Spreedly Services

Shared Responsibility Matrix

This Spreedly Services Shared Responsibility Matrix defines the security, compliance, and operational responsibilities between Spreedly and its customers. This matrix is intended to provide transparency and to ensure both parties understand their respective obligations.

Category	Spreedly Responsibilities	Customer Responsibilities	Shared Responsibilities
Infrastructure Security	• Secure underlying cloud infrastructure (physical security, network) • Implement data center controls (access control, surveillance)	• Use trusted devices for accessing the Spreedly application • Keep client-side devices updated with security patches	• Monitor and manage network traffic for suspicious activities
Application Security	• Secure code development (code reviews, vulnerability scanning) • Patch and update the Spreedly cardholder data environment	• Manage user access to the Spreedly application (role management) • Configure application settings according to best practices working with PCI Qualified Security Assessor (if applicable) and other professional advisors	• Report vulnerabilities or incidents
Data Security	• Encrypt sensitive data at rest and in transit • Apply encryption at database and file levels for sensitive data • Conduct vulnerability scanning and penetration testing on a regular basis and address based on risk posture • Follow change management best practices and communicate service impacting changes to customers • Configure and manage backups and redundancy for data	• Ensure that all data entered into the Spreedly's application is complete, accurate, compliant and entered into the correct fields. • Control customer-side encryption keys (if applicable), do not to share access secrets through communications with Spreedly or anyone else • Promptly notify Spreedly if a vulnerability is identified in the Spreedly application • Reference Spreedly's changelog for awareness of change activity and communicate questions or concerns • Define backup retention periods based on business needs; utilize Personal Data Redaction process as needed	• Be a good data steward to protect cardholder data and minimize the risk of a security breach • Take action on security vulnerabilities in a timely manner
Identity & Access Management	• Provide multi-factor authentication (MFA) and Single Sign-on (SSO) options • Manage and log access to the Spreedly application	• Enforce strong password policies for user accounts • Regularly review user access permissions	• Configure MFA or SSO where available
Compliance & Audit	• Ensure compliance with regulatory, industry and framework requirements • Maintain and communicate updates to Spreedly's subprocessors list • Provide audit logging and reporting tools	• Comply with local regulations in data entry and usage; work with a Qualified Security Assessor for PCI guidance and engage professional advisors as needed • Review Spreedly's subprocessors list and communicate any concerns or questions • Report compliance needs to Spreedly	• Provide audit logs for joint investigations
Incident Management	• Detect and mitigate infrastructure security incidents • Maintain an incident response plan • Provide timely response and communication of incidents on Spreedly status page • Conduct post-incident reviews to prevent future occurrences	• Promptly notify Spreedly of any data incidents • Take action as requested by Spreedly during incidents • Reference Spreedly status page for ongoing incident communication and status • Provide incident feedback and lessons learned to Spreedly	• Respond to incidents in a collaborative manner
Data Retention & Deletion	• Provide tools for data lifecycle management (archival and deletion) • Delete customer data after service termination per contract	• Use Spreedly tools to maintain data lifecycle according to business requirements • Request deletion of unnecessary or outdated data (ex. cleanse vault of unnecessary data)	• Collaborate on retention exceptions and comply with deletion policy
Business Continuity	• Provide business continuity and disaster recovery for the Spreedly cardholder data environment • Ensure Spreedly cardholder data environment third parties meet or exceed Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) requirements	• Ensure business continuity on customer side (data exports, etc.) • Communicate business continuity requirement needs and changes	
User Training & Awareness	• Provide cardholder data environment usage guides and security best practices • Train staff on secure development and management of the Spreedly cardholder data environment	• Train staff on secure use of the Spreedly application including but not limited training on PII/PCI/local data entry and tool usage requirements • Reference Spreedly's documentation for proper application usage	• Awareness of new security threats and updates