1. OBJECT

The purpose of this document is to describe the terms and conditions of personal information protection applied by DUCHESNE ET FILS LTÉE (hereinafter the "Company").

The requirements of this policy apply exclusively to the Company's deemed normal business activities, carried out during its operations.

These requirements are addressed to any person who may encounter personal information, in the context of activities involving directly or indirectly the Company.

The objectives of this policy are:

- Ensure the Company's compliance with the obligations of the Act respecting the Protection of Personal Information in the private sector (C.Q.L.R., c. P-39.1, hereinafter "PSPA").
- Protect the rights of the Company's employees, customers, and partners under articles 35 to 40 of the Civil Code of Québec in terms of protection of personal information.
- Prevent risks to the availability, integrity or confidentiality of personal information held, used, or stored by the Company as part of its business activities.

This document contains Information classified as **INTERNAL.** Its content must not be broadcast or distributed outside the Company and must be subject to appropriate controls for its classification.

2. RESPONSIBILITY FOR THE POLICY

The responsibility for the implementation of this policy lies with the President and Chief Executive Officer.

The responsibility for overseeing compliance with this policy rests jointly with the Director of IT Services and the Quality Assurance Specialist (RPRP).

3. DEFINITIONS

- **Authorization:** permission to perform a specific action.
- **Confidentiality**: characteristic of an information that is accessible only by authorized people.
- **Confidential**: category of classification of high-risk information, available within the designated areas of the Company and which, if revealed, may definitively undermine the financial, judicial, physical, or moral integrity of the Company or its employees, suppliers, and customers.
- **Information classification:** the process of distributing information according to predefined categories.
- **Availability**: characteristic of an information that can be used in a timely and appropriate manner by authorized people.

- **Incidents:** any event that potentially compromises the confidentiality, integrity, availability, or which constitutes a significant deviation from the normal functions of an information system containing personal information.
- **Information:** a set of data that may be stored, processed, or communicated.
- **Integrity**: characteristic of an information that has not been altered, modified, or destroyed without authorization.
- **Internal:** classification category of medium-risk information, available within the designated areas of the company and which, if disclosed, could potentially undermine the financial, judicial, physical, or moral integrity of the company or its employees, suppliers, and customers.
- **Public:** classification category of low-risk information, available to the public and which, if revealed, does not harm the financial, judicial, physical, or moral integrity of the Company or its employees, suppliers, and customers.
- **Information system:** a set of media (physical or digital) whose function is to store, process or communicate information.
- **Third party**: a person or company that does not have a contemporary employment relationship with the Company.
- **DUCHESNE ET FILS LTÉE**: a group of the DUCHESNE ET FILS LTÉE companies and any other external company that has been acquired.
- **Personal information:** Under the Act on the Protection of Personal Information in the private sector, a personal information "is ... any information that relates to a natural person and which allows to identify that person" (C.Q.L.R., c. P-39.1, s.2).

  Personal information of an individual (consider whether the information is referred to with another information about an individual or where its mere reference would reveal the identity of the individual to whom it relates):

  - Name;
  - Social Insurance Number;
  - Driver's licence number;
  - Health insurance number;
  - Address;
  - Telephone number;
  - Service number;
  - Age;
  - Gender;
  - Race, nationality or ethnicity;
  - Religion;
  - Marital status;
  - Medical, educational or professional history;
  - Online identifiers;
  - Employee identification number;
  - Banking or credit card information;
  - Information collected allowing the identity verification involving biometrics;

- Information that allows to geolocate a person.

Several elements specific to their physical identity (including photography), physiology, genetics, psychic, health, economic, cultural, or social identity, can also add to the list.

Information that is not considered as personal information:

- Information that does not directly relate to an individual (e.g., postal code);
- Information on a company;
- Anonymized information (to the extent that it cannot be linked to an identifiable individual);
- Governmental Information.

4. RIGHTS OF INDIVIDUALS

a. The Company respects the rights of individuals with respect to the protection of personal information, within the limits of laws and regulations. Individuals have the right to:

   i. To be informed about the processing of their personal data;

   ii. To know how, when, and why their personal data is shared;

   iii. To have access to their data;

   iv. To be forgotten;

   v. To be able to receive a copy of their personal data;

   vi. Opt-out of services such as automated decision-making, receiving chain emails, and other electronic messages;

   vii. To have their data rectified if it is not accurate;

   viii. To limit the processing of their data;

   ix. To be asked for consent when personal data is disclosed or requested from third parties if it is not clearly exempted by law.

b. The Company must ensure that it appoints a person responsible for the protection of personal information who will be responsible for individual rights, processing requests and complaints with respect to personal information within the time limits prescribed by the laws and regulations in force.

c. The Company must ensure that individuals are aware that their data is being processed and that they understand how they can exercise their rights.

d. The Company ensures the secure retrieval, correction or deletion of data following receipt of a request. It could refuse a request with justification or within the limits of the Act.

e. A record of requests and complaints will be maintained.

5. PROTECTION OF PERSONAL INFORMATION PROCESS

5.1 Roles and Responsibilities

The roles and responsibilities described below are required by the PISPA. The Company therefore has an obligation to appoint persons to occupy these roles. A Protection of Personal Information Management Committee may also be established based on the legal, contractual, and contextual needs of the Company.

