WCB Personal Information Privacy Policy

Effective: December 31, 2012

Approved by: Leo McKenna, CFO

1. PREAMBLE

The WCB of Nova Scotia (the 'WCB") collects, uses and accesses personal information under the authority of the *Freedom of Information and Protection of Privacy Act* ("FOIPOP") and the *Workers' Compensation Act* (the "Act"). This information is used only to administer the provisions of the *Act*, or a purpose consistent with the *Act*. This includes, but is not limited to, the following:

- determining eligibility for, and providing, WCB benefits and services to injured workers (e.g. managing RTW, rehabilitation, calculating and paying benefits);
- administering and managing services provided to injured workers, including paying, charging, billing, and collecting overpayments;
- maintaining WCB employee personnel records, payroll and benefits information (including compensating WCB staff), and financial management information systems; and
- maintaining employer firm level and accident experience data.

The WCB is committed to maintaining the privacy and confidentiality of the information it collects, protecting the privacy of our clients, and preventing privacy breaches. The WCB believes that one privacy breach is one too many, and we strive to improve our breach prevention performance. When collecting, using and disclosing personal information, the WCB upholds the principles of the Canadian Standards Association Model Code for the Protection of Personal Information as adopted by WCB program policy *10.3.10 Corporate Information Protection Policy*.

2. PURPOSE

The WCB protects the information it collects and only discloses it as permitted by law. This policy is designed to ensure the WCB meets its obligations:

- in the collection, protection, retention, use and disclosure of the personal information obtained by the WCB in the course of performing its operations as authorized by law; and
- in protecting personal information by making reasonable arrangements (e.g. security, administrative, contractual agreements) against such risks as unauthorized access, collection, use, disclosure or disposal.

3. DEFINITIONS

In this policy:

"confidentiality" means the obligation of an individual, organization or custodian to protect the information entrusted to it and not misuse or wrongfully disclose it;

"employee" means all employees of the WCB and includes members of the Executive and members of the WCB Board of Directors;

"personal information" as defined in FOIPOP, is recorded information about an identifiable individual. This includes:

- the individual's name, address or telephone number,
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

- the individual's age, sex, sexual orientation, marital status or family status,
- an identifying number, symbol or other particular assigned to the individual,
- the individual's fingerprints, blood type or inheritable characteristics,
- information about the individual's health-care history, including a physical or mental disability,
- information about the individual's educational, financial, criminal or employment history,
- anyone else's opinions about the individual, and
- the individual's personal views or opinions, except if they are about someone else.

“Privacy Advisory Committee (PAC)” is a WCB cross departmental committee that assesses the state of privacy within the organization by reviewing privacy breaches, root causes and trends. PAC acts as privacy champions by capturing learnings and developing advice and recommendations to help prevent future breaches and improve organizational privacy practices.

For the purposes of this policy, the term “Manager” refers to an employee’s immediate superior and includes the position titles “Manager”, “Director” and “Vice President.”

4. POLICY APPLICATION

This policy applies to:

- all employees of the WCB of Nova Scotia; and
- all information in the custody and control of the WCB of Nova Scotia.

5. POLICY STATEMENTS

5.1 Accountability

Protecting the personal information the WCB collects is a shared responsibility. All WCB employees are accountable to maintain the confidentiality of the information collected as part of the administration of the *Act* and protect the privacy of our clients.

The Chief Executive Officer (CEO) of the WCB is ultimately accountable for the WCB’s compliance with privacy legislation and policy.

WCB Legal Counsel (FOIPOP Administrator), under the general oversight of the Vice President responsible for Corporate Services, is responsible for the management of the WCB’s Privacy Program. The WCB’s Privacy Program includes, but is not limited to:

- privacy policy, procedure, and guideline development;
- privacy education and training;
- privacy inquiries and complaints;
- provision of advice and guidance to employees on privacy matters;
- promotion of a privacy culture within the WCB, the Workplace Safety and Insurance System, and third party partners.

Managers are responsible for ensuring employee compliance with applicable privacy law, policies, procedures, and guidelines.

