Ensuring the Privacy and Security of Our Clients' Data

Policy Statement

Leader Services believes the security of our web applications and the privacy of our client data are core components of the products and services we offer. In full compliance with all HIPAA/FERPA requirements, we have implemented numerous measures to protect our clients' information:

Network and data security

Firewalls

- Leader uses redundant hardware firewall devices as a gateway to control all incoming and outgoing traffic between Leader's internal network and the Internet. Packet filtering and port monitoring allow only certain protocols (HTTP, HTTPS, FTP) through the firewall to the "Demilitarized Zone (DMZ)" (comprising our web servers); access to the "Protected Zone" by remote employees is granted through a Virtual Private Network (VPN) protected by 168-bit Data Encryption Standards (3DES), an extremely secure encryption standard.

Virus Protection

- All of our desktop machines and web and database servers are protected by Computer Associates (CA) InoculateIT anti-virus software, with virus definitions updated automatically daily through an in-house server that synchronizes with the CA server as updates become available.
- Incoming e-mail is scanned at Leader's mail server and viruses are eradicated before the e-mail is accessible by the client.

Transaction Logging and Hardware Redundancy

- RAID technology hardware redundancy is in effect on all production web and database servers.
- Our client SQL databases are protected using transaction logging. The logs are backed up to a separate server using RAID hardware redundancy. Data can be rolled back to any previous transaction log backup if needed.

Backups

- Our web and database servers are backed up nightly and the backup tapes are rotated off-site.

Miscellaneous

- Web and database servers are patched regularly against recently-discovered vulnerabilities.
- Access logs, intrusion detection, and statistical reporting are supplied to management monthly.
- Data submitted by clients is stored on a database server that is separate from web application servers.

PAsecureID

- By following Leader's data submission recommendations, including the transmittal of student identifiable data via our secure upload site, student data, including the recently implemented PAsecureID, is protected.

continued on reverse

continued from reverse

Web Application Security

Client Login

- All web applications are protected by a user ID/password combination that must be entered by the client in order to access the application. This combination uniquely identifies the user (either an individual or an entity, *e.g.*, an LEA) to Leader. Login times and client IP addresses are logged by Leader's servers.

SSL Encryption

- Our web applications use 128-bit Secure Sockets Layer to encrypt communication between the web browser and Leader's servers (the same type of encryption used by banks, merchants, and other companies that require secure transactions over the web). The SSL certificate used to secure communication is a digital ID that verifies to site visitors that they are communicating with Leader's web site and encrypts all data communication between client and server.
- Leader's SSL certificates are issued by VeriSign, the most widely known and trusted third-party certification authority. Clients can click a VeriSign logo on the log-in screen of any Leader web application to instantly verify that the page originated through a server in Leader Services' domain. After the client logs into the site, he/she may check the SSL certificate's validity by using the tools built into the client's web browser (generally represented by a "lock" icon in the browser taskbar).
- Web browsers must be capable of supporting high-level encryption in order to use our web applications.

Secure Coding Practices

- Data entry fields are protected, where applicable, through character conversion to protect against SQL and script injection attacks.
- Leader monitors the SANS/FBI list of top vulnerabilities and takes recommended action to protect against them. Leader staff also subscribes to *bugtraq*, an e-mail listserv that monitors application security vulnerabilities.

Secure Upload Site

- Leader hosts a secure upload web application to protect all sensitive client data (www.leaderservices.com/uploads). We strongly encourage clients to submit all sensitive data through the secure upload site rather than via unencrypted e-mail.

Site Monitoring

- Our web sites are monitored for availability 24 hours a day by a third-party monitoring firm.

Physical security

- All web and database servers are located in our secure corporate headquarters, protected by card-access readers that only allow physical access to authorized personnel.
- We use industry-standard uninterruptible power supply devices for initial power backup to our web and database servers. The power supply system is further backed up by a dual-fuel automatic AC generator rated at 31.9 KVWA; the generator, tested weekly, keeps our website hardware running in the event of a public power grid failure.

Leader recognizes that since security threats continually evolve in sophistication and technique, this policy must be revisited and revised regularly in anticipation of and in response to possible threats.

LEADER
SERVICES

For more information, contact Bruce Bonacci, Information Technology Director, at (800) 522-8413.