Newfoundland and Labrador Hydro Protection of Privacy Policy

Policy Statement

Newfoundland and Labrador Hydro (Hydro or "the Company") respects the privacy and confidentiality of personal information supplied by its clients, customers, employees and users of its internet sites. Hydro has the right to collect, use and/or disclose this information for business purposes that a reasonable person would consider appropriate in the circumstances. However, Hydro has an important obligation to take all reasonable security measures to protect personal information from loss, theft or misuse.

Purpose

The purpose of this Policy is to confirm Hydro's commitment to full compliance with the Access to Information and Protection of Privacy Act, 2015 (ATIPPA – the "Act") and to protecting, and ensuring the privacy of, all personal information it collects in the course of conducting its business activities.

Guiding Principles

Hydro is responsible for the personal information under its control and for ensuring that all such information is collected, retained, used, and protected in a manner which fully complies with the protection of privacy standards outlined in the Act.

Definitions and Terms

Collection occurs when a public body gathers, acquires, receives, obtains or compiles personal information and then creates a record of that personal information.

This includes, but is not limited to, personal information that is:

- gathered by the Company in forms, interviews or correspondence,
- provided to the Company by another public body,
- collected by a contractor or other third party on behalf of the Company,
- in correspondence received by the Company, including unsolicited records (e.g., letters,

resumes, etc.), or
- captured through print, video or audio recordings and/or through other forms of electronic media.

Personal Information is recorded information about an identifiable individual, including:

- 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 status or history, including a physical or mental disability,
- information about the individual's educational, financial, criminal or employment status or history,
- the opinions of a person about the individual, and
- the individual's personal views or opinions, except where they are about someone else.

Personal information collected and recorded by the Company includes, but is not limited to, the following:

<u>Employees:</u>

- Name
- Address
- Date of birth
- Social Insurance Number (SIN)
- Phone number(s)
- Bank account identifier(s)
- Marital status
- Race
- Emergency contact
- Employment and residency information
- Tax information
- Credit and credit card information
- Garnishments
- Performance review and disciplinary records
- In some cases proof of Canadian citizenship
- Passport number
- Driver’s license information

- Medical information, including MCP number
- Life, disability and worker's compensation application forms
- Dependent medical documentation
- Dependent and beneficiary information

Customers:

- ID numbers
- Billing and electricity consumption records
- Service and equipment
- Credit information
- Work orders and work summaries
- Service complaints
- Program participation
- Supplier performance issues
- Information required for supplier registration and for contract administration
- Other relevant information regarding the provision of electrical service

Users of Hydro Web Sites:

- Internet Protocol (IP) address
- Browser type and version
- Page(s) visited
- Date and time of page(s) visited
- Length of time on the site

Privacy Breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information. Most breaches occur when personal information is stolen, lost or mistakenly disclosed. A willful privacy breach may result in a fine of up to $10,000 or imprisonment of up to six months, or both.

Privacy Complaint means a privacy complaint filed under the ATIPPA or an investigation initiated on the commissioner's own motion under subsection pursuant to s.73(3) of the ATIPPA.

Record means a record of information in any form and includes a dataset, information that is machine readable, written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium.

Significant Harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Scope of Application

This policy applies to all employees of Hydro and its subsidiary companies, as well as directors of the company, contractors, suppliers, agents and representatives.

Standards and Requirements

The following standards are outlined in the Act and apply to Hydro's collection, use, retention and/or disclosure of personal information:

1. Accountability – the Company is responsible for personal information in its custody and/or under its control and has designated an ATIPP Coordinator to ensure its employees, contractors and consultants, are in compliance with the Act.
2. Identifying Purposes and Consent – the Company identifies to the individual the authority and purposes of the collection and use of the personal information at the time of collection and the contact information of an employee who can answer questions about the collection. The Company obtains the individual's consent to the collection of sensitive personal information and personal information collected for the purpose of disclosure outside the Company. The Company collects personal information directly from the subject of the information whenever it is feasible and appropriate to do so. When direct collection is not feasible or appropriate, the Company makes every reasonable effort to ensure the accuracy of personal information collected from third parties. Written consent is the best practice. The Company ensures that informed consent is provided by individuals and makes best efforts to ensure individuals understand in advance the purpose for collecting the information, that consent is voluntary and that it can be withdrawn at any time.
3. Limited Collection – the collection of personal information shall be limited to that which is necessary for business purposes identified by the Company. Information is to be collected by fair and lawful means. A Privacy Notice is provided to the individual at the time of collection.
4. Limited Use, Disclosure and Retention – personal information shall not be used or disclosed for purposes other than those for which is was collected, except with the informed consent of the individual or as required by law. Personal information shall be retained only for as long as necessary for the fulfilment of those purposes.

5. Accuracy – personal information should be accurate, complete and up to date as necessary for the purposes for which it is to be used.
6. Safeguards – personal information shall be protected by appropriate security safeguards based on the sensitivity of the data.
7. Openness – the Company shall make available to individuals specific information about its policies and practices relating to the management of personal information.
8. Individual Access – upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the completeness and accuracy of the information and have it amended as appropriate. When personal information is used to make a decision affecting someone, the information will be kept for at least one year so that the individual will have sufficient opportunity to access the information, if desired.
9. Challenging Compliance – an individual can challenge the Company's compliance with the Act by contacting the Office of the Information and Privacy Commissioner.

In addition to the above, the Access to Information requirements of the Act include many standards and limitations related to the disclosure of personal/private information to third parties, which include provisions that limit or prevent disclosure in cases where it may be harmful to personal privacy.

Process/Procedure

Collection of Information

A Privacy Notice must be provided to the individual at the time personal information is collected. This must include the purpose for collecting the information, the legal authority for collecting it and the title, business address and business telephone number of an employee who can answer the individual's questions about the collection. A record of the consent, including the type of consent received (written/verbal/electronic) should be maintained.

Disposal of information

Destroyed information must not be readable.

Privacy Breach

In the event of a Privacy Breach, the **Privacy Breach Protocol** must be followed. The Privacy Breach Protocol involves the following five steps:

- Step 1 – Report
- Step 2 – Contain
- Step 3 – Evaluate Risks
- Step 4 – Notify
- Step 5 – Prevent

Responsibilities

ATIPP Coordinator

An ATIPPA Coordinator, appointed by the Company's President and CEO, is responsible for:

- Ensuring through appropriate internal communications, training programs and other initiatives that employees are aware of the requirements of the ATIPPA and their privacy protection responsibilities in relation to any personal information they collect, use, maintain, protect or disclose in the course of their work;
- Providing advice and oversight in relation to the internal processes used for ensuring the protection of privacy within the Company;
- Coordinating the Company's response to any requests for access to personal information under the ATIPPA; and,
- Generally acting as the Company's single point of contact on all questions and issues related to protection of privacy.

Employees

Employees are responsible for knowing and observing the requirements of this Policy and the ATIPPA in relation to any personal information which they are responsible for collecting, using and protecting in performing their work.

Supervisors

Supervisors are responsible for:

- ensuring the proper processes and procedures are used for the collection, use, disclosure and safeguarding of any personal information that is required and

used in their respective areas of responsibility;

- ensuring employees are properly informed and trained in relation to their personal protection of privacy responsibilities, and referring any unresolved questions or concerns to the ATIPPA Coordinator;
- immediately addressing any actual or potential non-compliance with protection of privacy standards, and reporting same to the ATIPPA Coordinator; and,
- assisting the ATIPPA Coordinator as required in any third party request for access to information related to their area of operations.