## RIGHT TO INFORMATION AND PROTECTION OF PRIVACY ACT (RTIPPA)

[Organization Name] is committed to upholding the privacy of private and identifiable information

according to the *Right to Information and Protection of Privacy Act* (RTIPPA) of New Brunswick. We are committed to collecting, using, disclosing, and discarding personal information entrusted to it in a secure, private, and correct manner.

DEFINITION

The following definition has been taken directly from RTIPPA:

“Personal information” means recorded information about an identifiable individual, including but not limited to,

(a) the individual’s name,

(b) the individual’s home address or electronic mail address or home telephone or facsimile number,

(c) information about the individual’s age, gender, sexual orientation, marital status or family status,

(d) information about the individual’s ancestry, race, colour, nationality or national or ethnic origin,

(e) information about the individual’s religion or creed or religious belief, association or activity,

(f) personal health information about the individual,

(g) the individual’s blood type, fingerprints or other hereditary characteristics,

(h) information about the individual’s political belief, association or activity,

(i) information about the individual’s education, employment or occupation or educational, employment or occupational history,

(j) information about the individual’s source of income or financial circumstances, activities or history,

(k) information about the individual’s criminal history, including regulatory offences,

(l) the individual’s own personal views or opinions, except if they are about another person,

(m) the views or opinions expressed about the individual by another person, and

(n) an identifying number, symbol or other particular assigned to the individual.

POLICY

As permitted by law, [Organization Name] will gather the personal information of employees and/or clients directly from the employee and indirectly through its partners in order to offer the services that it is authorized to give. Only the personal information required during the employment relationship will be collected by [Organization Name].

Disclosure

Personal information will only be used or disclosed by [Organization Name] for the reason for which it was collected, or for a use that is consistent with that purpose.

[Organization Name] may also use or disclose your personal information for other purposes allowed by RTIPPA, such as compliance with other legislation, providing a common or integrated service, program, or activity, making a payment, or law enforcement.

Before using or sharing your personal information for any other reason, [Organization Name] must obtain your permission.

Where [Organization Name] uses third-party service providers for services such as payroll or payment processing and needs access to information about an employee or client in order to execute services on behalf of [Organization Name], strict measures and direction will be taken to secure your information.

Safeguarding Information

[Organization Name] has established physical, administrative, and technological procedures to secure personal information in its possession and prevent theft, loss, and unauthorized access, use, or disclosure. These safeguards include, but are not limited to the following:

* Creating policies and making sure that employees are aware of them.
* Limiting access to personal information only to those with a valid need to know in order to execute their job obligations.
* Ensuring electronic systems and devices are secured.
* Establishing firewalls and encryption.
* Using security features when sharing data over the internet.
* Using secured filing cabinets and keeping a safe environment.
* Monitoring of retention schedules and ensuring that personal data is safely erased or de-identified when no longer needed.

Personal information may be stored on secure on-site servers or other internally hosted technologies by [Organization Name]. It may also be retained by third parties who [Organization Name] has engaged with to assist company operations via cloud services or other technology. Except for cloud storage and retrieval, these third parties do not use or have access to personal data. To secure personal information, [Organization Name] demands that third parties follow its policies, processes, and security standards.

Access to and Correction of Personal Information

Any public record, including records containing personal information, can be requested by an employee. An employee also has the right to request that personal information in [Organization Name's] records be corrected by coordinating with [department or person-in-charge].