SilkRoad Technology Security

KEEPING CLIENT DATA SAFE

Security is the foundation of our organization. SilkRoad Technology solutions have been built to keep your data safe. The SilkRoad Executive Leadership and Board of Directors are committed to preserving the confidentiality, integrity, and availability of client data.

SECURITY GOVERNANCE, RISK AND COMPLIANCE

SilkRoad uses CIS TOP 20, NIST and the ISO 27000 family of information security standards as the framework of our security practice. These policies and practices are evaluated semi-annually thru internal review and annually by an independent SOC 2 audit.

INFRASTRUCTURE SECURITY

SilkRoad provides best-in-class protection through its hardware, software, and operations management. The infrastructure layer is designed in a defense and depth approach to provide the highest levels of system confidentiality, integrity, and availability.

SYSTEM MONITORING

SilkRoad's IT Infrastructure is subject to annual penetration testing and scanned monthly for vulnerabilities using industry leading technology. A portfolio of tools are used to alert responsible groups of component failures and thresholds indicating problems.

SYSTEM REDUNDANCY

SilkRoad strives to eliminate any single point of failure by maintaining a highly available and secure environment that is ready for immediate failover. This is done through process flow among multiple devices and multiple service providers. This function is tested annually through our SOC 2 audit.

SilkRoad TECHNOLOGY

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) is encrypted throughout SilkRoad's applications and infrastructure. Data commonly accepted as sensitive and needing encryption would be social security numbers, driver's license numbers, and bank account numbers, as well as other fields determined by the client.

ORGANIZATIONAL SECURITY

All SilkRoad employees are required to complete security, privacy, and compliance training during their onboarding experience and on an annual basis. We believe that information security is every employee's responsibility in their day-to-day operations.

GENERAL DATA PROTECTION REGULATION (GDPR)

SilkRoad is a processor of foreign data and maintains all GDPR related standards and requirements for its clients. SilkRoad Technology also meets the requirements defined by the Swiss-US Privacy Shield Framework and the EU-U.S. Privacy Shield Framework. These requirements are examined yearly.

OPERATIONAL SECURITY

SilkRoad leverages industry leading anti-malware solutions to ensure that any malicious behavior that attempts to penetrate the firewall, IPS, and DMZ is caught at the server level and eradicated. SilkRoad leverages security solutions to continuously monitor the performance and safety of its solutions and network to mitigate risks and prevent system delays or outages. If an incident does take place, our Incident Response Plan includes the following key steps:

1. **Preparation** – Ensure steps have been taken to minimize the risk of any incident occurring through software and hardware tools and systems/ component monitoring
2. **Identification** – Determine if the incident is actual or if systems are presenting a false positive
3. **Investigation** – Examine the origin and the validity of the incident
4. **Containment** – Isolate the affected system(s) to limit the risk of the incident spreading
5. **Eradication** – Take the required steps to remove the threat
6. **Recovery** – Restore all affected systems to full availability
7. **Lessons Learned** – Document the incident, the causes, and steps used to resolve the problem. Identify improvement activity to ensure the incident is not repeated.

We also include Notification – Communicate the discovery of an incident to the appropriate response team, executive leadership, and any affected clients. Continue periodic notifications until the incident is eradicated.

SILKROAD CLIENTS CAN REMAIN CONFIDENT THEIR DATA IS PROTECTED, AND THE USABILITY AND AVAILABILITY OF THE DATA ARE PRESERVED.