TRxLink® Security

Security is a principal design element of TRxLink® and is embedded in all aspects of the system's implementation and its usage.

Agent Security

The TRxLink agent communicates with our servers using 256-bit SSL encryption providing an extra layer of protection for our users. This protection helps to defend against data theft during data communication between client sessions and the TRxLink servers. The agent does not require any ports to be opened on the customers' systems, because all communications take place using HTTPS.

As an added level of security, we additionally ask for the company ID besides the user name and password for login access authentication.

Physical Security

- **Data Centers:** Our information systems infrastructure (servers, networking equipment, etc.) is collocated at leading, top-tier hosting provider's data center. The data center is SSAE 16, CSAE 3416, and ISAE 3402 compliant for Managed Hosting and Colocation. We own and manage all of our equipment located at these data centers.
- **Data Center Security:** Our data centers are staffed and surveilled 24/7. Access is secured by security guards, visitors' logs, and entry requirements such as pass-cards and biometric recognition. Our equipment is kept in locked cages. External and internal CCTV tied back to DVR systems, video records are retained for 90 days. A proximity access control system is in place utilizing access card and biometric authentication. Intruder and door tampering alarms are in place and there is a secure managed loading dock.
- **Environmental Controls:** Our data center is maintained at controlled temperatures and humidity ranges which are continuously monitored for variations. Very Early Smoke Detection Apparatus (VESDA) provides the earliest possible warning of a potential fire event by detecting smoke at the incipient stage of fire. Photoelectric, ionization and heat detection sensors are also employed. INERGEN - a fire suppression clean-agent gas system and clean agent fire extinguishers are deployed throughout the facility.
- **Location:** All user data is stored on servers located in the United States.

Availability

- **Connectivity:** Fully redundant IP network connections with multiple independent connections to a range of Tier 1 Internet access providers.
- **Power:** Servers have redundant internal and external power supplies. Data center has backup power supplies, and is able to draw power from the multiple substations on the grid, several diesel generators, and backup batteries.
- **UPS:** Capacity, 6 x 500kVA UPSs (N+1)
- **Generator:** 3 x 1.5 MW generators (N+1) with two 12,000 gallon fuel tanks, 5 days before refueling.
- **Uptime:** Continuous uptime monitoring, with immediate escalation to our staff for any downtime.

- **Failover:** Our database is log-shipped to standby servers and can failover in less than an hour.

Network Security

- **Uptime:** Continuous uptime monitoring, with immediate escalation to our staff for any downtime.
- **Testing:** System functionality and design changes are verified in an isolated test "sandbox" environment and subject to functional and security testing prior to deployment to active production systems.
- **Firewall:** Firewall restricts access to all ports except 80 (http) and 443 (https).
- **Patching:** Latest security patches are applied to all operating system and application files to mitigate newly discovered vulnerabilities.
- **Access Control:** Secure VPN, multifactor authentication, and role-based access is enforced for systems management by authorized engineering staff.
- **Logging and Auditing:** Central logging systems capture and archive all internal systems access including any failed authentication attempts.

Storage Security

- **Backup Frequency:** Database backups are continuous done hourly internally, then daily to a centralized backup system for storage in multiple geographically dispersed sites.
- **Production Redundancy:** Data is stored on a RAID 10 array. O/S is stored on a RAID 1 array.

Organizational & Administrative Security

- **Employee Screening:** We perform background screening on all employees.
- **Training:** We provide security and technology use training for employees.
- **Service Providers:** We screen our service providers and bind them under contract to appropriate confidentiality obligations if they deal with any user data.
- **Access:** Access controls to sensitive data in our databases, systems and environments are set on a need-to-know / least privilege necessary basis.
- **Audit Logging:** We maintain and monitor audit logs on our services and systems (our logging systems generate gigabytes of log files each day).
- **Information Security Policies:** We maintain internal information security policies, including incident response plans, and regularly review and update them.

Software Development Practices

- **Stack:** The primary platform for TRxLink is Microsoft .NET, SQL Server and Windows Server.
- **Coding Practices:** Our engineers use best practices and industry-standard secure coding guidelines to ensure a secure, sustainable and expandable product.