Security Statement

This Security Statement applies to the products, services, websites and apps offered by Quantum Leap Inc. We refer to those products, services, websites and apps collectively as the “services” in this Statement. This Security Statement also forms part of the user agreements for Quantum Leap customers.

Quantum Leap values the trust that our customers place in us by letting us act as custodians of their data. We take our responsibility to protect and secure your information seriously and strive for complete transparency around our security practices detailed below. Our Privacy Policy also further details the ways we handle your data.

Physical Security

Quantum Leap’s information systems and technical infrastructure are hosted within world-class, SOC 2 accredited data centers. Physical security controls at our data centers include 24x7 monitoring, cameras, visitor logs, entry requirements, and dedicated cages for Quantum Leap hardware.

Compliance

Quantum Leap is compliant with the Payment Card Industry’s Data Security Standards (PCI DSS 3.2) and can therefore accept or process credit card information securely in accordance with these standards. Quantum Leap re-certifies this compliance annually.

Access Control

Access to Quantum Leap’s technology resources is only permitted through secure connectivity (e.g., VPN, SSH) and requires multi-factor authentication. Our production password policy requires complexity, expiration, and lockout and disallows reuse. Quantum Leap grants access on a need to know on the basis of least privilege rules, reviews permissions quarterly, and enables customers to revoke access immediately after employee termination.

Security Policies

Quantum Leap maintains and regularly reviews and updates its information security policies, at least on an annual basis. Employees must acknowledge policies on an annual basis and undergo additional training such as HIPAA training, Secure Coding, PCI, and job specific security and skills development and/or privacy law training for key job functions. The training schedule is designed to adhere to all specifications and regulations applicable to Quantum Leap.

Personnel

Quantum Leap conducts background screening at the time of hire (to the extent permitted or facilitated by applicable laws and countries). In addition, Quantum Leap communicates its information security policies to all personnel (who must acknowledge this) and requires new employees to sign non-disclosure agreements, and provides ongoing privacy and security training.

Dedicated Security Personnel

Quantum Leap also has a dedicated Trust & Security organization, which focuses on application, network, and system security. This team is also responsible for security compliance, education, and incident response.

Vulnerability Management and Penetration Tests

Quantum Leap maintains a documented vulnerability management program which includes periodic scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications. All networks, including test and production environments, are regularly scanned using trusted third party vendors. Critical patches are applied to servers on a priority basis and as appropriate for all other patches.

We also conduct regular internal and external penetration tests and remediate according to severity for any results found.

Encryption

We encrypt your data in transit using secure TLS cryptographic protocols. Quantum Leap data is also encrypted at rest.

Development

Our development team employs secure coding techniques and best practices. Developers are formally trained in secure web application development practices upon hire and annually.

Development, testing, and production environments are separated. All changes are peer reviewed and logged for performance and audit purposes prior to deployment into the production environment.

Asset Management

Quantum Leap maintains an asset management policy which includes identification, classification, retention, and disposal of information and assets. Company-issued devices are equipped with full hard disk encryption and up-to-date antivirus software. Only company-issued devices are permitted to access corporate and production networks.

Information Security Incident Management

Quantum Leap maintains security incident response policies and procedures covering the initial response, investigation, customer notification (no less than as required by applicable law), public communication, and remediation. These policies are reviewed regularly and tested bi-annually.

Breach Notification

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Quantum Leap learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under applicable country level, state and federal laws and

regulations, as well as any industry rules or standards applicable to us. We are committed to keeping our customers fully informed of any matters relevant to the security of their account and to providing customers all information necessary for them to meet their own regulatory reporting obligations.

Information Security Aspects of Business Continuity Management

Quantum Leap's databases are backed up on a rotating basis of full and incremental backups and verified regularly. Backups are encrypted and stored within the production environment to preserve their confidentiality and integrity and are tested regularly to ensure availability.

Your Responsibilities

Keeping your data secure also requires that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems.

Logging and Monitoring

Application and infrastructure systems log information to a centrally managed log repository for troubleshooting, security reviews, and analysis by authorized Quantum Leap personnel. Logs are preserved in accordance with regulatory requirements. We will provide customers with reasonable assistance and access to logs in the event of a security incident impacting their account.