

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.

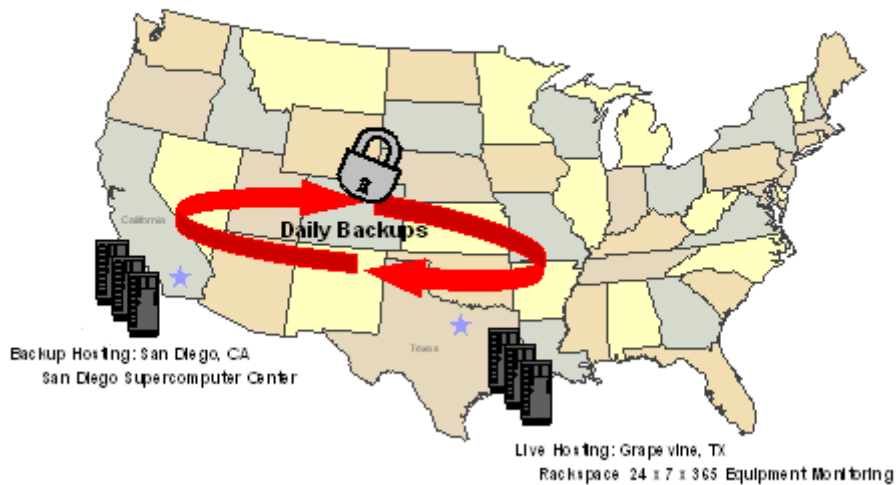
Pangea Foundation's world-class IT Infrastructure provides you with the option of multi-regional redundancy to give you peace of mind. Both our primary hosting data center in Grapevine, Texas and our backup hosting data center in San Diego, California meet the highest industry standards for physical security, system security, network security, and operational security.

Physical Facilities Security

Pangea Foundation's multi-regional hosting package offers you the option of bolstering your disaster recovery plan with server redundancy in geographically disparate regions to ensure your data is protected in the event of a local, regional, or national disaster.

INFORMATION TECHNOLOGY INFRASTRUCTURE

Multi-Regional Redundancy and Disaster Recovery Strategy



Primary Data Center

Pangea Foundation works with the leading managed hosting provider in the world—Rackspace®. Information about Rackspace can be found at www.rackspace.com. Pangea Foundation's primary data center is located in Grapevine, Texas. To maximize security, Pangea Foundation ensures that the equipment it uses in its live hosting environment is dedicated equipment. 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 production 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 contaminants
- An advanced fire suppression system is designed to stop fires from spreading in the unlikely event 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

Backup Data Center

Pangea Foundation's primary backup servers are hosted at the [San Diego Supercomputer Center \(SDSC\)](#). With capacity for up to 25 petabytes of tape archive, the SDSC is considered an international leader in data management, systems security, high-performance computing and networking.

As a major partner in both the [U.S. TeraGrid Initiative](#) and the [Cyberinfrastructure Partnership \(CIP\)](#), the SDSC supports several of America's cutting-edge research-oriented computational environments and aims to spur the expansion of strategic infrastructure activities throughout the national community.

The SDSC adheres to the most advanced security protocols, including 24-hour surveillance, picture identification for access, redundant electrical generators, redundant data center air conditioners, advanced fire suppression, and other backup equipment and devices designed to keep servers continually operating.

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 secured 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 Pangea Foundation's IT Hosting environments communicate.

Data Reliability and Backup

All networking components, Web servers, and additional application servers are configured in a redundant configuration. All customer data is automatically backed up on a nightly basis. System patching provides ongoing protection from exploits. Daily backups are stored in two data centers located 1,400 miles apart on a 24 hour basis. Data backups are stored for two weeks on servers located in our primary data center, and archived indefinitely on servers located in our backup data center.

Anti-virus Protection

Pangea Foundation's software applications come standard with anti-virus protection from [Symantec™](#), a global leader in infrastructure software. With anti-virus protection, customer data is automatically protected from destructive viruses, worms, spyware, and adware.

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 primary data center. In the unlikely event that the primary hosting facility went offline due to a natural disaster, and the existing disaster recovery and business continuity plan was insufficient, a contingency plan is in place for Pangea Foundation's backup hosting facility to be up and running with the most recently backed up data within 24 to 48 hours.

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 primary hosting provider. Rackspace is known for designing [The Zero-Downtime Network™](#). The Zero-Downtime Network gives Pangea Foundation 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 overall 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.

Compliance Management

Today's risks and regulations are so numerous and dynamic that it's easy to fall behind and end up with a false sense of security. After all, what was compliant last year might not be compliant this year. To help ensure that your data meets the highest standards of security and compliance, Pangea Foundation enables you to leverage the services of one of the world's leading experts in software application security and compliance management.

