communication is being authenticated and/or encrypted.
    - Application-level audit trails are being maintained to review the use of administrative privilege(s).
    - Server build out uses hardening and protection mechanisms through templates and automation.
    - Antivirus, logging, and monitoring tools are deployed across all required resources.

- Authentication & Authorization mechanisms are in place for secure access control.

- **High Availability, Disaster Recovery & Risk Mitigation.**
  - Salsa maintains a highly available and auto-scaling environment to be able to sustain failures, performance demands, and security events.
  - Regular assessments are conducted to identify and remediate risks.
  - Local and offsite backups are maintained down to point in time increments.
  - Fraudulent credit card testing protection is being performed via Machine Learning.
  - Oncall pager schedule is being maintained to assure 24x7 availability.
  - Salsa has a formal incident response and recovery plan to deal with any service or security incident that may arise.
  - If a catastrophic event occurs Salsa is able to recover services to an alternative site with minimal downtime.

- **Application and Development Security**
  - Salsa uses best-practice SDLC and OWASP controls for application development.
  - Use of external 3rd party application pen-testing and vulnerability assessment on a regular basis.
  - Segregation of production and LAB environment is implemented at the network layer.
  - Production data is not allowed to be moved to any other network segment for testing or any other reason.

- **Internal and Office Security**
  - Office network protection controls include firewalls, VLANs, and wireless access point security.
  - Centralized access control is implemented on the bases of need to know and least privilege principle and no direct production access is allowed from any networks.
  - VPN is used to network all offices for cross-office secure communication and management.
  - Background checks are used for employees and contractors who require access to production services.
  - All physical access is being monitored by video and requires special location-based access control.
  - Salsa employees go through annual security awareness training to keep up to date on recent security issues and employees are notified of security threats that may arise like phishing attacks etc.