5.1.1 Executive authority of the Company

a. Must absolutely be the most authoritative person in the Company;

b. Implementation of policies and procedures in terms of Personal Information Protection;

c. Oversight of compliance of policies and procedures in terms of personal information protection;

d. Appointment of an Officer responsible for the protection of personal information;

e. Approval of action plans and distribution of human and financial resources.

5.1.2 Officer responsible for the protection of personal information

a. Documentation of confidentiality incidents;

b. Maintaining a logbook of confidentiality incidents;

c. Reporting accidental disclosure of personal information to the competent authorities;

d. Understanding and application of the legislation concerning protection of personal information;

e. Ongoing training and employee awareness as part of the Protection of Personal Information Program;

f. Participation in Privacy Impact Assessment (PIA) exercices;

g. Management of access to information requests;

h. Management of complaints concerning the protection of personal information.

5.1.3 Employees, suppliers and other third parties

a. Adherence to the rules of governance relating to protection of personal information;

b. Participation in the Training and Awareness Program relating to the Protection of Personal Information;

c. Reporting suspected or confirmed confidentiality incidents.

5.2 Obligations

The obligations described below are explicitly or implicitly described by the PIPA. The Company and its Protection of Personal Information Program are bound by these obligations.

5.2.1 General

a. The Company is required to appoint a person who is responsible for compliance with applicable laws related to the protection of personal information. The contact information (email and telephone) of this person is published on the Company's website(s).

b. The Company has an obligation to protect all personal information, regardless of the medium (physical or digital) or state (at rest, in transit or in use), required by one or more of its business processes.

c. The Company is required to respect all the principles of protection of personal information set out in the Protection of Personal Information Act and to demonstrate them in the context of evaluations or audits.

d. The Company has an obligation to make publicly available specific information about its policies and practices regarding the protection of personal information.

e. The Company has the obligation to make the relevant changes to its Protection of Personal Information Program according to the ratification, modification, or deletion of applicable laws, and this, as soon as possible.

5.2.2 Collection of Personal Information

a. The Company has an obligation to determine *a priori* the useful purposes of the personal information before any collection, use, communication or (non-accidental) disclosure of personal information.

b. The Company has an obligation to inform and obtain *a priori* the consent of any individual affected by a (non-accidental) collection, use, communication, or disclosure of personal information unless it is not appropriate to do so.

c. The Company is required to collect only the personal information that can be demonstrated as being useful to one or more of the Company's business processes.

d. The Company has an obligation to destroy or anonymize personal information once it is no longer necessary for the purposes for which it was collected.

e. The Company is required to disclose the existence, nature, and use of the personal information under its responsibility, to the owner of the personal information in question who requests it.

f. The Company has an obligation to allow access to the personal information under its responsibility to the owner of the personal information in question who requests it.

5.2.3 Inventory of Personal Information

a. The Company has an obligation to create, set up, document, and maintain an inventory of the personal information under its responsibility. This inventory must address the following characteristics for each of the personal information under its responsibility:

   i. Storage locations
   ii. Description of personal information
   iii. Medium used for preservation
   iv. Types of personal information
   v. Scheme of access to the personal information in question
   vi. Classification of personal information
   vii. List of controls applied to affected personal information.
   viii. Maximum shelf life
   ix. Prescribed method of destruction

b. The Company has an obligation to maintain the accuracy of the personal information contained in the inventory.

c. The Company has an obligation to maintain the accuracy of the inventory of personal information to meet legislative requirements for the use, storage, and destruction of personal information.

5.2.4 Protection of personal information

a. The Company has an obligation to establish, implement, document, and maintain a risk management process applied to the protection of personal information. This risk management process should address the following characteristics for each of the risks:

   i. Date of identification
   ii. Reporting person
   iii. Threat type
   iv. Vulnerability type
   v. Covered information assets
   vi. Risk impact measurement
   vii. Risk probability measure
   viii. Security controls in place
   ix. Identification of residual risks
   x. Security controls to be put in place.
   xi. Residual risk action plan
   xii. Responsible for the targeted risk

b. The Company is required to implement and use the necessary security controls prescribed by personal information classification level.

c. The Company has an obligation to always measure the effectiveness of the security controls in place.

d. The Company has an obligation to use and maintain the systems, technological tools, and expertise necessary to protect personal information.

e. The Company is required to create, implement, and maintain a restrictive scheme for access to personal information. This scheme must ensure that individuals only have minimal access to the personal information necessary to perform their duties, and only in a timely manner. This access scheme should address the following characteristics for each of the accesses:

   i. Individual or group to be accessed.
   ii. Personal information subject to access
   iii. Type of personal information
   iv. Type of medium containing the personal information
   v. Access type (write / read / delete)
   vi. Date of entry in service for the access
   vii. Last date of access modification
   viii. Access expiry date

5.2.5 Use of personal information

a. The Company has an obligation to ensure that personal information is not used other than in the manner declared at the time of collection.

b. The Company has an obligation not to sell, rent or trade personal information without the express consent of the owner of the personal information.