Data Vulnerability Assessment Snapshot

Using a trusted data vulnerability assessment and compliance management solution, Pangea Foundation can validate compliance with a variety of regulations such as:

- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Federal Information Security Management Act (FISMA)
- Payment Card Industry (PCI) Data Security Standard
- Gramm-Leach-Bliley Act (BLBA)
- Statement on Auditing Standards Number 70 (SAS-70)

Data vulnerability scan tests can detect more than 3,000 network, operating system and application vulnerabilities. The internal vulnerability scanning service can detect and evaluate vulnerabilities across all areas of Pangea Foundation's IT environment from behind the firewall, and provide recommended courses of action.

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.

Employee Background Checks

At Pangea Foundation, we employ extensive fingerprint background checks on 100% of Pangea Foundation employees to ensure that our employees meet the highest levels of integrity. But we don't stop there. We only work with hosting providers that meet this important requirement, too. Each data center employee working for our primary hosting provider undergoes multiple and thorough background security checks before they're hired.

Access Restrictions

Pangea Foundation's employees are required to review, understand, and sign confidentiality agreements that require them to maintain the strict confidentiality and security of client data. Access to confidential information is restricted to authorized personnel only. 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.

128-bit Secure Sockets Layer Encryption (SSL)

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

Encryption forms the basis of data integrity and privacy necessary for Web commerce. Secure Sockets Layer Encryption, or SSL, is an advanced encryption technology that protects Pangea Foundation's software applications. Without encryption, the integrity of data that is transmitted through public and private networks can be compromised.

SSL uses public key encryption methods to verify the authenticity of a server or client and encrypt communications between them. SSL encryption protects network access, online communications, and digital communications by creating a secure channel between Pangea Foundation's technology infrastructure and Pangea Foundation's users.

Pangea Foundation offers strong encryption options to secure your data and communications, including the 128-bit VeriSign® SSL Certificate. Trusted by more than 500,000 businesses, VeriSign is the SSL Certificate provider of choice for more than 93% of the Fortune 500 and the top 10 banks in the United States. A more affordable and considerably faster version of SSL Certificate to implement is the SSL 123, capable of 128-bit encryption for securing your data transactions. Although its issuing process isn't as thorough as VeriSign's, it's considered an effective option for encrypting data transmitted from sensitive applications to users online.

SGC (Server-Gated Cryptography) enabled SSL certificates.

With Pangea Foundation, you can have confidence knowing that your software is protected by Server-Gated Cryptography enabled SSL certificates. Server-Gated Cryptography enabled SSL certificates offer the most powerful SSL encryption commercially available. Although an SSL is capable of 128-bit encryption, millions of people still use older computer systems that are incapable of strong encryption. Legacy browsers and operating systems often fail to step up to strong encryption without a Server-Gated Cryptography enabled SSL certificate. Examples include:

- Various Internet Explorer browser versions from 4.01 to 5.01
- Various Netscape browser versions from 4.07 to 4.72
- Various Windows 2000 systems that use Internet Explorer

When an SSL handshake occurs between a server and a client, a certain level of encryption is determined by the SSL Certificate, the Web browser, and the client operating system. Strong encryption, at 128 bits, calculates 288 times as many combinations as 40-bit encryption. That means it's *over a trillion times a trillion times stronger*.

Authentication

Users of Pangea Foundation's secure Software-as-a-Service solutions may only access these applications with a valid username and password. Pangea Foundation software solutions are encrypted through 128-bit SSL certification while in transmission. Users must use passwords that meet Pangea Foundation's 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.

Application-level Firewall

According to [Gartner](#), “75% of hacks occur at the application level.” That’s why, in addition to the robust firewall that protects our hosted environment, Pangea Foundation offers you the option of incorporating a highly advanced layer of security into your software: a one-of-a-kind *application-level* firewall.

Developed by [Fortify® Software](#), this unique “internal firewall” monitors and protects your software from the inside-out. So rather than focusing on eliminating intrusions solely with perimeter solutions and firewalls, this breakthrough approach tackles security threats directly at the root cause—the software application. It’s the first and only application-level intrusion prevention solution for software applications already in deployment and it was designed to protect you from even the most *sophisticated* intrusions. The result: unparalleled information security *and* the peace of mind that comes from knowing that your software is fortified by the same security solution used by organizations like these:

- The top five commercial banks and seven of the world’s eight largest banks
- Five of the top seven computer software companies
- Three of the top five aerospace and defense industry leaders
- The United States Air Force
- The United States Navy
- The United States Army
- Three of the top five telecommunications companies
- Three of the top six securities industry firms
- Two of the world’s most visited Internet companies
- Two of the top three insurance companies
- The #1 enterprise software company
- The #1 wireless voice and data carrier in the U.S.
- The #1 computer peripherals company
- The world’s largest dedicated semiconductor foundry
- 17 of the Fortune 100
- Over 30 of the Fortune Global 500