NORSECO R&D EXPERTISE SELECTION W.H.PERRON

9406-5299 Québec Inc.

Effective date: September 2023
Update date:

Privacy Policy

Approval

The *Privacy Policy* (the "*Policy*") was adopted as tabled by the Board of Directors of Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc. during a board of directors' meeting.

1. Objective

In the course of its operations, the *Organization* collects, uses and communicates *personal information* of employees, members, customers or partners.

The O*rganization* believes in the importance of protecting the privacy of the individuals with whom it interacts and is committed to implementing, monitoring and maintaining appropriate privacy practices.

This Policy (hereinafter the "Policy") sets out the principles and guidelines that guide Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc. (hereinafter the "*Organization"*) in the collection, use, retention and disclosure of personal information in accordance with Bill 25 on the protection of personal information. This policy applies to all employees, members, customers, suppliers and other stakeholders of the O*rganization*. It sets out the principles that the *Organization* applies when handling *personal information*, and pursues the following objectives:

- Establish a governance framework for the handling of *personal information*.
- Establish the roles and responsibilities of the stakeholders involved in applying the Policy.
- Establish guidelines for the management of personal information, which include the following:
  - Put in place organizational and technical measures to ensure the protection of data, *personal information*, all according to the risks associated with its processing.
  - Put in place mechanisms so that individuals can exercise their rights with regard to their *personal information*, and be informed accordingly.

2. Definitions, scope, compliance and exemptions

Definitions of the terms used in this Policy, i.e. words in italics and beginning with a capital letter, are given in Appendix C of this Policy.

This Policy applies to the *Organization*, i.e. all sectors of Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc. More specifically, it applies to its employees, consultants and suppliers (the "*Personnel* ") who process *personal information on* behalf of the *Organization*.

Compliance with this Policy is mandatory and the *Organization* undertakes to respect it. Any request for derogation must be duly justified and must be submitted to the *Privacy Officer.*

3. Structure of the Governance Framework

This Policy provides a framework for the *Organization's privacy* practices.
Other *Policies* and *Guidelines* documents are derived from the Policy to support it.

- The Policy sets out the vision and implements the *Privacy* principles.
  of the *Organization* and its foundations.
- To support the Policy, the *Organization* has set up *Guidelines* to document orientations, requirements and expectations, i.e. the "what to do".
- The *Organization* may establish processes, guides and procedures to provide a detailed list and sequence of activities required to implement the *Guidelines*.

As the protection of *Personal Information* requires the implementation of appropriate and adequate security measures, the Policy must also be read and interpreted in correlation with the *Organization's Information Security Policy* and its related directives.

4. Additional content to ensure the protection of personal information

In addition to the present policy, Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc. has implemented an *Information Security Policy* that plays a complementary role in ensuring respect for the protection of personal information and regulatory compliance.

To clarify certain issues and provide employees with the tools they need to ensure compliance with this Policy, the following guidelines have also been put in place.

- Directive on the transfer of personal information outside Quebec (other Canadian provinces and/or abroad).
- Directive on data retention.
- Privacy Impact Assessment Directive.
- Consent directive.
- Privacy policy – employees.
- Privacy policy – recruitment.
- Directive on third-party management.
- Directive on individual rights and complaints management.
- Directive on the Acceptable Use of Information Assets.
- Directive on the destruction, anonymization and depersonalization of personal information.

In addition to the aforementioned policies and directives, certain guides and procedures may be drawn up as required by the sectors concerned to ensure compliance with regulations.

5. Legal and regulatory considerations

The *Organization* does business in several Canadian provinces and is therefore subject to various provincial and federal privacy laws and regulations (the "*Privacy Act").*

- **At the federal level**: *The Organization* is subject to *PIPEDA* for transfers of *personal information* between Canadian provinces, as well as for other cases where provincial *privacy legislation* cannot be applied, for example, where provinces have not adopted legislation substantially similar to *PIPEDA*. The *Organization* is also subject to the Canadian Personal Information *Protection and Electronic Documents Act,* which governs, among other things, the sending of commercial electronic messages, such as e-mails designed to sell a product or service, and the installation of cookies or "tracking pixels".

- **At the provincial level:** *The Organization* is subject to the applicable *privacy* regulations of the Canadian provinces in which it carries out its activities, when these involve the *Processing* of *Personal Information*. More specifically, and without limiting the generality of the foregoing, the *Organization* is subject to *ARPPIPS*, *PIPAAB* and *PIPABC*, as well as the *ESA*.

6. Privacy Principles

The *Organization* undertakes to implement, apply and maintain the technical and organizational measures necessary for the implementation of the principles listed below that apply to the processing of Personal Information. These principles are aligned with the requirements of PIPEDA, ARPPIPS, PIPAAB and PIPABC and are known as the "10 Fair Information Principles" (the "Principles").

6.1 First principle - Responsibility

The *Organization* is responsible for the *Personal Information under* its control. It shall designate an individual who is accountable for its compliance with these principles. This person assumes the role of *Privacy Officer* in accordance with ARPPIPS and *PIPEDA*.

The Organization establishes and implements the appropriate *Documents* in order to be able to demonstrate its compliance with the *Regulations*.

6.2 Principle 2 - Identifying Purposes

The purposes for which *Personal Information is* collected shall be identified by the *Organization at* or before the time the information is collected. The *Organization* may only collect *Personal Information* that is necessary for the purposes identified, and shall collect such information by fair and lawful means.

