eCOMPLIANCE SECURITY STATEMENT

eCompliance's health & safety management system ("Management System") is a software-as-a-service (SAAS) solution protected by state-of-the-art infrastructure/physical and application security services.

Infrastructure/Physical Security

eCompliance maintains production servers in a Tier 1 hosting data center provided by Rackspace which is certified is SAS 70 Type II compliant. The data center and associated servers undergo an annual SOC (Service Organization Control) 1 audit which ensures that the data center servers meet the stringent international standards for hosting SAAS. This hosting environment meets the highest security standards by ensuring that the following is adhered to:

- Physical access to servers are restricted by keycard protocols, biometric scanning protocols, interior and exterior surveillance, background security checks;
- Precision Environment Infrastructure - Redundant HVAC (Heating Ventilation Air Conditioning) system, advanced fire suppression systems;
- Conditioned Power – Redundant Power systems to deliver UPS (Uninterruptible Power Supply) and on-site diesel generators in case of extended power outage; and
- Core Routing Equipment - redundant, enterprise-class routing equipment, fiber carriers enter data center at disparate points to guard against service failure.

Application Design and Architecture

Our Management System application has been architected from the ground up to be a reliable and secure solution. Designed in-house by our own Canadian-Based Software Engineers and Network Team, every release of Management System goes through extensive manual and automated testing to ensure data integrity for upgrades, optimization for performance and data security. Our software products boast over 10,000 unit tests, written test-first (TDD), as well as functional tests and over 100,000 tests are run daily to ensure quality. Our engineering practices ensure that quality is "built-in" and our industry best practices ensure that quality is maintained in the system.

Application Security

The data of eCompliance clients are stored on dedicated servers accessed through Secure Socket Layer (SSL), a cryptographic protocol that provides secure communications over the Internet. By using SSL, all sessions to Management System are encrypted. Communication between a user and the server also requires the user to log in from a standard web browser with approved authentication credentials (username and password). Our application utilizes numerous framework level protections to help prevent Web application vulnerabilities such as cross-site request forgery (CSRF), cross-site scripting (XSS), and SQL injections. All stored passwords are fully encrypted with secure one-way hash algorithm preventing them from being retrieved. SSL certification enables secure communication between client Communication between the server and the client.

Internal and Third Party Testing and Assessments

eCompliance tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities. Third-party assessments are also conducted regularly:

- Application vulnerability threat assessments
- Network vulnerability threat assessments
- Selected penetration testing and code review
- Security control framework review and testing

Monitoring and Backups

The entire Management System infrastructure is proactively monitored 24x7x365 with immediate notifications sent to our IT support team in the event of network, server, services or application failures.

To ensure business continuity our dedicated servers have hard disks with hardware RAID (Level 5) configurations that employ techniques of striping, mirroring, or parity to create reliable data stores with industry best uptimes and fault tolerance. This ensures that a hard disk failure does not affect performance and data integrity by ensuring server uptimes.

Customer database backups are performed daily, and are stored both on-site and off-site. Weekly Full, Daily Incremental backups are performed and verified. On-site backups are retained for two weeks, and off-site backups are retained for four weeks at a minimum. Off-site backups are also semi-staged and ready in the event of a regional datacenter failure significant enough to warrant a rapid-failover to a secondary-recovery site.

Financial Data (only applicable to credit card payers)

All financial credit card transactions are enabled via a gateway provided by TD Canada Trust and stored on PCI-Compliant servers. Financial data is passed directly from the client browser through a secure SSL connection to TD Canada Trust and at no stage is any financial data stored on any eCompliance systems. Once processed, TD Canada Trust generates a reference number which is used for billing.

Privacy Policy

eCompliance takes customer privacy seriously. For more information, please see our Privacy Policy at http://www.ecompliance.com/about-us/legal-info/