Personal Privacy Model Policy

1. **PRIVACY LAW COMPLIANCE**

XYZ Company's policy is to comply with the privacy legislation of each province and territory. Because employee privacy rights vary from jurisdiction to jurisdiction, some of the rights, obligations and procedures set out in this Privacy Policy may not apply the same way—or apply at all—to XYZ Company employees working in certain locations and/or conducting certain operations.

This privacy policy has been developed to comply with Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"). PIPEDA sets out rules for the collection, use and disclosure of personal information in the course of commercial activity as defined in the Act.

- **The Ten Principles of PIPEDA summarized that are the basis of this Policy are:**

1. **Accountability:** organizations are accountable for the personal information they collect, use, retain and disclose in the course of their commercial activities, including, but not limited to, the appointment of a Chief Privacy Officer;
2. **Identifying Purposes:** organizations are to explain the purposes for which the information is being used at the time of collection and can only be used for those purposes;
3. **Consent:** organizations must obtain an Individual's express or implied consent when they collect, use, or disclose the individual's personal information;
4. **Limiting Collection:** the collection of personal information must be limited to only the amount and type that is reasonably necessary for the identified purposes;
5. Limiting Use, Disclosure and Retention: personal information must be used for only the identified purposes, and must not be disclosed to third parties unless the Individual consents to the alternative use or disclosure;
6. **Accuracy:** organizations are required to keep personal information in active files accurate and up-to-date;
7. **Safeguards:** organizations are to use physical, organizational, and technological safeguards to protect personal information from unauthorized access or disclosure.
8. **Openness:** organizations must inform their clients and train their employees about their privacy policies and procedures;
9. **Individual Access:** an individual has a right to access personal information held by an organization and to challenge its accuracy.
10. **Provide Recourse:** organizations are to inform clients and employees of how to

bring a request for access, or complaint, to the Chief Privacy Officer, and respond promptly to a request or complaint by the individual.

2. **DEFINITIONS**

- **“Personal information”** means any information about an employee. It includes, without limitation, information relating to identity, nationality, age, gender, address, telephone number, email address, Social Insurance Number, date of birth, marital status, education, employment health history as well as certain personal opinions or views of an Individual.
- **“Business information”** means confidentiality of business information will be treated with the same security measures by XYZ, as is required for employee personal information under PIPEDA.

3. **LEGISLATION**

Personal Information Protection and Electronic Documents Act PIPEDA (Canada)

4. **SCOPE**

This statement of policy and procedure applies to all non-union employees.

5. **EMPLOYEE PERSONAL INFORMATION**

XYZ Company collects and maintains different types of personal information concerning employees, including the personal information contained in:

- Resumes and job applications;
- References and interview notes;
- Photographs and video;
- Letters offering and accepting employment;
- Mandatory policy acknowledgement sign-off sheets;
- Payroll information; including but not limited to social insurance number, pay cheque deposit information, and GRRSP/ESP information;
- Wage and benefit information;
- Forms relating to the application for, or in respect of changes to, employee health and welfare benefits; including, short- and long-term disability, medical and dental care; and
- Beneficiary and emergency contact information.

XYZ Company also collects personal information such as names, home addresses, phone numbers, personal email addresses, dates of birth, employee identification numbers and marital status, and any other information necessary to XYZ Company’s business purposes, which is voluntarily disclosed in the course of an employee’s application for and employment with XYZ Company.

From time to time, XYZ Company may receive personal information about employees collected from third parties in the course of business interactions. In those circumstances, XYZ Company will take reasonable steps to ensure that those third parties have the right to disclose employee personal information to XYZ Company.

6. **PURPOSE OF COLLECTING EMPLOYEE PERSONAL INFORMATION**

XYZ Company uses, collects, and discloses personal information about employees for business purposes, including:

- Establishing, managing, or terminating your employment.
- Deciding if you're eligible to be offered a job, including verification of your references and qualifications.
- Administering pay and benefits.
- Processing employee work-related claims (e.g. workers' compensation, insurance claims, etc.).
- Establishing training and/or development requirements.
- Conducting performance reviews and determining performance requirements
- Assessing qualifications for a particular job or task.
- Gathering evidence for disciplinary action or termination.
- Establishing a contact point in the event of an emergency (such as next of kin).
- Complying with applicable labor or employment laws.
- Compiling directories.
- Ensuring the security of company-held information; and
- Other purposes as are reasonably required by XYZ Company.

7. **USE OF PERSONAL EMPLOYEE INFORMATION**

Personal information will be used for only those purposes to which the employee has consented. XYZ Company is generally not required by privacy laws to get consent to collect, use or disclose personal information for the purpose of establishing, managing or terminating your employment.

