Security Policies

Security and privacy of information is a top priority of ComplyWorks. Providing a solution that ensures all information providers are always in control of who can access their data is critical to our success, since we are entrusted with the stewardship of highly sensitive, confidential information.

Distributed Architecture

ComplyWorks has deployed its technical infrastructure using a distributed architecture technology. This provides for 99.99% guaranteed scheduled up time, eliminating the pitfalls of Disaster Recovery and Business Continuity (DRBC) processes and plans. With automatic integral failover across multiple servers in separate locations delivery is ensured.

The ComplyWorks servers are installed in two separate, secure data centers. The data centers are located in Calgary, Alberta and Vancouver, British Columbia, Canada. Both centers are connected to the North American Internet backbone using two separate major network providers at both locations.

Each data center houses a minimum of two large capacity physical servers owned by ComplyWorks. Each physical server in each data center is configured to run multiple virtual servers. The database server clusters run on virtual servers, separate from the web application and file system virtual servers. All virtual servers on one physical server are paired with a matching virtual server on the other physical server.

The servers run as a load balanced cluster. The file systems and database clusters are mirrored between all server pairs and between each data center, providing for full redundancy across four hardware platforms distributed across two North American Locations. This configuration assures availability even if one or more servers, or even an entire hosting centre, fails.

Physical Security

The ComplyWorks server platform resides in secure, bunkered data hosting facilities. The facility provides:

- Protection against unauthorized access through the use of two-factor card-key and user password, as well as on-site security personnel and 24 hour video monitoring.
- Redundant multiple connections to the primary Internet backbone to protect against loss of network connectivity.
- Redundant power supplies and independent power generators to ensure continuity in the event of electrical supply problems.
- Fire and flood mitigation and suppression systems.

Network (Electronic Security)

The software, computing and communications hardware that enable the ComplyWorks platform is protected by firewalls and surveillance equipment.

- All internal process communications within the hosting facility and between the primary ComplyWorks platform and all distributed nodes or components are encrypted with 128 or 256-bit encryption algorithms, which is equal to or significantly higher standard than what is deployed and deemed acceptable by major banks.
- Security also applies to the connections between the client's systems and the ComplyWorks platform. ComplyWorks will recommend and deploy the best method for securely exchanging data. ComplyWorks will accommodate a customer's preferred method, only on the condition that such method does not compromise the security or integrity of the ComplyWorks platform, data, or that of our other clients.
- Typically, interaction between a client's system and ComplyWorks Utility is protected by firewalls at both sites and incorporates 128-bit or 256-bit encryption to ensure privacy of the information.

Personnel Security

The importance of correct handling of sensitive information is ingrained in our corporate culture.

- Staff screening, hiring and management practices place emphasis on integrity and accountability and the rules for accessing client data.
- Access to client data is restricted to only those who need it to perform the required service.
- Employees are trained to fulfill their roles as trusted guardians of our client's sensitive data.
- Policies regarding staff turn-over or termination ensure the discontinuation of data access when required.

Security Features of the ComplyWorks web service

The following security features are being incorporated into the Web Service:

- All data is stored in a SQL database that is housed in our secure facility, along with the main system. External ports are closed. Key IT personnel have access to the system and database facility via secure VPN and SSH connections.
- **Secure Socket Layer protocol**. Logon page and services are only accessible via HTTPS 128-bit encryption. This ensures that the bit stream between the servers and client is, at all times, encrypted. This requires a trusted public certificate. Our single-root CA 128/256 SSL certificate ensures us that the authenticity of our certification is recognized by all browsers.
- **Passwords are stored using a standard DES one-way encryption algorithm.** The use of one-way encryption means that no key exists that would enable it to be decrypted. In order to logon successfully, a user's password must encrypt to the identical pattern as the stored reference, but there is no way to otherwise know what that password is. This means that even ComplyWorks staff have no means of determining a user's password and can only perform a reset.
- **CAPTCHA feature for performing Logon and Agreement**. CAPTCHA stands for "Completely Automated Public Turing test to Tell Computers and Humans Apart". Essentially, it is a test that humans can easily answer, but is extremely difficult (nothing's impossible) for a software program to handle. This feature works by generating an image representation of a random number. An automated software program, attempting to break in, would need to employ sophisticated optical character recognition to attempt to get the number. This technique is growing in popularity, but is still found on only the more sophisticated web applications.
- **Multi-level entitlement/authorization system**. Every page or feature in the application can be set to work for a specific level of authorization and can enable feature subsets based on specific service options associated with the specific user or their member account. Both the top and left menus will display only those features that the user is allowed. Any attempt to bypass the menu and target the browser directly to a page that the user is not authorized to access will force a logon scenario.
- **Code is guarded against "SQL Insertion" attacks.** Some secure web service developers are unaware of the techniques that can be used to override seemingly safe user inputs in order to take control of the database. This application will thwart any such attempt.
- **Activity logging**. The application will log significant activities, such as Member or User profile Adds/changes/deletions. These logs will be viewable by ComplyWorks staff and administrators. Important activities or requests will be queued up for staff/admin to take action such as invoicing or audit.
- **Error/Exception reporting**. The system automatically sends comprehensive error reports to the development group in the event of a software error or unhandled exception. This enables us to provide rapid response to any customer-affecting problem, and enhances our continuous improvement efforts.
- **Archives/Backups**. Deleted database records will be sent to an archive (a mirror of the main database structure), so that data is recoverable in the event of an accidental deletion. Full data backups are securely transferred to a secure offsite location, either by physical or electronic means, to provide business continuity in case of unforeseen catastrophe affecting the primary site.
- **Integration**. Any data exchange between the ComplyWorks platform and client or third party (WCBoards, Insurance providers, etc) is required to meet the ComplyWorks security standards. ComplyWorks has developed ComplyWorksX client integration component which is used to perform controlled data import and export functions using secure SOAP/SSL communication protocols. This solution provides secure exchange of information without requiring alterations to the client's existing firewalls and security measures.

