1209 King St. West   + 1.800.686.1915
Suite # 201   info@ecompliance.com
Toronto, ON M6K 1G2   ecompliance.com

Memo: From eCompliance to IT Departments Everywhere

Dear IT Professionals,

Your colleagues have indicated interest in using eCompliance to address their safety and compliance challenges. The purpose of this document is to provide an overview of the technical architecture of the eCompliance SaaS software solution.

We've divided this document into three parts:

1. Security & Privacy – we're safe and secure
2. Sustainability & Maintainability & Quality – we're low maintenance
3. Usability – our solution is straight-forward and effective

1. **Security & Privacy**
   We securely serve clients maintaining sensitive oil and gas, manufacturing, construction, nuclear information, private health information, and more. Our proven, cloud-based health and safety management software is protected by state-of-the-art security services at multiple levels, including physical security, infrastructure security and application security.

   Infrastructure/Physical Security:
   eCompliance maintains production servers in a Tier 1 hosting data center provided by Rackspace which is certified as SAS 70 Type II compliant. The data center and associated servers undergo an annual SOC (Service Organization Control) audit which ensures that the data center servers meet the stringent international standards for hosting Software-as-a-Service (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, dited by and independent firm
   - Use best-in-class network firewalls and internal firewalls between application and database layers
   - VPN/SSH access to application infrastructure restricted to only application developers and operations staff with strict permissions
   - Application and infrastructure logs monitored and reviewed daily
   - 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
   - Core Routing Equipment - redundant, enterprise-class routing equipment, fiber carriers enter data center at disparate points to guard against service failure

1209 King St. West   + 1.800.686.1915
Suite # 201   info@ecompliance.com
Toronto, ON M6K 1G2   **ecompliance.com**

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 the eCompliance 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 including:

- 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 eCompliance 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.

1209 King St. West
Suite # 201
Toronto, ON M6K 1G2

+ 1.800.686.1915
info@ecompliance.com
ecompliance.com

2. **Sustainability & Maintainability & Quality**

<u>**Application Architecture**</u>
The eCompliance Management System has been architected from the ground up to be a reliable solution with quality built-in. Designed in-house by our own Canadian-based Software Engineers and Network Team, every release of eCompliance 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 throughout the life of the system.

- No integration with existing systems needed – for example, our automated email notification feature does not need a tie into Exchange Server, etc.
- Can support data imports from existing systems if needed – i.e. new lists of staff can be imported on a regular basis; we have an Excel importer
- Need API's? – Our Application Program Interface (API) is able to access your eCompliance account data using HTTP and XML. The API makes it easy to create services and desktop applications that integrate with your eCompliance account.

3. **Usability**

We keep it simple – we make the most important features easy to use without complexity. We focus on the safety and compliance users that need to get stuff done every day and build a product around them.
- Tens of Thousands of Users – With tens of thousands of users of eCompliance products we've gone through hundreds of build, measure, learn iterations in order to continuously perfect how we present our features making them easier and delightful to use.
- Support – Support is available through various channels: email, phone, online FAQ's and forums, short "how to" video's and more.
- Check out our App! – Our Management System and App solutions seamlessly sync. We've spent the development time and dollars making sure that end users have the simplest interface from their mobile device. It can't get any easier than downloading an App and logging in.