Policy Name:	Confidentiality and Privacy Policy		Policy #:	001	
Approved Date:		Revision Date:			
Approved By:	[Company Name] Management				

Purpose

The purpose of this policy is to ensure the protection of sensitive information at [Company Name]. This includes proprietary business information ("Trade Secrets"), client data, and the personal and medical information of our employees. This policy establishes the rules for collecting, using, and disclosing information in compliance with Manitoba legislation.

Policy Statement

[Company Name] is committed to maintaining the highest degree of integrity and confidentiality. We recognize that in the course of business, employees will have access to sensitive information. Unauthorized disclosure of this information can damage the Company's reputation, financial stability, and the trust of our employees and clients.

We are strictly bound by the confidentiality provisions regarding medical information and safety complaints under The Workplace Safety and Health Act and The Workers Compensation Act.

Roles and Responsibilities

Employer: Responsible for, as much as is reasonably practicable:

- Establishing administrative, technical, and physical safeguards to protect confidential information (e.g., locked file cabinets, password-protected systems).
- Ensuring that the identity of any worker who raises a safety and health concern is not disclosed to anyone, except as required by law or necessary to investigate the complaint (WSH Act).
- Limiting access to employee personnel files and medical information to only those who have a legitimate work-related "need to know."
- Ensuring that any medical information received (e.g., WCB forms, sick notes) is stored separately from the general personnel file.

Supervisors: Responsible for, as much as is reasonably practicable:

- Treating all employee medical information (diagnosis, functional limitations, prognosis) as strictly confidential.
- Never disclosing the identity of a worker who reports a safety violation or harassment complaint to the rest of the team.

- Ensuring that sensitive discussions (e.g., performance reviews, return-to-work planning) are conducted in private areas.
- Collecting only the minimum amount of information necessary to manage the workforce (e.g., asking for a return date, not a specific medical diagnosis).

Employees: Responsible for, as much as is reasonably practicable:

- Keeping all proprietary business information (client lists, pricing, software, processes) confidential during and after employment.
- Refraining from accessing, reading, or sharing another colleague's private information (e.g., salary, home address, medical status) without authorization.
- Reporting any potential breaches of confidentiality or lost company devices immediately to a Supervisor.
- Not discussing internal investigations or safety complaints with uninvolved parties to preserve the integrity of the investigation.

General Procedures

A. Employee Medical Information

In accordance with The Human Rights Code and best practices derived from PHIA (Personal Health Information Act) principles:

1. **Collection**: The Company will not request a medical diagnosis. We will only request information regarding functional abilities, restrictions, and expected duration of absence.
2. **Storage**: All medical notes, WCB claim forms, and disability management plans must be stored in a secure, confidential file separate from the employee's performance/disciplinary file.
3. **WCB Claims**: Information received from the Workers Compensation Board regarding a claim is strictly confidential and may only be used for the purpose of managing the return to work.

B. Workplace Safety Complaints (Whistleblower Protection)

Under The Workplace Safety and Health Act, if an employee exercises their right to refuse dangerous work or reports a safety concern:

1. The Company will protect the identity of the complainant.
2. The name of the informant/complainant shall not be disclosed to the person against whom the complaint was made unless strictly necessary for the investigation or required by law.

C. Business and Client Information

1. Employees may not remove confidential business records (physical or digital) from the premises without express permission.
2. Upon termination of employment, employees must return all confidential documents, devices, and access keys.

Training and Communication Plan

New Hires: This policy will be reviewed and signed during the onboarding orientation.

Supervisors: Specific training will be provided to management.

Communication: A copy of this policy will be available in the Employee Handbook.

Policy Review

To ensure compliance with *The Workplace Safety and Health Act* and changing business needs, this policy will be reviewed by Senior Management in consultation with the Workplace Safety and Health Committee/Representative:

- Every three (3) years; or
- Following any significant privacy breach or incident; or
- Upon changes to relevant privacy or employment legislation.

Regulatory References

This policy is drafted in compliance with:

- *The Workplace Safety and Health Act (Manitoba)*, C.C.S.M. c. W210 – specifically provisions regarding the protection of complainant identity and confidential information.
- *The Human Rights Code (Manitoba)* – regarding the protection of privacy related to protected characteristics (disability).
- *The Workers Compensation Act (Manitoba)* – regarding the confidentiality of claim data.
- *The Employment Standards Code (Manitoba)* – record-keeping obligations.
- *Personal Information Protection and Electronic Documents Act* (PIPEDA) – as it applies to commercial activities and client data

Print Name: _____ Signature_____