Privacy Policies

ComplyWorks Privacy Guidelines incorporate the provisions of Part 1 of the Personal Information and Electronic Documents Act (PIPEDA - Government of Canada), the principals of the Personal Information Protection Act (PIPA - Government of Alberta) and the ten principles of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information.

Application of Privacy Principles:

1. RESPONSIBILITY:

ComplyWorks has appointed a Privacy Officer who is responsible for ensuring compliance with ComplyWorks Privacy Policy and Guidelines. Responsibility rests with the Privacy Officer even though other individuals within ComplyWorks may be responsible for the day-to-day collection and processing of personal information. The privacy officer for ComplyWorks is the manager of customer service.

ComplyWorks is responsible for all personal information in its possession or control, including information that has been transferred to a third party for processing.

ComplyWorks will use contracts or other means to provide an appropriate level of protection when a third party processes information on behalf of the company. ComplyWorks will, from time to time, establish procedures to implement its commitment to privacy, including:

- Procedures to protect personal information.
- Procedures to receive and respond to complaints and inquiries.
- Communications and training programs to provide information to ComplyWorks staff about privacy policies and practices.

2. IDENTIFYING PURPOSES:

ComplyWorks identifies the purposes for which personal information is collected at or before the time the information is collected, and documents those purposes.

ComplyWorks collects only that information necessary for the purposes that have been identified.

ComplyWorks specifies (verbally, electronically or in writing) and explains the identified purpose(s) to the individual at or before the personal information is collected.

When personal information is collected for a purpose not previously identified, the new purpose is communicated to the individual prior to use. In such cases, the consent of the individual is required before the information is re-used.

ComplyWorks collect personal information from individuals in order to:

- Collect customer contact information in order to manage customer accounts
- Collect potential customer contact information in order to follow-up with these individuals to determine their interest in the products and services provided by ComplyWorks as well as to inform them of new products, services or promotions.
- Screen individuals for employment, volunteer or contracting suitability.
- Manage and administer personnel (including performance appraisal, security and access control and discipline).
- Manage and administer compensation and benefits programs.
- Administer payroll.
- Administer occupational health and safety programs.
- Monitor and track skills and competency development.
- Meet legal and regulatory requirements (e.g. Employment Standards Legislation, Canada Customs and Revenue Agency reporting requirements).
- Facilitate ComplyWorks audits when required to do so.
- Provide contact information of ComplyWorks staff and volunteers to ComplyWorks insurers.
- Provide such information as may be required for administration of ComplyWorks programs..

ComplyWorks is not responsible for the management of Personal Information collected by its customers through use of ComplyWorks products and services. For information on the privacy, protection and management of this information, applicants must contact these organizations directly. However, ComplyWorks employs reasonable measures to ensure the safety and protection of its customers' information by employing policies and procedures for the safety and protection of this information. These measures are outlined in the contracts signed by customers of ComplyWorks. Furthermore, ComplyWorks considers all information collected by its customers as strictly confidential and does not access or use its customer's information other than for data maintenance, auditing or trend analysis to provide feedback and benchmarking purposes.

3. CONSENT:

ComplyWorks uses reasonable efforts to ensure that individuals understand how their personal information will be used. ComplyWorks obtains consent as required for the collection, use and disclosure of personal information, except where inappropriate.

When determining the form of consent, ComplyWorks considers the sensitivity of the information and the reasonable expectations of the individual. Express consent will be obtained when the information is likely to be considered sensitive; implied consent may be appropriate when information is less sensitive. Consent may also be given through an individual's authorized representative (such as a legal guardian or a person having power of attorney).

