



## **Edge Technology – Network & Security**

Several layers of protection to ensure that your data is secure. These begin with a network built on industry standard hardware with Cisco equipment, and continue with physical security, a dedicated, highly trained security staff, vulnerability assessment systems, multiple firewalls, and dedicated intrusion prevention systems. Additionally, we have an ISO 9001/SAS 70 certified data center.

## **Network Accessibility and Redundancy**

Our web repositories have 99.98% uptime, because our systems running in a facility using dual backup generators, with dual redundant battery backups, three main backbone internet carriers providing up to 100 megabyte (67 T1's) of internet backbone connectivity.

## **Privacy & Security Policies**

We take security and confidentiality very seriously and have many procedures in place to ensure the highest level of compliance. In short, security starts with people. When we first hire an employee we train them on the sensitive nature of the work that we do. Additionally, every employee must sign a confidentiality agreement before working on any new project. We also make every attempt not to use temporary employees. Further, employees also undergo a thorough interview process, background check and drug screening prior to hiring. Our facilities are designed with security in mind as well. Our freestanding locations are alarmed and monitored 24/7. CCTV in use 24 hours. All production is monitored by our bespoke workflow software that tracks every box in process. This software informs us of where each box is in the production process, as well as tracks everyone who has performed services on it. Additionally, we have special box safe rooms where all work must be stored and returned when not being processed.

## Network Security/Connectivity

- Critical Systems are housed in a secure data center facility.
- Internet connectivity to critical systems is accomplished via two active and one standby connection via major carriers, BGP routing, and constant monitoring of performance metrics.
- We have a continually updated Security Policies and Procedures Manual.
- A multi-interface firewall is utilized to restrict traffic to allowed ports. The fire wall employs an External 'DMZ' subnet to isolate and divert incoming Internet traffic. Repository data resides on an internal subnet protected by router access control and stateful inspection firewall.
- Firewall/Intrusion Prevention is handled by Cisco ASA 5520 Adaptive Security Appliance and Trend Micro regularly updated IPS signatures.
- Firewall configuration/logging is audited daily to ensure sound configuration and respond to prohibited activity.
- The Repository website utilizes data encryption via 128-bit SSL certificate to keep transferred information confidential.
- The repository website utilizes additional freestanding security applications to enforce logon security, with another layer also being utilized at the database level.
- Centrally managed anti-virus suite is utilized to prevent virus infections.
- Change Control procedures are in place to protect environment from unplanned or untested changes.
- Patch management is regularly scheduled and managed via centralized audit and deployment system.
- Vulnerability management is accomplished with vendor-recommended tools on a periodic basis to ensure compliance with security policy.

## System Administration/Programmer Access Control

- Access is controlled via Active Directory Authentication as well as Application Specific Authentication.



In Partnership  
with