5.2 Privacy Framework

The WCB collects, accesses, stores, uses, and discloses information as authorized by law (including WCB program policy). These laws and policies include, but are not limited to, the following:

- *The Workers' Compensation Act*;
- *The Freedom of Information and Protection of Privacy of Act*;
- *The Privacy Review Officer Act;*
- *The Personal Information International Disclosure Protection Act*;
- *10.3.10 Corporate Information Protection Policy;*
- *10.3.5 Access by Employers to Information Contained in Clients' Claim Files.*

The WCB shall establish (and WCB employees will follow) procedures, protocols, and guidelines to support maintaining confidentiality of information and the protection of privacy including, but not limited to, the following:

- Privacy Breach/Complaint Protocol;
- E-mail usage guidelines;
- The establishment of a Privacy Advisory Committee; and
- Routine Access Guidelines.

5.3 Consent and Accuracy

Where not already authorized by law or WCB program policy, the WCB will obtain the consent of the person the information is about prior to collecting, accessing, storing, using, or disclosing their personal information.

The WCB makes efforts to keep the personal information it collects as accurate, complete, and up-to-date as possible at the time of collection, and as is necessary for the purposes for which it is used. The WCB will correct or annotate records where appropriate to ensure the accuracy of the information. The operational procedure *Change of Worker Personal Information* provides guidance to WCB employees.

Injured workers (or others persons whose personal information the WCB has collected), have the right to request access to the information we hold about them, and have it updated or amended as appropriate.

5.4 Safeguards

The WCB protects the information we collect by putting in place safeguards and procedures to prevent unauthorized access, collection, use, disclosure, and disposal of information. These include administrative, technical and physical safeguards to protect information from loss, misuse, unauthorized access, disclosure and destruction. These safeguards include, but are not limited to, the following:

- Working with service providers, System Partners, stakeholders, and injured workers to limit the collection of personal information to only that which is necessary to administer the *Act* or for a similar purpose;
- Limiting access to employees who are required to have access to carry out their jobs;
- Building security;
- Privacy training for all employees;
- Prior to discussing an injured worker's claim details with an individual or an employer's business information over the phone, WCB employees take steps to verify that they are speaking with the injured worker in question, their authorized representative, or the employer's representative. The operational procedure *External Telephone Inquiries* provides guidance on verifying the identity of persons making inquiries.
- All WCB employees are required to sign a Confidentiality Agreement upon being hired, receive a copy of this policy, and participate in annual privacy training;
- Password protection, encryption and firewalls on computers; and
- Procedures, practice directives, and approvals related to the transfer of personal information via:
    - Fax (operational procedure *Faxing Personal Information);*
    - E-mail (*E-mail Usage Guidelines*);

- the removal of personal information from the country by WCB employees and/or remote access to the WCB computer network while out-of-country.

5.5 Information Sharing Agreements

The WCB, under authority of *FOIPOP* and the *Act*, may enter into information sharing agreements with government departments or agencies, associations, or research entities. Where the WCB enters into such an agreement, the WCB will require (to the extent of our legal authority) that the party to the agreement have adequate safeguards in place to protect information arising, obtained or compiled in connection with the performance of the agreement from inadvertent disclosure.

5.6 Service Providers

The WCB, under authority of the *Act* and *FOIPOP*, is permitted to enter into contracts with service providers to administer the provisions of the *Act*. In doing so, the WCB may disclose personal information to service providers if it is for a purpose for which it was collected or a use compatible with that purpose. The WCB requires these service providers comply with WCB privacy policies and *FOIPOP*.

5.7 Privacy Risk Assessment

The WCB will consider the risks to, and impact on, the personal information it collects and handles when undertaking:

- projects;
- new programs or services;
- significant changes to existing programs or services;
- new (or revised) agreements or contracts with external associations, agencies, bodies, or persons; and
- new or significant changes to existing security mechanisms used to manage and control access to personal information.

The Privacy Risk Assessment Tool (PRAT) (guide in Appendix A) will assist in determining whether or not there are privacy risks created by the undertakings listed above. Where privacy risks are identified, the party responsible for the coordination/management of the undertaking will consult with WCB Legal Counsel (FOIPOP Administrator) to identify whether or not further investigation of the risks (e.g. completion of a Privacy Impact Assessment) is required and/or the development of mitigation strategies.

Risk mitigation activities will be implemented that are appropriate to the nature and level of privacy risks identified.