ComplyWorks obtains consent for the collection, use or disclosure of information through various means, including verbal, written (e.g. signed forms) or electronic processes.

In rare circumstances, ComplyWorks may collect and use personal information without the individual's knowledge or consent. For example:

- If it is clearly in the interests of the individual and consent cannot be obtained in a timely way (e.g. when the individual is seriously ill).
- If obtaining prior consent would defeat the purpose of collecting the information (e.g. in the investigation of alleged criminal activity).
- In the case of an emergency where the life, health or security of the individual is threatened.

ComplyWorks generally seeks to obtain consent at the same time personal information is collected. ComplyWorks may, however, seek consent to use and disclose personal information after it has been collected, but before it is used or disclosed for a new purpose (e.g. before disclosing board member information to a funding organization if this purpose was not previously contemplated).

Consent may be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice. ComplyWorks and/or the Privacy Officer informs individuals of the implications for withdrawing consent.

4. LIMITING COLLECTION:

ComplyWorks limits the amount and type of personal information collected to that which is necessary for the identified purpose.

ComplyWorks collects information by fair and lawful means.

ComplyWorks may collect the following information from employees and contractors:

- demographic and contact information including home address and telephone number, date of birth, and social insurance number.
- training, experience and skills as necessary to establish competence, and regulatory, employer or industry standards compliance.
- education and employment history.
- banking or financial information.
- health information.
- security background checks, as required.

ComplyWorks may collect the following personal information from customers of ComplyWorks:

- names and contact information, including home address and telephone numbers.
- HSE system and performance documentation, interview records, client employee HSE system compliance assessments, equipment assessments, COR audits, and any other relevant audit documentation.
- demographic information about customer(s) for ComplyWorks programs, including number and ages of employees interest in programs or facilities for system planning purposes.
- financial information, if members involved in programs with financial eligibility requirements, or where payment is required for programs or services.
- limited medical information for members or employees of members participating in business activities.

ComplyWorks may collect personal information through the following means:

- solicited and unsolicited resumes and correspondence
- completed application forms (paper or on-line format) for employment, benefits, grants and bursaries, volunteer opportunities, business and other program registrations, etc.
- worksite audits, inspections and assessments in person and through telephone interviews.
- on-line forms through the website.

5. LIMITING USE, DISCLOSURE AND RETENTION

ComplyWorks does not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Notwithstanding the above, ComplyWorks may disclose personal information without consent:

- to a lawyer representing ComplyWorks.
- to a company or individual employed by ComplyWorks to perform functions on its behalf (e.g. outsourced information processing function, administration of health services plan).
- in order to collect a debt owed by the individual to ComplyWorks.

- to comply with a subpoena, warrant, or court order, as required or authorized by law (e.g. Employment Standards Legislation).
- when the information is publicly available (e.g. telephone directory information), to a public authority in the event of imminent danger to any individual.

ComplyWorks obtains consent for all other disclosures of personal information for purposes other than those for which the information was initially collected (e.g. to provide references regarding current or former employees. ComplyWorks does not require consent to confirm an individual's employment record (e.g. confirm years of employment, and position held)).

Only ComplyWorks employees, contractors or volunteers with a business need-to-know, or whose duties so require, are granted access to personal information.

ComplyWorks has developed guidelines and implemented procedures with respect to the retention of personal information. ComplyWorks retains personal information only as long as it is necessary for the identified purpose, or as required by law. Where personal information is used to make a decision about an individual, ComplyWorks retains the information, or the rationale for making the decision, long enough to allow the individual access to the information after the decision has been made.

Personal information that is no longer required to fulfill the identified purposes or required by law to be retained is destroyed, erased or made anonymous.

6. ACCURACY

ComplyWorks provides our best efforts to ensure that personal information collected, used and disclosed is as accurate, complete and up-to-date as necessary for the intended purpose.
Personal information is kept sufficiently accurate, complete and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the subject individual.

ComplyWorks updates personal information as and when necessary to fulfill the identified purpose or upon notification by the individual who is the subject of the information.

7. SAFEGUARDS

ComplyWorks protects personal information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction, regardless of the format in which it is held.

ComplyWorks has developed and implemented information security policies and procedures that outline physical, organizational, and technological measures in place to protect personal information as appropriate to the sensitivity of the information. These same measures are employed in the safeguarding and protection of information resources of ComplyWorks customers.

