complysci

Security Ecosystem

An Overview of Administrative, Physical and Technological Safeguards

Security at Every Level

ComplySci implements security at all levels of the infrastructure stack and employs the latest technologies to safeguard client information. Critical information security practices like software development and infrastructure security are regularly reviewed by independent information security organizations.

Administrative Safeguards

- ComplySci maintains and regularly updates its information security program
- ComplySci maintains data classification policies to ensure that client data is
- appropriately handled throughout the organization
- Multi-jurisdictional background and identity checks are performed on all employees
- Access to ComplySci production infrastructure, including client relevant systems, is restricted to a small subset of employees whose access is based on need-to- know principles
- Employees are provided regular security training utilizing a 3rd party curriculum as well as frequent follow-up alerts and security reminders

Physical Security

ComplySci maintains infrastructure in the most technically sophisticated datacenters available which are also used by some of the most security conscious technology organizations and financial institutions like Salesforce.com and Microsoft.

Physical security features include:

- Anonymous buildings with embassy grade car barriers and damage resistant construction
- Comprehensive access controls consisting of 24x7 staffing, one-time use ID cards, mantraps, biometric authentication, complete area video surveillance, silent alarms and roving security patrols
- Sophisticated environmental control systems including redundant electrical connections, independent power generation provided by onsite diesel generators with priority fuel resupply, battery backup, IR gas/leak detection systems, redundant physically separated Internet circuits
- Independently audited to SOC 1 criteria and meet several ISO standards
- Independent security assessment provided by Cyber GRX, with results available upon request

Network Security

ComplySci employs proven security practices along with multi-level security products from leading security vendors. Network security features include:

- 24x7 security operations center administered by a nationally recognized managed security services firm
- 24x7 incident response and management
- Latest perimeter firewall and intrusion detection systems coupled with network based intrusion protection together with 24x7 log monitoring and analytics,
- Two-factor authentication for employee remote access to internal networks together with host lockdown to prevent unauthorized data transfer

Host Security

ComplySci uses well-known branded hardware products with proven reliability and security features.

- Hosts equipped with comprehensive data protection including RAID, network interface redundancy, secure lights-out management and remote reporting
- Vulnerability management program with periodic scans across COMPLYSCI infrastructure to detect insecure configurations or newly found vulnerabilities
- Semi-annual 3rd party penetration testing to confirm infrastructure security posture
- Email threat defense provided byProofPoint.

Application Security

ComplySci employs layered safeguards with PTCCTM and ComplySci applications and implements security best practices including:

- Strong password policies including lockout andauditing
- One-way encryption for stored passwords
- Industry standard TLS encryption for user sessions
- AES 256 full database encryption
- AES 256 encryption for all feed data
- Granular supervisor and user permission options to permit minimum access
- needed to complete tasks
- Semi-annual 3rd party code review against 100+ point threat model and OWASP top 10 criteria

Reliability and Recovery

ComplySci maintains disaster recovery safeguards such as:

- Backup datacenter located in a separate region from the primary datacenter
- Encrypted replication of PTCC and ComplySci data between datacenters to ensure a backup of the most recent client data without the security and custody issues of removable storage
- Periodic failover testing to assure contracted mean time to recovery and recovery point objectives

Privacy and Confidentiality

ComplySci understands the importance of maintaining the confidentiality and privacy of client data and implements the following safeguards:

- Maintain a current, regularly reviewed privacypolicy
- Self-certified to stringent European privacy standards via both EU Safe Harbor and Privacy Shield frameworks: http://safeharbor.export.gov/companyinfo.aspx?id=17967
- ComplySci does not share information with any affiliates or third-party entities. No vendors or contractors have access to client data or the systems on which it is stored.

Certifications and Documentation

- Compliance Science, Inc dba ComplySci is SSAE 16 SOC I Type II certified.
- Compliance Science third party security assessment by Cyber GRX that is available
- upon request.
- Compliance Science Information Security Policy