

LEADERSHIP STRATEGIES

Maximizing People Results TM

8776 East Shea Blvd., #B3A-313

Scottsdale, AZ 85260 USA

Tel: 480-467-0344 Fax: 480-467-0308

www.peoplereults.com

Statement of Security Measures for Profiles International Hosted Web Systems

Our servers are hosted at a world-class hosting facility in a metropolitan area to ensure high availability of network and power resources. Physical security at the hosting facility is high. Only authorized hosting facility employees may enter the locked machine room where servers are housed. No servers are directly accessible from the Internet. All servers are on a private network address range and located behind a state-of-the-art, enterprise-class firewall product. The same firewall also protects the servers from users and systems on other servers at the same hosting facility.

Only web traffic is allowed to the application servers from the Internet at large. No traffic is allowed to reach the database servers from the Internet; only the application servers are allowed to communicate directly with them. Certain special addresses are allowed to connect to the application and database servers to perform system administration and testing functions by authorized Profiles International personnel.

Unnecessary services and connection methods have been disabled and security patches for system vulnerabilities are routinely applied. All login and credit card transactions are performed using SSL encrypted connections.

Databases are backed up every 30 minutes to ensure the highest data recoverability.

The Data Center

Our hosting facility provides the world-class infrastructure necessary to maintain Profiles web servers 24x7. The data center has been engineered to avoid any single point of failure in connectivity, power, or HVAC. And because it is not open to the public, only a handful of highly trained, level-three technicians are allowed within close physical proximity to the servers. **Physical Security:** The data center is physically isolated from everyone but level three technicians. Public access is strictly forbidden. Access to the floor the data center resides on is restricted to those holding facility military-grade pass cards. Furthermore, Biometric hand scanners restrict access to the data center itself. **Location:** San Antonio is an ideal location for the data center because of the absence of natural disasters. San Antonio is on the most seismically stable soil in the US. In fact, San Antonio is one of only two places in the US that Lloyd's of London will underwrite for earthquake insurance. Additionally, the absence of hurricanes and tornadoes make the data center the perfect location for mission-critical data. **Conditioned Power:** Data centers power systems are designed to run uninterrupted even in the unlikely event of a total power outage. All servers are fed with conditioned UPS (Uninterruptible Power Supply) power that will run if utility power fails. The UPS power subsystem is N+1 redundant with instantaneous failover in case the primary UPS fails. In the event of an extended power outage, an on-site diesel generator can run indefinitely. The generator is regularly tested to ensure that it will continue to function in

the event of an emergency. **A Precision Environment:** All air is circulated and filtered every 90 seconds to remove dust and contaminants. The data center's HVAC (Heating Ventilation Air Conditioning) system is N+1 redundant to ensure that - even in the event of an entire HVAC system failure - there is a duplicate system on standby to take over. An advanced fire-suppression system is in place to prevent any fire from spreading - in the unlikely event that one could start. All cables to servers and routing equipment are securely tied down, and cable racks suspended from the ceiling provide dual routes for all cables. In the event that all cables on a cable rack are cut or burned, packets of data will automatically be routed to a second set of cables on the other side of the data center.

Connectivity Connections to multiple backbones ensure that data reaches the end-user in the fastest, most efficient manner possible. The facility also has peering agreements with local ISPs to allow fast delivery of packets when possible. **BGP4 Routing:** The Center runs the Border Gateway Protocol (BGP4) for best case routing. An entirely switched, Cisco powered network employs Cisco GSR 12000 class routers running HSRP (N+1 hot failover) to ensure that data can be routed even in the event of a router failure. The BGP4 protocol is a standard that allows for the routing of packets of information sent out from the network. Each packet of information is evaluated and sent over the best route possible. Because of the redundant network architecture, packets may be sent via alternative routes even if they are being delivered to the same end user. Should one of the providers fail, packets leaving the network are automatically redirected through another route via a different provider. **Guaranteed packet Delivery:** Facility pays the providers to make sure that packets of information are delivered to the end user's eyeballs. This offers significant advantages over simply peering with the major backbones. Peering agreements rarely include Service Level Agreements (SLAs) so no one is accountable for lost packets at congested exchange points. Because the facility actually has SLAs with all their providers, they are able to guarantee that all packets will leave their network at full speed. **Bandwidth Utilization:** The network has plenty of excess capacity, even during peak hours. This allows for accommodating even the largest spikes in traffic that are often associated with the most popular Web sites. Facility is always adding network connectivity and new routes in an effort to make sure content is delivered to users as efficiently as possible. A low bandwidth utilization also allows for maximum uptime, even if one of the providers has an outage.