ComplyWorks protects personal information disclosed to, or processed by third parties by contractual agreements which address the following as necessary:

- identifying the types of records provided, collected, created, or maintained in order to deliver the service, and specifying any applicable privacy legislation;
- stipulating the confidentiality of the information and the purposes for which it is to be used;
- identifying the organization(s) having custody and control of the records, including the responsibility and process for handling requests for access to information;
- ensuring that third parties and their employees having access to ComplyWorks and information assets are aware of, and understand their responsibility to adhere to ComplyWorks information handling and security policies, including maintaining the confidentiality of personal information;
- ensuring that ComplyWorks has access to information produced, developed, recorded or acquired by third parties as a result of the contract, including timely access in response to requests for information, and specifying that third parties shall not deny access to, or retain custody of, personal information because of late or disputed payment for services;
- requiring third parties to report breaches of confidentiality and privacy to ComplyWorks Privacy Officer within 48 hours of knowing that the breach occurred;
- addressing disaster recovery and backup of any information assets and systems in the custody of the third party;
- addressing the disposition (e.g. destruction or return) of all of ComplyWorks information assets (e.g. records, hardware, system documentation) upon termination of the contract;
- specifying any audit or enforcement measures that ComplyWorks will undertake to ensure that third parties comply with information handling and security provisions outlined in contractual agreements (for example, non-disclosure agreements, audit trails, regular review of third party access requirements, inspection of third party premises).

ComplyWorks ensures that all employees and volunteers are aware of its privacy policies and procedures, and understand the importance of maintaining the confidentiality of personal information.
01254
Care shall be taken in the disposal or destruction of personal information to prevent unauthorized parties from obtaining access to the information.

8. OPENNESS

Upon request, ComplyWorks makes available specific information about its policies and practices relating to the management of personal information, including:

- the means of gaining access to personal information held by ComplyWorks; identification of personal information held by ComplyWorks, and a general account of its use;
- ComplyWorks Privacy Policy, Guidelines and related procedures are posted and available on our website; reference to the statement of ComplyWorks Privacy Policy on ComplyWorks website, if applicable.

To make an inquiry or lodge a complaint about ComplyWorks personal information handling policies and procedures, contact:

ComplyWorks Privacy Officer
Suite 600, 4838 Richard Rd SW |
Calgary AB Canada
T3E 6L1
info@complyworks.com

9. INDIVIDUAL ACCESS

Upon request, ComplyWorks provide individuals with access to their personal information held by the company. Individuals have the right to challenge the accuracy and completeness of their personal information held by ComplyWorks, and to have it amended as appropriate.

All requests by individuals (e.g. customers, employees, volunteers, contractors) to access their personal information held by ComplyWorks, or to correct or amend their personal information, should be directed to the designated Privacy Officer. Such requests should be in writing.

ComplyWorks responds to requests for access to personal information within 30 business days.
Responding to an individual's request for information is usually done at no or minimal cost to the individual. However, a fee for reasonable costs incurred may be charged when responding to more complex requests, provided the individual is informed in advance.

In order to safeguard personal information, ComplyWorks may request sufficient information from the individual to verify that person's identity.

Limitations to Individual Access
ComplyWorks provides individuals access to their personal information subject to limited and specific exceptions. ComplyWorks will refuse access to personal information if:

- ComplyWorks has disclosed information to a government institution for law enforcement or national security reasons;
- it would reveal personal information about a third party unless there is consent or a life-threatening situation;
- doing so could reasonably be expected to threaten the life or security of another individual;
- the disclosure would reveal confidential commercial information; or
- the information is protected by solicitor-client privilege.

If access to information is refused, ComplyWorks shall, in writing, inform the individual of the refusal, the reason(s) for the refusal, and any recourse the individual may have to challenge ComplyWorks decision.

Correction/Amendment of Personal Information

ComplyWorks corrects or amends personal information as required when an individual successfully demonstrates the inaccuracy or incompleteness of the information. Amendment may involve the correction, deletion, erasure, or addition to any personal information found to be inaccurate or incomplete.

Any unresolved differences as to accuracy or completeness shall be noted in the individual's file. Where appropriate, ComplyWorks shall inform any third parties having access to the personal information in question as to any amendments, or the existence of any unresolved differences between the individual and ComplyWorks.

10. CHALLENGING COMPLIANCE

ComplyWorks investigate all complaints concerning compliance with its Privacy Policy, guidelines and practices, and responds within 30 days of receipt of a complaint. If a complaint is found to be justified, ComplyWorks takes appropriate measures to resolve the complaint including, if necessary, amending its policies and procedures. Individuals shall be informed of the outcome of the investigation regarding their complaint.

Complainants may address inquiries or complaints concerning compliance with these policies or guidelines by contacting ComplyWorks Privacy Officer as set out in these Guidelines under Principle 8 (Openness). A complaint may also be addressed in writing to the Privacy Commissioner of Canada at 112 Kent Street, Ottawa, Ontario, K1A 1H3 -or- to the Office of the Information and Privacy Commissioner of Alberta, #410 - 9925 - 109th Street, Edmonton, AB, T5K 2J8, 780-422-6860, www.oipc.ab.ca.