Security Overview

In order to provide industry leading design, architecture and operational processes, Vision has employed a three layer security strategy, including:

- CoreSite Data Center
- Network Architecture
- Software Design

CoreSite Data Center

CoreSite operates 16 data centers across the United States creating 2.7 million feet of data center space serving over 800 customers. All of the centers feature extensive physical security as well as redundant power and cooling systems. (SSAE 16 audit reports available upon request.)

Vision has partnered with CoreSite to provide a hosting environment with comprehensive security protocol, including:

- Staffing by in-house security officers 24/7/365
- Security personnel undergoes annual training and certification
- Perimeter fencing
- Interior and perimeter IP-DVR cameras
- Mantrap or double mantrap entries
- Biometric and keycard scanners
- Option for above and below enclosed floor caging
- PCI DSS, SOC 1 Type 2 and SOC 2 Type 2 validation
- N, N+1, and 2N UPS systems. N+1 generators

Network Architecture

- Fully Redundant Datacenter Architecture
- Redundant Cogent & Level3 internet connections with automated BGP Failover
- Redundant HA routers at primary and DR datacenters
- Redundant HA firewalls at the Primary and DR datacenters
- Redundant Storage Area Network (SAN) Storage
- Redundant HA Virtualized Server infrastructure
- Redundant Core Switching
- Disaster Recovery data center located in Dallas for geographic separation
- DDOS protection provided by Black Lotus, who is owned by Level 3 and is one of the top DDOS protection providers available.
- Daily backups retained on a two week rolling basis
- Working with security and networking specialists for DR and additional security consultation

- **Directory Browsing Hack:** We use ASP.NET MVC to hide our website file/folder structure and prevent directory browsing.
- **Cross-Site Scripting Attack (XSS):** We encode query string values and database values when they are displayed on the UI.
- **Input Validation Attack:** When forms are submitted to the backend, the system checks all inputs to prevent inserting HTML to non-HTML database columns.
- **SQL Query Injection Attack:** We use Entity Framework to query data from database and insert data to database; there is no logic to build SQL script with concatenated SQL text parameter, which prevents SQL injection attacks.
- **Cross-Site Request Forgery (CSRF) Attack:** For all forms which post values to the database, we add anti-foreign tokens (based on timestamp and the form) to prevent the attack.
- **Testing:** Each code update is scanned by Qualys to look for any vulnerabilities.
- Each site on the server has its own database, site location folder, application pool and site instance. Each database can only accept connections from its associated site.
- To maintain a small profile, the only additional software on the server is McAfee VirusScan Enterprise and, if the Convert to PDF function is desired, Microsoft Office.
- No open source software is used.
- All credentials are encrypted in the database.