5.8 Transparency

The WCB will post the *Worker's Guide to Privacy Protection at the WCB* and related information on the WCB website. As well, the WCB will provide copies of its privacy policy and associated policies/guidelines to any person who requests them. The information made available will include:

- the name or title, and the contact information for the WCB Legal Counsel (FOIPOP Administrator) and any other individuals responsible for managing privacy in the WCB; and
- the procedures, processes, or policies for gaining access to information.

Injured workers may request a copy of their claim file. Requests will be responded to in accordance with Section 193 of the *Act,* program policies *Photocopying of Clients' Files* 10.3.4 and *Access by Employers to Information Contained in Clients' Claim Files* 10.3.5.

Employers' requests for injured worker claim file documents will be responded to in accordance with Section 193 of the *Act*, program policy 10.3.5 *Access by Employers to Information Contained in Clients' Claim Files*; and operational procedure *Access by Employers to Information Contained on a Worker's Claim File*.

5.9 Complaints

Injured workers, WCB employees or members of the public have the right to make a complaint to the WCB about the way the WCB has handled the personal information we collect. Complaints will be responded to in accordance with the WCB's *Privacy Breach and Complaint Protocol*. If they are not satisfied with the WCB's response to the complaint, they have the right to file a complaint with the Nova Scotia Privacy Review Officer.

6.0 Inquiries

Please direct questions about this policy to WCB Legal Counsel (FOIPOP Administrator) or their designate.

APPENDIX A

WCB Privacy Risk Assessment Tool (PRAT)

WCB Responsibility to Protect Personal Information

"Personal information," as defined in FOIPOP, is recorded information about an identifiable individual. This includes:

- the individual's name, address or telephone number,
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- the individual's age, sex, sexual orientation, marital status or family status,
- an identifying number, symbol or other particular assigned to the individual,
- the individual's fingerprints, blood type or inheritable characteristics,
- information about the individual's health-care history, including a physical or mental disability,
- information about the individual's educational, financial, criminal or employment history,
- anyone else's opinions about the individual, and
- the individual's personal views or opinions, except if they are about someone else.

The personal information of injured workers or employees is not the WCB's personal information, and does not belong to the WCB. The WCB collects the information for the purpose of carrying out our obligations under the *Workers' Compensation Act*. We must abide by the WC and FOIPOP Acts when collecting, using, handling, sharing, transmitting, or disclosing this personal information. We have a legal and ethical responsibility to take all reasonable steps to ensure the **undertakings** we initiate do not place the personal information of injured workers or employees (or anyone) at undue risk.

What is an "undertaking"?

An undertaking includes:

- projects;
- new programs or services;
- significant changes to existing programs or services;
- new (or revised) agreements or contracts with external associations, agencies, bodies, or persons; and
- new or significant changes to existing security mechanisms used to manage and control access to personal information.

Examples of undertakings that may create privacy risks include (but are not limited to) staff relocations, changes to WCB data systems (AS400, E-file, accounting systems, phone systems), new/revised program or administrative policies, new/revised procedures or business processes, business plans, social marketing proposals, and draft regulatory/legislative changes.

What is PRAT?

The WCB Privacy Risk Assessment Tool (PRAT) is a series of questions designed to assist you in identifying and assessing any privacy risks associated with your undertaking. The goal is to ensure that all appropriate steps are taken to contribute to the protection of personal information and the prevention of privacy breaches.

A PRAT should be completed at the onset of any undertaking once the objectives are known, in order to initially identify and consider potential privacy risks. Note that it may be appropriate to complete additional PRATs at various points during an undertaking, should the nature of work, deliverables, actions or outcomes evolve over the course of the undertaking. For example, if the undertaking is a project which involves the design and implementation of a new information system, it may be appropriate to complete a PRAT as part of the planning stage (e.g., Project Objectives Document development), during/following the design phase, and again during implementation to ensure that all emerging privacy risks are considered and mitigated.

If you answer "yes" to any of the questions in the PRAT, you (the party responsible for the coordination/management of the undertaking) will consult with the WCB's Privacy Coordinator and/or WCB Legal Counsel (FOIPOP Administrator) to identify whether or not further investigation of the risks is required and possible mitigation strategies that may be appropriate.

