Overview: Security & Confidentiality

Vanco Payment Solutions operates with an unwavering commitment to security and confidentiality and incorporates risk management into every facet of its business. This commitment is demonstrated by the following audits and actions.

SOC 1℠ Type 1 Audit

The Service Organization Control (SOC) 1℠ Type 1 Audit Report is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1℠ Type 1 audit describes the extensive controls Vanco has put into place for processing transactions and confirms the company's suitability for achieving its stated objectives.

Payment Card Industry (PCI) Data Security Audit

Vanco is a PCI Level 1 Compliant Service Provider. The security requirements in the audit pertain to all system and network components, which include, but are not limited to: servers, firewalls, applications, routers, encryption, privilege management, stored data and tracking system access. As part of this PCI Level 1 audit, Vanco is required to participate in both quarterly security scans and a yearly external penetration test of its network and systems. The security scans and penetration tests are conducted by an independent assessor that focuses on probing Vanco's systems.

System Redundancy: Application and File Replication

All applications are web based and designed for easy replication. All system activity is mirrored in real time and critical files are replicated throughout the day between two locations—a Tier III data center in Eden Prairie, Minnesota and a Tier III co-location in Atlanta, Georgia.

Disaster Recovery

Once a month, to test systems and to verify business interruption and disaster recovery readiness, all essential business functions are performed from the St. Paul facility.

Systems Security

Vanco maintains an Information Security Policy and a Computer Security Incident Response Plan. Both plans are reviewed quarterly and updated as needed.

Data Encryption

All confidential data transmitted by Vanco over any public communications network is encrypted by strong cryptography and encryption techniques (256-bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), and Internet Protocol Security (IPSEC) to safeguard data during transmission. All confidential data transported in readable storage media is also encrypted using AES-256.

Overview: Security & Confidentiality

Risk Management / Mitigation / Assessment

Risk management and risk assessment are critical functions. Vanco has tools in place to consistently assess risk concerns. Weekly risk management meetings are held to address current risk issues. As needed, meetings are held to analyze threats and vulnerability to systems with appropriate countermeasures implemented. An annual Risk Assessment meeting is held to discuss the company's Risk Management Plan for the upcoming year, resulting in the formal plan designed to address key risk management points. The Compliance and Risk Management Department along with members of the senior management team participate in all risk management discussions.

Employee Security Requirements

Vanco performs background checks on all new employees. All employees are required to receive and sign on the first date of employment, a Confidentiality and Non-Disclosure Agreement and, an Employee Information Security Policy Summary and corresponding Agreement to Comply with Information Security Policies document.

Additionally, all employees are required to attend quarterly compliance meetings that include a review of the Employee Information Security Policy and Confidentiality and Non-Disclosure Agreement.