SLOPE SECURITY POLICY

This Slope Security Policy (this "**Security Policy**") is incorporated into and made a part of the written agreement between Slope and Customer that references this document (the "**Agreement**") and any capitalized terms used, but not defined herein, shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this Security Policy, this Security Policy shall govern.

Slope utilizes infrastructure-as-a-service cloud providers as further described in the Agreement and/or Documentation (each, a "**Cloud Provider**") and provides the Service to Customer using a Virtual Private Cloud (VPC) and storage hosted by the applicable Cloud Provider (the "**Cloud Environment**"). Slope may review and update this Security Policy from time to time and will provide notice to Customer of such updates. The updated Security Policy will be made available at https://slopesoftware.com/legal/. Customer's continued use of the Service following the Version Date of the updated Security Policy shall signify your acceptance of the terms set forth in the updated Security Policy.

1. Encryption

1.1. Encryption of Customer Data. Slope stores all Customer Data at-rest using AES 256-bit (or better) encryption. Slope uses Transport Layer Security (TLS) 1.2 (or better) for all Customer Data in-transit between Users' browsers and the Service.

1.2. Encryption Key Management. Slope's encryption key management includes regular rotation of encryption keys. Slope logically separates encryption keys from Customer Data.

2. System & Network Security

2.1. Access Controls. All Slope personnel access to the Cloud Environment shall be via a unique user ID and consistent with the principle of least privilege. All such access requires a VPN, with multi-factor authentication and passwords meeting or exceeding industry best practice length and complexity requirements.

2.2. Separation of Environments. Slope logically separates production environments from development and testing environments. The Cloud Environment is both logically and physically separate from Slope's corporate offices and networks.

2.3. Firewalls / Security Groups. Slope shall protect the Cloud Environment using industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required.

2.4. Hardening. The Cloud Environment shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Policy.

2.5. Monitoring & Logging.

2.5.1. Infrastructure Logs. Monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least 90 days.

2.5.2. User Logs. Slope also captures logs of certain user-related activities and changes within the Account.

2.6. Vulnerability Detection & Management.

2.6.1. Anti-Virus & Vulnerability Detection. The Cloud Environment leverages advanced threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "**Malicious Code**"). Slope does not monitor Customer Data for Malicious Code.

2.6.2. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Service. Upon becoming aware of such vulnerabilities, Slope will use commercially reasonable efforts to address them as soon as practicable based on the potential impact to the Service.

3. Administrative Controls

3.1. Personnel Security. Slope requires criminal background screening of its personnel as part of its hiring process, to the extent permitted by applicable law.

3.2. Personnel Agreements. Slope personnel are required to sign confidentiality agreements. Slope personnel are also required to adhere to Slope's information security policy, which includes acknowledging responsibility for reporting security incidents involving Customer Data.

3.3. Personnel Access Reviews & Separation. Slope reviews the access privileges of its personnel to the Cloud Environment at least quarterly, and removes access on a timely basis for all separated personnel.

3.4. External Threat Intelligence Monitoring. Slope reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities that are relevant and rated as critical or high are prioritized for remediation in accordance with Section 2.6.2 (Vulnerability Management) of this Security Policy.

3.5. Change Management. Slope maintains a documented change management program for the Service.

4. Physical & Environmental Controls

4.1. Cloud Environment Data Centers. Slope requires each Cloud Provider to maintain appropriate physical and environmental controls for its data centers hosting the Cloud Environment and regularly reviews those controls as audited under the Cloud Provider's third-party audits and certifications. Each Cloud Provider is required to have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, shall include, but are not limited to, the following:

4.1.1. Physical access to the facilities are controlled at building ingress points;

4.1.2. Visitors are required to present ID and are signed in;

4.1.3. Physical access to servers is managed by access control devices;

4.1.4. Physical access privileges are reviewed regularly;

4.1.5. Facilities utilize monitor and alarm response procedures;

4.1.6. Use of CCTV;

4.1.7. Fire detection and protection systems;

4.1.8. Power back-up and redundancy systems; and

4.1.9. Climate control systems.

4.2. Slope Corporate Offices. Slope maintains technical, administrative, and physical controls for its corporate offices, which include, but are not limited to, the following:

4.2.1. Physical access to the corporate office is controlled at office ingress points;

4.2.2. Visitors are required to sign in;

4.2.3. Physical access privileges are reviewed regularly;

4.2.4. Fire detection and sprinkler systems; and

4.2.5. Climate control systems.

5. Incident Detection & Response

5.1. Security Incident Reporting. In the event Slope becomes aware of a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "**Security Incident**"), Slope shall notify Customer within 24 hours after becoming aware of such Security Incident via Customer's Account.

5.2. Investigation. In the event of a Security Incident as described above, Slope shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

5.3. Communication and Cooperation. Slope shall provide Customer timely information about the Security Incident to the extent known to Slope, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Slope to mitigate or contain the Security Incident, the status of Slope's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records affected by the Security Incident. Notwithstanding the foregoing, Customer acknowledges that Slope personnel does not have visibility into or familiarity with the content of Customer Data, it will be unlikely that Slope can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of Slope with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Slope of any fault or liability with respect to the Security Incident.

6. Deletion of Customer Data

6.1. By Customer. The Service provides Customer controls for the deletion of Customer Data, as further described in the Documentation.

6.2. By Slope. Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of the period within which Customer may exercise its Retrieval Right, as set forth in the Agreement, Slope shall promptly delete any remaining Customer Data.

7. Shared Security Responsibilities

7.1. Shared Security Responsibilities. Without diminishing Slope's commitments in this Security Policy, Customer agrees:

7.1.1. Slope has no obligation to assess the content of Customer Data to identify information subject to any specific legal, regulatory or other requirement and Customer is responsible for making appropriate use of the Service to ensure a level of security appropriate to the particular content of Customer Data;

7.1.2. to be responsible for managing and protecting its User credentials, including but not limited to (i) requiring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) reporting to Slope any suspicious activities in the Account or if any Users credential are compromised, and (iii) maintaining appropriate password uniqueness, length, complexity, and expiration;

7.1.3. to appropriately manage and protect any Customer-managed encryption keys to ensure the integrity, availability, and confidentiality of the key and Customer Data encrypted with such key.