Availability

Network Quality: Facility is officially a "Cisco Powered Network" meaning it uses only Cisco Systems Network gear. Redundant network components are used to ensure uptime and eliminate any single point of failure. The network is multi-homed through multiple redundant high-speed connections providing fast, reliable connectivity.

Network Uptime: Facility guarantees that the network will be available 99.999% of the time in a given month (no more than 24 seconds downtime per month), excluding scheduled maintenance. Network downtime exists when a particular customer is unable to transmit and receive data and facility records such failure in the trouble ticket system.

Hardware Guarantee: Facility guarantees the functioning of all leased hardware

components and will replace any failed component at no cost to the customer. Hardware replacement will begin immediately upon identification of the hardware failure and is guaranteed to be complete within 2 hours of problem identification. Hardware is defined as the Processor(s), RAM, hard disk(s), motherboard, NIC card and other related hardware included under the server lease.

Network Providers

Facility utilizes multiple OC12, OC3 and DS3 connections to multiple network providers to ensure fast, reliable connectivity, including:

AT&T (OC-12) AT&T is among the world's premier voice, video and data communications companies, serving consumers, businesses and government. AT&T has annual revenues of nearly \$66 billion and 162,000 employees, and provides services to customers worldwide. AT&T runs the world's largest, most sophisticated communications network, is the largest cable operator in the U.S., and has one of the largest digital wireless networks in North America. AT&T is a leading supplier of data and Internet services for businesses and offers outsourcing, consulting and networking-integration to large businesses.

Qwest Communications International (OC-12)

Quest Communications International is a leader in reliable and secure broadband Internet-based data, voice and image communications for businesses and consumers.

Sprint (OC-12) Sprint is a global communications company serving 26 million business and residential customers in more than 70 countries.

Time Warner Telecom (OC-12)

Time Warner Telecom is a subsidiary of Time Warner Telecom Inc., headquartered in Littleton, Colo. Time Warner Telecom delivers "last mile" broadband data, dedicated Internet access and voice services for businesses in 21 states. One of the country's premier competitive telecom carriers, Time Warner Telecom offers broadband services primarily to large and medium customers in 44 U.S. Metropolitan areas over its fast, powerful and flexible, fiber, facilities-based metro and regional optical networks.

UUNET, an MCI WorldCom company, is a global leader in Internet communications solutions offering a comprehensive range of Internet services to business customers worldwide. Providing Internet access, web hosting, remote access and other value-added services, UUNET offers service in over 100 countries, to more than 70,000 businesses, and owns and operates a global network in thousands of cities throughout North America, Europe and Asia Pacific.

Application Systems and Architecture

Our custom enterprise web applications are developed using premier, industry-standard development tools from leading vendors, and build on and extend the fault-tolerance, robustness and security of the infrastructure that they rest on. Database functions are isolated to multiple, multi-cpu, dedicated database servers, where all data is housed (no data is stored on the web servers). Applications are load-balanced across multiple web servers, allowing new features and system enhancements to be rolled out without

interrupting existing user connections to applications. With the existing configuration, multiple servers can fail and sites will still be available to users. Advanced monitoring systems dispatch immediate notifications to appropriate personnel in the event of performance degradation or system failures. All servers are homed in private networks behind a state-of-the-art, enterprise-class firewall product. The same firewall system also protects the servers from users and systems on other servers at the hosting facility. Only web traffic is allowed to the application servers from the Internet at large. No traffic is allowed to reach the database servers from the Internet; only the application servers are allowed to communicate directly with them. Unnecessary services and connection methods are disabled, and security patches for system vulnerabilities are routinely applied as they become available. All login and credit card transactions are performed using SSL encrypted connections. All production web servers and database servers are backed up nightly. An offsite tape-rotation scheme is employed to ensure that backups of data are always available, even in the unlikely event of a large-scale disaster. (Note: These backup measures are in place to facilitate restore operations during the course of disaster recovery operations, such as a server or facility failure, and are not available for the restore of user- or organization-specific information which has been deleted by end users of the systems.)

LEADERSHIP  STRATEGIES
Maximizing People Results TM
8776 East Shea Blvd., #B3A-313
Scottsdale, AZ 85260 USA
Tel: 480-467-0344 Fax: 480-467-0308
www.peoplereults.com