WHITE PAPER

SECURITY INFRASTRUCTURE AND POLICIES

AT

Vision i-knowledge

Security, for Vision, is foundational to its operations dealing as it deals with sensitive business segments such as Healthcare. Vision has implemented multi-tiered security measures that comply with all international regulatory requirements to give each client peace of mind. Vision is covered by the HITECH Act and complies with HIPAA requirements. With Vision your data is safe, secure and in accordance with mandatory guidelines concerning security and privacy.

Details of our security measures are given below.

Physical Security

Vision's full suite of physical security measures reassure even the most critical and sensitive client.

- Vision carries out operations in a modern commercial complex manned round the clock by professional security staff.
- Each employee is recruited only after a thorough background check. Even during employment, checks are discreetly carried out on his movements and lifestyles.
- The reception area is the only part open to public. Access to areas beyond, is only by proximity cards issued by our security wing.
- Each square foot of the facility is under security video surveillance linked to central DVR monitor. Security staff constantly monitors all video units at a centralized console.
- Staff members are not permitted to carry any personal items to their work areas and must leave all such belongings including mobiles at the staff check in counter.
- Biometric Access Control limits entry to the interior parts to only authorized personnel. The system records, logs and monitors movement and such records are accessible to security staff / senior management for review.
- The in-house server facility is a highly restricted area and entry is permitted to only a select few using biometric access control.
- A security officer patrols each floor and is authorized to carry out surprise random searches of any employee at any time.
- Data is stored in central, highly secure servers located in strong rooms. Staff workstations do not have any removable storage devices. USB ports are disabled to prevent the possibility of attempts at recording data.

Multi-Tiered Data Security

If physical implementation is the most stringent, software and hardware firewall data security implementation is no less so. Vision has in place the latest and updated multi-tiered data security measures to guarantee total safety. These measures are:

- Secure, authorized access to select personnel through implementation of Active Directory and Domain Controllers on our servers. Implementation includes specific rights assignment to each user, throttling in case of unsuccessful login attempts as well as session timeouts.
- Deployment of hardware and software integrity monitoring network firewalls and application firewalls.
- Secure Socket Layer implementation on our intranet portal with SSL certificate from Symantec to ensure highest levels of encryption.
- Symantec Endpoint protection solution has been implemented to take care of Virus and Malware threats. Symantec Endpoint not only takes care of virus threats, it also provides our data with layered protection at the endpoint. It also takes care of intrusion detection and prevention
- Web protection software limits access to only permitted sites and blocks attempts at intrusions, tunneling, malware, phishing and spying as well as hacking. Constant software updates are a part of the process to keep systems fully protected at all times. An updated internet security architecture is always up and running at all times.
- Audit of user activities are an ongoing process through monitoring of system and server logs.
- All systems are partitioned and assigned security classifications according to nature of job and designation of personnel.
- Vulnerability assessments are an ongoing process to prevent latest hacking and intrusion attempts from gaining entry and tunneling through.
- All measures comply with international regulatory requirements in this regard with documentation for each step in each section and department.
- Separate team of security specialists monitor hardware, software, networks and configurations following a documented process.

Remote Access and Work Security

Authorized Vision staff members are provided passwords to log into a client's network through a secured VPN/remote desktop access method. The double authentication process in which an employee must first log into our server and then log into a client's server assures security and then only can the member access and work on data residing on a client's server. Once the agent logs out of the system, he cannot access the data.

Security Policies

- Vision is sensitive to security and safety of data of each client and has in place the strictest and toughest policies to ensure security. All measures we follow are documented and each staff member must read, understand and sign an agreement before he begins work. Breach of any of the laid down policies can lead to strict sanctions and/or disciplinary action.

- Each staff member undergoes training on HIPAA and understands the importance of data security. In addition there are regular refresher courses to keep each staff member updated.

- Employees, vendors and associates are all governed by HIPAA and a well-defined NDA and confidentiality agreement.

- Reports are prepared by key personnel and transmitted in encrypted, non-editable formats.

- From time to time we have security specialist review our systems and recommend latest implementations to keep our entire security updated in accordance with latest developments.