c. The Company is required to obtain the consent of the Officer responsible for the protection of personal information, prior to any internal or external disclosure of personal information.

d. The Company has an obligation to establish, use and maintain formal processes necessary for the internal and external communication of personal information. This obligation contains exceptions provided for by the laws and regulations in force.

e. The Company is required to establish, use, and maintain a list of all third parties involved in the collection, processing, or disclosure of personal information. This list should address the following characteristics for each of the third parties:

   i. Third parties subject to access
   ii. Personal information subject to access
   iii. Type of personal information
   iv. Type of medium containing the personal information
   v. Geographic location of the storage of personal information at the third party
   vi. Type of use of personal information
   vii. Access type (write / read / delete)
   viii. Date of entry in service for the access
   ix. Access expiry date

f. The Company is required to use contractual agreements with third parties governing any action affecting personal information under the Company's

responsibility. These agreements set out the obligations and responsibilities of each party.

5.2.6 Transfer of data outside of Quebec

a. The Company has an obligation to limit the transfer of personal information across borders regardless of the medium.

b. The Company has an obligation, in the event of the inevitability of a cross-border transfer of personal information, to inform the owner of the personal information and to obtain his or her *prior consent*.

c. The Company has an obligation to ensure that all legal requirements for cross-border transfers of personal information are met before a transfer takes place. A Privacy Impact Assessment (PIA) will be produced on a case-by-case basis.

5.2.7 Data portability

a. In response to a written request from the owner of the personal information, the Company is required to communicate to the owner, in a structured and commonly used technological format, computerized personal information in the Company's possession.

b. Personal information may also be disclosed to a person or organization authorized to collect the information, at the request of the owner of the personal information in question.

5.3 Consent

Before proceeding with the voluntary collection, use, communication or disclosure of personal information, the Company must obtain the consent of the owner of the personal information in question.

5.3.1 Characteristics of consent

a. The Company has an obligation to obtain clear consent: so that the potentially consenting person can clearly understand the purpose of the consent.

b. The Company has an obligation to obtain free consent: so that the potentially consenting person is not subjected to any coercion or constraint and acts of his or her own free will.

c. The Company has an obligation to obtain informed consent: so that the potentially consenting person can make a choice with knowledge of the obvious implications and consequences of his or her choice.

d. The Company has the obligation to obtain specific consent: so that the potentially consenting person can consent to a specific and clearly circumscribed purpose.

e. The Company has an obligation to obtain granular consent: so that the potentially consenting person can consent for each particular purpose.

f. The Company has an obligation to obtain understandable consent: so that the potentially consenting person can consent to simple and clear terms.

g. The Company has the obligation to obtain separate consent: so that the potentially consenting person can consent separately to any other information when the request is made in writing.

h. The Company has the obligation to obtain temporary consent: so that the potentially consenting person can consent for the time necessary to achieve the purposes for which it has been requested.

i. The Company has an obligation to provide a simple mechanism for the individual to withdraw consent at any time and for any purpose and to inform the individual of the consequences of a withdrawal. This mechanism must be accessible to all and publicized.

5.3.2 Consent of minors

In Quebec, a minor is anyone **under the age of 18**.

a. If the minor is under 14 years of age, consent to the use or communication of his or her personal information must be given by the parent or holder of parental authority.

b. If the minor is 14 years of age or older, consent may be given by the minor himself or by the parent or holder of parental authority.

c. If this collection is clearly for the benefit of the minor, the Company may nevertheless proceed with this collection without parental consent.

5.3.3 Exceptions to Consent

When the health or safety of a person is threatened by an urgent and dangerous situation:

a. The Company may disclose that individual's personal information without consent to any person to whom such disclosure is to be made.

b. The Company must establish the urgency and danger of the situation for it to disclose the information without consent.

To prevent an act of violence, including suicide, the Company may:

c. Disclosing personal information without consent. However, this communication must be limited to people exposed to this danger, their representative, and any person likely to help them, such as a police officer, a suicide prevention centre, a CLSC worker, the DYP, a health professional, etc.

5.4 Other Considerations

To comply with the legal requirements of the PPIA, there are other elements to consider.

a. The Company has an obligation to establish, use and maintain an incident management process for information assets.

b. The Company is required to establish, use, and maintain a general data classification policy, including the classification of personal information.

c. The Company is required to establish, use, and maintain a policy on the management of requests and complaints regarding the management of personal information.

d. The Company is required to establish, use, and maintain a policy on training and risk awareness with respect to personal information.

6. COMPLIANCE

6.1 Compliance measures

The Company establishes this policy and ensures that it is adhered to and complied with by using:

a. Control tools

b. Internal and external audits

c. Feedback to the person responsible for the policy

6.2 Exceptions

Any exception to these guidelines must first be subject of a request in writing and approved by the Company using the appropriate documentation.

Any exception without prior approval will be treated as non-compliance with these guidelines.

6.3 Non-compliance

Anyone who deviates significantly from these guidelines may be subject to disciplinary action up to and including termination of employment.

7 REVISION

This policy will be reviewed ONCE A YEAR, or as required by contractual, legal, or contextual changes.