Vurke Inc.

Technology, Finance, People.

SECURITY MEASURES

This document makes an attempt to explain the security measures taken by Vurke and its partners for protecting and safeguarding Vurke's customers and their data.

Please note that Vurke's Customers are responsible for complying with local, state, national, and foreign laws, including those related to data privacy and transmission of personal data, even when a service provider holds their data. Vurke maintains a formal and comprehensive security program designed to ensure the security and integrity of customer data, protect against security threats or data breaches, and prevent unauthorized access to the data of its customers.

501 Silverside Road, Suite 105, #3243, Wilmington, DE 19809, USA

Physical & Operational Security

Vurke's dedicated servers are hosted with SoftLayer® - an IBM company. SoftLayer has developed and uses SecurityLayer®, a unique approach to security that provides multiple, overlapping tiers of protection for the SoftLayer infrastructure. SecurityLayer surrounds Vurke's environment with layer upon layer of defenses—both hardware- and software-based—to avoid, repel, or withstand any threat. Through SoftLayer's best-in-class operational procedures and partnerships with industry-leading security technology providers, SecurityLayer portfolio of security provisions and options that maximize Vurke's uptime, protect private information, and significantly mitigate business risk.

Overlapping Layers of Protection SecurityLayer monitors every facet of the infrastructure and operations. Unique, Highly-Secure Network Design, SoftLayer's revolutionary Network-Within-a-Network topology provides true out-of-band management for full remote access with no exposure to external threats.

Every SoftLayer data center is fully audited based on SSAE 16 reporting on controls to meet industry-recognized requirements for security—no exceptions.

Data Center and Server Room Measures

- Data centers located only in facilities with controlled access and 24-hour security
- No server room doors are public-facing
- Server rooms are staffed 24/7
- Un-marked entry and exit doors
- Digital security video surveillance
- Biometric security systems
- Server room access strictly limited to SoftLayer employees and escorted contractors or visitors
- Barcode-only identification on hardware; no customer markings of any type on the servers themselves

Operational Measures

- Engineers and technicians trained on internal industry standard policies and procedures and audited yearly
- Geographic redundancy for all core systems for disaster recovery and business continuity
- 2-factor authentication for Customer Portal access adds greater server security
- All data removed from re-provisioned machines with drive wipe software approved by the Department of Defense
- Ongoing PCI DSS compliance; currently undergoing Level 1 Audit
- Current SSAE 16 SOC1 report, with no exceptions noted

Network Security

SoftLayer's innovative network architecture and commitment to using the most advanced hardware technologies dramatically minimizes the data centers' and server exposure to outside threats. The network integrates three distinct and redundant network architectures into the industry's first Network-Within-a-Network topology. Systems are fully accessible to your administrative personnel but safely off-limits to others.

The SoftLayer Network-Within-a-Network

- Public Network handles public traffic to hosted websites or online resources
- Private Network allows for true out-of-band management through a distinct stand-alone third carrier over SSL, PPTP, or IPSEC VPN gateways
- Data Center to Data Center Network provides free, secure connectivity between servers housed in separate SoftLayer facilities

System, Application & Data Security

- Latest operating system security patches and upgrades
- McAfee® Virus Scan and Host Intrusion Servers. These systems combine anti-virus, anti-spyware, firewall, and intrusion prevention technologies to stop and remove malicious software.
- McAfee Windows VirusScan Anti-Virus delivers always-on, realtime anti-virus protection for Windows environments to monitor for potential attacks.
- McAfee Host Intrusion Protection with Reporting Full white-listing and black-listing monitoring of applications.
- Dedicated Hardware Firewalls for the highest assurance of uptime.

Encryption of Data in Transit

Users access Vurke via the Internet protected by Secure Socket Layer version 3 (SSL v3) or Transport Layer Security (TLS). This secures network traffic from passive eavesdropping, active tampering, or forgery of messages. Vurke has also implemented proactive security procedures such as perimeter defense and network intrusion prevention systems. Vulnerability assessments and penetration testing of the Vurke network infrastructure are also evaluated and conducted on a regular basis.

Data Backups

Vurke's master production database is replicated in real-time to a slave database maintained at an offsite data center. A full backup is taken from this slave database each day and stored at the offsite data center facility. Vurke's database backup policy requires database backups and transaction logs to be implemented so that a database may be recovered with the loss of as few committed transactions as is commercially practicable. Transaction logs are retained until there are two backups of the data after the last entry in the transaction log. Database backups of systems that implement interfaces must be available as long as necessary to support the interfacing systems. This period will vary by system. Backups of the database and transaction logs are encrypted for any database which contains customer data.

Database Security

Vurke encrypts sensitive attributes of customer data within the application before it is stored in the database. This is a fundamental design characteristic of the Vurke technology. Vurke relies on the Advanced Encryption Standard (AES) algorithm with a key size of 128-bits.