



## Re:source® Visibility Data and System Security Statement

Infrastructure and security standards for Re:source Visibility meet the rigorous technical and operational requirements of IT/IS departments at the world's largest telecom organizations. The extensible, software-as-a-service (SaaS) platform is protected by the most advanced technology for Internet security available today.

### User Access/Data Vaulting

Access to the Re:source Visibility application is via industry standard Secure Socket Layer (SSL) technology. Client information is protected using both server authentication and data encryption, ensuring that data is safe, secure and available only to registered users in your organization. The platform encrypts all data at rest either via database encryption or database access encryption keys with a minimum of a 256-bit encryption.

Users are granted unique login credentials (user name and password) for a given company, and assigned to a specific data vault. Data vault access is controlled at the database and application level to guarantee security of customers' proprietary information. This segregation allows users across global corporations and partners within a service chain to collaborate and manage inventory while ensuring complete data confidentiality.

Assigned privileges based on user role control what a user can see and what a user can do within the application by combining the operations that a user can perform (functional role) with the data that they are allowed to view within their data vault (Visibility role). The system administrator within the organization defines and assigns these roles and privileges based on client preference.

### Operating Environment, Data Security and Disaster Recovery

Re:source Visibility is hosted in a secure server environment that uses firewalls and other advanced detection technologies to prevent malicious intrusion attempts. Monitored at all times, the platform is protected by Cisco ASA security devices which control and inspect all inbound and outbound packets through this firewall system. All files uploaded are pre-staged on a separate server and scanned for viruses before being moved to the Re:source Visibility platform. This protects the server systems from files forwarded from an infected PC or server.

A redundant, enterprise-grade Windows environment extends to Trade Wings' core database and application layers. Core databases are mirrored onsite, with logs shipped offsite for disaster recovery purposes. All Trade Wings server facilities have physical access restrictions in place to avoid non authorized personnel from accessing the platform at the server level, and at all server-level network interface points. The platform hardware minimizes single points of failure where feasible by utilizing hardware redundancy technology (N+1 power supplies, RAID 10 or higher, Multiple Network Interfaces, redundant mirrored memory).

## **Trade Wings' U.S. Co-Location Facility**

Trade Wings' servers are housed at a co-location facility, which operates under specifications that meet or exceed strict Bellcore and industry standards, such as:

- Redundant climate control
- Inergen fire suppression and air evacuation fire suppression
- Multiple entrances for diverse fiber optic connectivity
- Separate pathways for interconnectivity to upstream carriers
- Security system and video monitoring
- 24x7 monitoring of all connections through separate NOCs
- 24x7 secure swipe card access
- Dual bus uninterruptible power supply
- Back-up generator onsite for prolonged outages

In the event of hardware failure or facility loss, the platform is recoverable to normal operating standards per the timeframes documented in Trade Wings' standard Service Level Agreement (SLA).

*Product and network specifications subject to change without notice.*

*Rev.1.0 -Published October 15, 2010*