

# TECHNOLOGY OVERVIEW

## PROTECTING CUSTOMER DATA

Protecting your data is our number one concern. Compliance11 uses the highest levels of security and industry standards to ensure that your data is protected. Compliance11's production servers are hosted in a SAS70 Type II compliant environment by Rackspace, the world's leader in hosting, and it is tested and certified on a regular basis by Trustwave, an industry leading security firm. Rackspace is also Safe Harbor certified, as defined by the EU Commission's Data Protection Directive, meaning that data flows to Rackspace are acceptable.

## PHYSICAL SECURITY

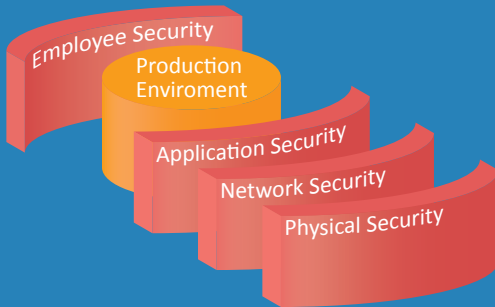
- **Security Badge** - Card reader access is required to enter the facility.
- **Biometric Scanning** - Biometric scanning is required for access to the data center floor.
- **Proximity Readers** - Proximity readers track all movement between areas.
- **Security Cameras** - Security cameras are located throughout the entire facility to monitor and record activity.
- **Security Personnel** - 24/7 onsite staff provides additional protection against unauthorized entry.
- **Unmarked Building** - Facilities are unmarked to help maintain a low profile.
- **Audits** - Rackspace physical security is audited by an independent firm.

## NETWORK SECURITY

- **Firewalls** - Access is limited to certain ports by a series of firewalls.
- **Intrusion Detection** - Systems proactively monitor for malicious connection activity.
- **Anti-Virus** - Anti-virus software is active on all servers.
- **Patches** - Security patches are applied proactively based on vendor recommendations.
- **SSL** - All data transferred between the user's browser and Compliance11 is protected using Secure Socket Layer (SSL) encryption.
- **PGP Encryption** - All back-end file transfers are encrypted using PGP encryption.
- **Administrative Access** - Administrator access to the production infrastructure requires two-factor (hardware token) authentication.

## APPLICATION SECURITY

- **Database Encryption** - Sensitive personal information is encrypted in the database.
- **Application Architecture** - Compliance11's application is built using J2EE and Oracle database, the de facto industry standard for highly scalable, secure, fault tolerant, enterprise applications.



## SAS 70 TYPE II CERTIFICATION

Statement on Auditing Standards No.70 (SAS 70) is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants. Type I Certification measures a single point in time, while Type II Certification measures and evaluates operating effectiveness over a period of time.

SAS 70 Type II Certification is third party verification that services are undertaken in a controlled manner and the auditor finds sufficient processes, controls and safeguards to keep assets and data safe from theft, corruption or mishandling.

## SAFE HARBOR CERTIFICATION

The US Department of Commerce partnered with the EU Commission and developed a "Safe Harbor" framework that was approved by the EU Commission in 2000. Certifying to the Safe Harbor assures EU Organizations that a company provides "adequate" privacy protection, as defined by the Data Protection Directive.

U.S. organizations participating in the safe harbor are deemed adequate and data flows to these companies are acceptable. Furthermore, all 25 Member States of the EU are bound by the European Commission's finding of adequacy.

- **Penetration Testing** - Internal and external penetration tests are conducted periodically by an independent third party.
- **No Cookies** - No cookies are used to store information on customer workstations.
- **IP Login Restrictions** - Access can be limited by source IP addresses.
- **Single Sign-On** - Access to the application can be granted via corporate directory.
- **Password Expiration** - User passwords can be set to expire on a periodic basis.
- **Password Re-Use** - The re-use of previous user passwords can be disallowed.

### *EMPLOYEE SECURITY*

- **Background Check** - All employees are subject to a background check that checks the following: SSN Verification, Address History, 7-Year National Criminal Database Search and Courthouse Verification of Criminal Database Records.
- **Information Security Policy** - All employees periodically certify to have read and comply with Compliance11's Information Security Policy.
- **Personal Trading Supervision** - All employee's personal security transactions are monitored.

### *PRODUCTION ENVIRONMENT*

- **Redundant Servers** - Compliance11's application tier has load balanced, redundant servers. If an application server fails, users are able to login to the other server immediately with no data loss. Compliance11's database tier has a redundant server and uses shared disk. If the database server fails, users are able to login again within minutes with no data loss.
- **RAID Storage** - If a hard drive fails, there will be no interruption of service since all storage is RAID 5 with a hot spare.
- **Disaster Recovery** - In the event of a major disaster at the primary hosting site, users will be able to login to another server hosted at a remote secondary site within hours. No more than two hours of data will be lost.
- **Network Availability** - The network's configuration was co-developed with Cisco and includes six separate fiber conduits into the facility from different communication providers.
- **Backup** - Database backups are done every two hours and are immediately sent electronically to the disaster recover site.
- **SAS70 Type II** - Rackspace is SAS70 Type II certified.
- **UPS** - Upon power loss, UPS systems can provide 30 minutes of battery life under peak load.
- **Generator** - Two sets of diesel generators have enough fuel stored to provide 48-hours of power under full load.