Where it is determined the privacy risks of an undertaking are substantive and/or far reaching a **Privacy Impact Assessment** (PIA) may be required. A PIA is a comprehensive due diligence exercise used to identify, document and address potential privacy risks for the undertaking.

PRAT Process

Below is a guide to filling out a PRAT. At the end of the guide is a link to a blank PRAT template for use with your undertaking or project.

Completed PRATs are to be signed by those accountable for preparing the information, and those responsible for making decisions or recommendations related to their outcomes. This is the case even if there are not any "yes" answers to the PRAT questions, in order to maintain documentation of the consideration of privacy risks from the undertaking. Signed PRATs should be kept with other project or undertaking documentation, with an electronic copy submitted to Legal Services for archive (privacy@wcb.gov.ns.ca).

WORK SAFE. FOR LIFE.
WORKERS' COMPENSATION BOARD OF NOVA SCOTIA

Guide to the WCB Privacy Risk Assessment Tool

Name of undertaking:

Description of undertaking:

Provide a brief description of the undertaking. Explain the purpose and the role personal information plays. Note whether this is a new program/service/contract/data system/procedure etc., or a modification of existing.

Risk Assessment

Key Questions	Yes	No	Supporting Information
1. Will **new types** of personal information be collected, used, viewed, transmitted stored or disclosed?			*Note: Information that is not needed for the undertaking should not be collected "just in case". There must be a reasonable link between the information collected and the objectives of the undertaking.*
2. Will personal information already provided to the WCB **be used, sent, transmitted, available to, given, or otherwise disclosed** to either internal or external parties (eg.contractors, subcontractors, service providers, employers or other third parties)? **Note:** a third party with a contract to perform services for WCB is considered an outside party.			*Note whether this transfer of data is already occurring, or is new. If it is sent to external parties – note any agreements we have with them to protect privacy.*
3. Does the project involve a **change in administrative paperwork or policy** which will impact **the way** personal information is collected, used or disclosed?			*A change in an internal business process/policy may lead to or require changes in how we collect, store, access or process personal information. Example: Development of a new form or change to an existing form and/or its internal processing.*
4. Will the requirements for retention, storage or destruction of personal information be new or different?			*Example: An information exchange agreement with another agency requires the WCB destroy (or retain) personal information on a different timeline or in a different way.*

5. Will personal information be **linked, matched, merged or combined** with other personal information?			*Example: New database structure or files may be created by collecting and adding new information to an existing database. This could have implications for accuracy, storage, access, safeguards, etc. of the personal information.*
6. Will **access to personal information** collected or stored as part of the undertaking be provided or available to individuals who do **not** currently require access as part of their job duties/contracted role?			*Remember to consider project staff access to personal information as they carry out project responsibilities, as well as end user access to personal information once the project, program, process etc. has been implemented.*
7. Will **access to a system or database** be expanded or rolled out beyond current parameters, controls, levels, or number of users?			*If the undertaking will result in new users and/or access parameters to a database, describe who and how.*
8. Will there be any changes to the security, accessibility (locations and/or users), or use of a software, hardware or operating system or program?			*List any changes (e.g. security levels).*

IF YES TO ANY OF THE ABOVE QUESTIONS:

Risk Mitigation Activities

For each question with a "Yes" in the above checklist, describe the intended risk mitigation strategies that will be implemented.

Privacy Impact Assessment (PIA) Required?

☐ **Yes** ☐ **No**

Consult with the WCB Privacy Coordinator and/or Legal Counsel (FOIPOP Administrator) to discuss the initially identified risks and mitigation plans. Based on the level of risk(s), it may be determined that a PIA is required. Document the rationale for whether or not a PIA is required and record the proposed schedule/timeline for PIA completion (the PIA should be considered as a deliverable associated with the undertaking).

SIGN OFF:

Initiative/Undertaking Lead	Date
Legal Counsel	Date
Department Director or Project Sponsor	Date

Regardless of whether or not undertakings trigger privacy risks (i.e., any "Yes" answers in checklist), or will require a PIA, completed PRATs must be reviewed & signed off on by the parties above as documentation of the consideration of privacy risks as part of your undertaking. Forward all completed and signed PRATs to Legal Services – privacy@wcb.gov.ns.ca