Headset's Security Overview

Headset maintains a comprehensive security program designed to protect the confidentiality, integrity, availability, and security of the Headset applications and any customer data therein. An overview of the physical, administrative and technical safeguards underpinning the Headset's security program follows.

Application Security

Encryption of Customer Data. Headset encrypts Customer Data at-rest using AES 256-bit (or better) encryption. Headset leverages Transport Layer Security (TLS) 1.2 (or better) for Customer Data in-transit over untrusted networks.

Encryption Key Management. Headset's encryption key management conforms to NIST 800-53 and involves regular rotation of encryption keys. Headset logically separates encryption keys from Customer Data.

Security in our Application Development Lifecycle. Headset uses the git revision control system. Changes to Headset's code base go through a suite of automated tests and go through a round of manual review. When code changes pass the automated testing system, the changes are first pushed to a staging server wherein Headset employees are able to test changes before an eventual push to production servers and our customer base. We also add a specific security review for particularly sensitive changes and features. Headset engineers also have the ability to "cherry pick" critical updates and push them quickly to production servers.

In addition to a list where all access control changes are published, we have a suite of automated unit tests that check that access control rules are written correctly and enforced as expected. We also work with third-party security professionals to: (i)Test our code for common exploits and (ii) use network scanning tools against our production servers.

Threat Detection. Headset leverages advanced threat detection tools which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code ("Malicious Code"). Note that Headset does not monitor Customer Data for Malicious Code. In addition, Headset crowd-sources vulnerability assessment through an ongoing bug bounty program. An ongoing bounty Program is a cutting-edge approach to an application assessment or penetration test. Traditional penetration tests use only one or two personnel to test an entire scope of work, while an ongoing bounty leverages a crowd of security researchers. This increases the probability of discovering esoteric issues that automated testing cannot find and that traditional vulnerability assessments may miss in the same testing period.

Datacenter Security

Datacenters. Headset's applications are hosted with the world's leading data center providers. Access to these data centers is strictly controlled and monitored by security staff, tight access control, and video surveillance. Our data center partners are SOC 2 Type II and ISO 27001 certified and provide N+1 redundancy to all power, network, and HVAC services.

Headset Corporate Security Policies & Procedures

Security at the Headset Office. Our office is secured via keycard access. We monitor the availability of our office network and the devices on it. We collect logs produced by networking devices such as firewalls, DNS servers, DHCP servers, and routers in a central place. The network logs are retained for the security appliance (firewall), wireless access points, and switches.

Employee Training. Headset maintains a documented security awareness and training program for its personnel, including, but not limited to, onboarding and on-going training.

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

Employee Workstations and Laptops. All laptops and workstations are secured via full disk encryption. We diligently apply updates to employee machines and monitor employee workstations for malware.

Vendor Risk Management. Headset maintains a vendor risk management program for vendors that process Customer Data designed to ensure each vendor maintains security measures consistent with Headset's security policies.

Incident Detection & Response

Security Incident Reporting. If Headset becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "Security Incident"), Headset shall notify Customer without undue delay, and in any case, where feasible, notify Customer within 72 hours after becoming aware.

Investigation. In the event of a Security Incident as described above, Headset 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.

Communication and Cooperation. Headset shall provide Customer timely information about the Security Incident to the extent known to Headset, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Headset to mitigate or contain the Security Incident, the status of Headset's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Headset's communications with Customer in connection with a Security Incident, shall not be construed as an acknowledgment by Headset of any fault or liability with respect to the Security Incident.