PANGEA FOUNDATION SECURITY STATEMENT

Pangea Foundation's information systems offer multiple layers of security to help ensure that the integrity of your data is never compromised. We know that security is crucial to you. That's why we devote significant resources toward safeguarding and protecting your information, with hosting infrastructure that meets the highest industry standards for physical security, system security, network security, and operational security.

Physical Facilities Security

Pangea Foundation works with one of the leading managed hosting providers in the world—Rackspace®. Information about Rackspace can be found at **www.rackspace.com**. To maximize security, Pangea Foundation uses dedicated equipment in its hosting environment. In other words, Pangea Foundation does not share its equipment with other companies. Pangea Foundation also updates its server equipment regularly to ensure that current technology performance standards are met. The integrity of the equipment in our hosting environment is proactively monitored 24/7. Following is a short list of physical security guarantees:

- Rigorously monitored access to all data centers, using keycard protocols, biometric scanning protocols, and continuous interior and exterior surveillance
- Unmarked facilities to help maintain low profile
- Data centers are isolated from everyone but authorized level three technicians, without exception
- All data center employees undergo thorough background security checks before being employed
- All data centers' HVAC (Heating Ventilation Air Conditioning) systems are N+1 redundant ensuring that a duplicate system can immediately come online in the event of an HVAC system failure
- All air is circulated and filtered every 90 seconds to remove dust and contaminates
- An advanced fire suppression system is designed to stop fires from spreading if one should occur
- All cables are securely tied down with cable racks suspended from ceilings providing dual routes for all cables, and in the unlikely 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
- In the unlikely event of a total utility power outage, all data center power systems are designed to run uninterrupted supplied by conditioned UPS (Uninterruptible Power Supply) power
- The UPS power subsystem is N+1 redundant, with instantaneous failover if primary UPS source fails
- For extended utility power outages routinely tested, on-site diesel generators can run indefinitely
- All data centers use only fully redundant, enterprise-class routing equipment
- All routing equipment is housed in a secured core routing room fed by its own redundant power supply
- Fiber carriers enter facilities at disparate access points to guard against service failure
- Physical security audited by an independent firm

System Security

Dedicated Firewall

Pangea Foundation's systems are protected by Cisco Firewalls. These fully managed devices include 24/7 monitoring by Rackspace Managed Network Security experts. All of our equipment is dedicated and used exclusively by our clients. A dedicated firewall acts as a protective barrier to keep destructive forces away from your mission-critical data. Unlike shared firewall devices that leave the possibility of unauthorized access by any other customer sharing the same firewall, a dedicated firewall provides protection exclusively to your server, and ultimately, a greater level of security for your peace of mind.

Although software firewalling has its place, it does not offer the same level of security as a dedicated hardware device. The Cisco switches, routers, and firewalls that we employ in production perform Stateful Packet Inspection (SPI) and allow for traffic logging, auditing, and shaping. Additional security options such as a Virtual Private Network access are not available with software or shared firewall solutions.

Virtual Private Network

In addition to filtering traffic, a dedicated firewall allows for a more secure form of communication with the implementation of a Virtual Private Network (VPN). A VPN encrypts all traffic between servers and creates a secure link through which various environments communicate.

In addition to protecting communication between servers, administrative connections to all Application and Data Servers are protected through a separate VPN Connection. This protects the communication between a technician and the server during any deployment or troubleshooting sessions, ensuring no action can be intercepted by a 3rd party.

Data Reliability and Backup

All networking components, web servers, and additional application servers are configured in a redundant configuration. Customer data is automatically backed up on a nightly basis and stored in a secure location onsite for a minimum of seven days. Beyond that, backups are compressed, encrypted with a passcode, transferred via secure channels and archived in an offsite secure storage environment on a nightly basis for long-term storage. Long-term storage backups are destroyed after not less than twelve months following the date of the original backup, unless otherwise agreed to in writing. System patching provides ongoing protection from exploits.

Anti-virus Protection

Pangea Foundation's servers are protected against destruction and data loss due to Viruses, Trojans, Worms and Malware with automatic real-time updates and around-the-clock monitoring 24x7 provided by a global leader in endpoint, network and data security. With this level of protection, customer data is protected against the newest threats—automatically.

Beyond the protection of our data and application servers, Pangea Foundation also enforces strict anti-virus protection on all development and testing platforms. This layer of protection guards against attack at the source of all development code before it is released into test and live environments.

Independently Audited Disaster Recovery and Business Continuity Plans

Independently audited disaster recovery and business continuity plans are in place for the headquarters and support services of Pangea Foundation's hosting data center.