8. **EMPLOYEE CONSENT NOT REQUIRED**

XYZ will use personal information **without** the individual's consent, where:

- the organization has reasonable grounds to believe the information could be useful when investigating a contravention of federal, provincial, or foreign law, and the information is used for that investigation.
- an emergency exists that threatens an individual's life, health, or security.
- the information is for statistical study or research.
- the information is publicly available.
- the use is clearly in the individual's interest, and consent is not available in a timely way.
- knowledge and consent would compromise the availability or accuracy of the information.
- collection is required to investigate a breach of an agreement.
- to comply with valid legal processes such as search warrants, subpoenas, or court orders.
- as part of XYZ Company's regular reporting activities; and
- to protect the rights and property of XYZ Company.

9. **CONSENT WITHDRAWAL BY EMPLOYEE**

An employee, at any time, may withdraw consent subject to legal, contractual, and reasonable notice. All communications withdrawing or varying the terms and conditions of consent must be in writing and addressed to the appropriate employer authorities.

10. **EMPLOYEE MONITORING**

The work output of XYZ Company employees, whether in paper record, computer files, or any other storage format belongs to XYZ Company. Such work output and the tools used to generate it are always subject to review and monitoring by XYZ Company **and employees should not have any expectation that this constitutes employee private information.**

In the course of conducting business, XYZ Company may monitor employee activities on our premises by installing surveillance cameras at workplaces that pose high security risks. Any such surveillance cameras are there for the protection of employees and third parties, and prevent theft, vandalism and damage to XYZ Company goods and property. In most cases, recorded images are routinely destroyed and not shared with third parties. **Exception**: Such records may be turned over to the police or other appropriate government agency or authority where there's suspicion of a crime or such disclosure is otherwise necessary to enforce the laws.

XYZ Company also reserves the right to monitor all employees' computer and e-mail use.

11. **EMPLOYEE PERSONAL INFORMATION SAFEGUARDS**

XYZ Company will use physical, organizational, and technological measures to safeguard personal information to only those XYZ employees, volunteers, or third parties who need to know this information for the purposes set out in this Privacy Policy.

Management and persons in authority are required to sign a confidentiality agreement binding them to maintain the confidentiality of all personal information to which they have access.

Physical Safeguards: Active files are stored in locked filing cabinets when not in use. Access to work areas where active files may be in use is restricted to XYZ Company employees only and authorized third parties.

All inactive files or personal information no longer required are shredded before disposal to prevent inadvertent disclosure to unauthorized persons.

Ensure that personal information does not get lost, or destroyed and secure personal information from unauthorized access, copying, use, modification, or disclosure.

12. **EXPIRY OF EMPLOYEE PERSONAL INFORMATION**

Except as otherwise allowed or required by law, XYZ Company shall retain employee personal information only for as long as necessary to fulfill the purposes for which collected it. Once determined that retaining information is no longer necessary, XYZ Company will destroy or erase or make it anonymous so that it can't be associated with or tracked back to employees.

13. **XYZ COMPANY´S RIGHT TO REVISE THIS PRIVACY POLICY**

XYZ Company may amend this Privacy Policy by changes to legal requirements or internal information policies and practices. Employees will be notified of any changes and receive a revised version of the Privacy Policy.

14. **ACCURACY**

XYZ endeavors to ensure that any personal information provided by the individual in his or her active file(s) is accurate, current, and complete as is necessary to fulfill the purposes for which the information has been collected, used, retained, and disclosed. Individuals are requested to notify XYZ of any change in personal or business information.

15. **OPENNESS / TRANSPARENCY**

XYZ will endeavour to make its privacy policies and procedures known to the employee via this Privacy Policy as well as the XYZ Privacy Statement.

16. **EMPLOYEE ACCESS TO THEIR OWN INFORMATION**

An employee who wishes to review or verify what personal information is held by XYZ Company, or to whom the information has been disclosed (as permitted by the Act), may make the request for access, in writing, to the XYZ Company Privacy Officer. Upon verification of the individual’s identity, the Privacy Officer will respond within 30 days.

If the employee finds that the information held by XYZ is inaccurate or incomplete, upon the individual providing documentary evidence to verify the correct information, XYZ Company will make the required changes to the individual’s active file(s) promptly.

17. **COMPLAINT PROCEDURE**

If an employee has a concern about personal information handling practices, a complaint, in writing, may be directed to XYZ Company Privacy Officer.

Upon verification of the employee identity, Privacy Officer will act promptly to investigate the complaint and provide a written report of the investigation’s findings to the employee.

Where Privacy Officer makes a determination that the employee complaint is well founded, the Privacy Officer will take the necessary steps to correct the offending information handling practice and/or revise privacy policies and procedures.

Where XYZ Company’s Privacy Officer determines that the employee complaint is not well founded, the employee will be notified in writing.

If the employee is dissatisfied with the finding and corresponding action taken by

XYZ Company Privacy Officer, the employee may bring a complaint to the Federal Privacy Commissioner at the address below:

The Privacy Commissioner of Canada

112 Kent Street

Place de Ville

Tower B, 3rd Floor

Ottawa, Ontario K1A 1H3

Toll Free 1-800-282-1376

Email notification@priv.gc.ca