Network Security

Without the best network, world-class software applications can become average. It's one of the reasons Pangea Foundation chose Rackspace as its hosting provider. Rackspace is known for designing **The Zero-Downtime Network™**. The Zero-Downtime Network delivers 100% network uptime. How is this achievable?

- Not using its network for purposes other than managed hosting—no telecom or cable TV services take priority over customer needs;
- Using only high performance bandwidth, unlike cheaper hosting providers;
- Partnering with nine network providers to provide multiple redundancies in information flow to and from data centers and end users;
- Fiber carriers enter data centers at disparate access points protecting network from complete service failure in the unlikely event of a network outage;
- Rackspace's Proactive Network Methodology continually monitors and automatically improves the network topology and configuration in real-time based on route efficiency and end-user performance, ensuring the fastest and most reliable network connections;
- Maintaining low network utilization, providing resiliency from the largest Internet routing issues;
- A highly redundant network configuration co-developed with Cisco to protect against single points of failure at the shared network level;
- Partnering with Cisco and Arbor-Networks to create ever-improving methods to monitor and secure the Rackspace network from intrusions.

Administrative Security

Traditionally, security incidents have originated from inside organizations about four times more frequently than from the outside. So even when your data is protected by the best technologies, it remains vulnerable to whatever shabby protocols and shoddy standards exist within your provider's organization. At Pangea Foundation, we work hard to take practical action by implementing policies and institutionalizing security protocols aimed at ensuring the integrity and protection of your information.

Pangea Foundation's employees are required to review, understand and sign policies, procedures and confidentiality agreements that require them to maintain the strict confidentiality and security of client data. Access to confidential information is restricted to authorized personnel who have passed thorough background security checks. Pangea Foundation and hosting provider employees do not have direct access to the production equipment, except when necessary for system management, maintenance, monitoring, technical support at the customer's request and backups.

Application Security

Pangea Foundation draws from a broad knowledge and a conscientious pledge to understanding sophisticated application development methods and advanced vectors of attack. We understand that system security is not a one-time effort. Securing systems is an ongoing endeavor to stay ahead of attacks and vulnerabilities. We use many sources of information to determine our level of protection against the newest vulnerabilities and work with Rackspace to implement protections as quickly as possible. These updates are tested and reviewed before being applied to ensure security updates won't adversely impact software and data systems.

Website Security

Authenticating user identify is not only a best practice, it's also a privacy and security imperative necessary to meet regulatory compliance standards, including Federal HIPAA guidelines.

Encryption forms the basis of data integrity and privacy necessary for web commerce. When an SSL or TLS handshake occurs between a server and a client, a certain level of encryption is determined by the Security Certificate, the web browser, and the server operating system. Without encryption, the integrity of data being transmitted through public and private networks can be compromised. Pangea Foundation leverages strong encryption protocols to secure your data and communications. In fact, current key strength is an industry-leading 256 bit certificate, far exceeding most websites in operation today. You can be confident knowing that the information you transmit to our data servers will be protected during transmission.

We continually fine-tune the balance between delivering the optimum user experience and achieving the highest possible levels of server security. The certificates we employ to encrypt traffic to our application servers are reviewed on an ongoing basis. This helps us stay ahead of the latest vulnerabilities and helps to ensure that information is transmitted over the most secure channel possible. During our review process, each application server undergoes multiple security checks and is evaluated against the latest vulnerabilities to determine the effectiveness of the upgraded security controls. If any controls are deemed inadequate or missing, they are immediately updated or installed.

Secure Sockets Layer Encryption, or SSL, has recently become vulnerable to sophisticated attack methods and may be subject to risk. That's why our application servers employ the upgraded Transport Layer Security (TLS) protocol. To ensure the latest threats are dealt with head-on, our certificates, server protocols and encryption standards are routinely scanned against industry best practices.

Authentication

Users of Pangea Foundation's software applications may only access them with a valid username and password. Pangea Foundation's applications are encrypted through 256-bit secure certificate while in transmission. Users must use passwords that meet defined security standards. An encrypted session ID is used to uniquely identify each user and this session ID is automatically scrambled at periodic intervals.

Automatic Session Termination

To comply with security regulations, protect the privacy of sensitive information, and protect you from liability, Pangea Foundation's software applications employ automatic session termination if users do not interact with them for more than 20 minutes. If no interaction with the software has occurred for more than 20 minutes, subsequent login is required. The automatic session termination is a security feature designed to prevent someone other than the logged-in user from accessing information. It's particularly important in environments where users are called away from their computers on a regular basis.