6.3 Third principle - Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of *Personal Information,* including the collection of *Personal Information* from a third party unless inappropriate. Where Personal Information is collected, the *Organization* strives to obtain the informed, express and voluntary consent of the individual concerned, except where otherwise permitted or required by law. The *Organization may* obtain such consent from *third parties*, such as partners or suppliers.

6.4 Fourth principle - Limiting collection

The *Organization* collects personal information from its customers, suppliers, members and employees in the course of its business and operational activities. The types of information collected may include, but are not limited to, names, addresses, telephone numbers, e-mail addresses, government identification numbers, financial information and credit history.

The *Organization* only collects personal information that is necessary for the purposes for which it is collected and ensures that the persons concerned are informed at the time of collection.

The *Organization* may collect personal information from third parties, such as credit bureaus, only with the consent of the person concerned or if authorized by law.

6.5 Fifth principle - Limiting use, communication and storage

Personal Information shall only be used or disclosed for the purposes for which it was collected, unless the individual concerned has consented to a subsequent use or as required by law. The *Organization* retains *Personal Information* only as long as necessary to fulfill these purposes. Furthermore, *Personal Information is* only used by the *Organization* for ethical purposes.

The *Organization* undertakes not to use personal information for direct marketing purposes without the prior consent of the person concerned. The *Organization* may use personal information to communicate with data subjects, manage customer and supplier accounts, offer products and services, carry out market analyses and conduct satisfaction surveys.

The *Organization* may share personal information with third parties, such as service providers and business partners, only to the extent necessary to fulfill the purposes for which the information was collected or as permitted by law.

The *Organization* retains personal information only as long as necessary for the fulfillment of the purposes for which it was collected, unless a longer retention period is required or permitted by law. The *Organization* establishes appropriate retention periods for the personal information it holds. These retention periods are determined taking into account legal requirements, the purposes for which the information was collected, and the *Organization*'s operational and commercial needs. Once personal information is no longer required for the purposes for which it was collected and legally authorized, the *Organization* will take appropriate measures to securely destroy it or render it anonymous, except where further retention is required or authorized by law.

6.6. Sixth principle - Accuracy

Personal Information must be as accurate, complete and up-to-date as possible in order to meet the purposes for which it is to be used. If Personal Information held by the *Organization* is inaccurate, incomplete or out of date, the *Organization* will make the necessary corrections as soon as possible. If the *Organization* refuses a request for correction, it will inform the person concerned of the reasons for the refusal.

6.7 Seventh principle - Safety measures

Personal Information must be protected by security measures appropriate to its degree of sensitivity. To this end, the *Organization* applies an ***Information Security Policy***.

This policy states, among other things, that the *Organization* recognizes the importance of preserving the confidentiality and integrity of the personal information it holds. The *Organization* implements appropriate security measures to protect such information against unauthorized access, loss, theft, misuse, disclosure, alteration or destruction. These security measures include reasonable and appropriate physical, technical and administrative controls.

Safety measures include, but are not limited to:

- The implementation of personal information security policies and procedures to educate and train employees in the secure management of personal information.
- Limiting access to personal information to authorized employees who need it to perform their duties.
- The use of passwords, firewalls, encryption and other security technologies to protect personal information from unauthorized access.
- Regular data backup to ensure availability in the event of accidental loss or destruction.
- Continuous monitoring of IT systems and networks to detect and prevent security breaches.

Online privacy

If the *Organization* collects personal information through its website or other online platforms, it implements appropriate measures to protect the confidentiality of this information, such as SSL security certificates, firewalls and encryption protocols. The *Organization* informs users of its websites about the collection and use of personal information, cookies and similar technologies used.

In the event of a personal data breach, the *Organization* will take appropriate measures to remedy the situation. This includes prompt notification of the persons concerned, the competent authorities and, where applicable, the Office de la protection du consommateur du Québec, in accordance with the legal requirements in force.

The *Organization* is committed to ensuring that its third-party service providers, who have access to personal information in the course of their activities, comply with similar security standards. Appropriate confidentiality and security clauses are included in contracts with these suppliers to guarantee the protection of personal information.

The *Organization* encourages individuals to play an active role in protecting their personal information. It informs them of the importance of maintaining the confidentiality of their identification information, choosing strong passwords, and reporting any suspicious activity or security breach.

6.8 Eighth principle - Transparency

The *Organization* makes its Privacy Policy readily available to the public. The *Organization* may also make its other privacy policies and guidelines available to those who request them.

By implementing measures for accessing and correcting personal information, the *Organization* demonstrates its commitment to the transparency, accuracy and integrity of the personal data it holds, in accordance with the requirements of Bill 25 and the rights of individuals over their personal information.

6.9 Ninth principle - Access to *personal information*

Upon request, the *Organization will* inform any person of the existence, use and disclosure of his or her Personal Information and allow him or her access to such information. An individual may challenge the accuracy and completeness of the *Personal Information* and have it amended as appropriate.

Internal disclosure

The *Organization* is committed to limiting access to personal information to those employees who need it to fulfill their responsibilities. Internal disclosure of personal information is strictly controlled and monitored.

External disclosure

The *Organization* only discloses personal information to third parties with the consent of the individual concerned, except where required or authorized by law. When personal information is disclosed to third parties, the *Organization* takes steps to ensure that such third parties provide an adequate level of protection for personal information.

The *Organization* recognizes the right of individuals to access their personal information held by the *Organization* and to request corrections if such information is inaccurate, incomplete or out of date. To exercise their right of access or correction, individuals may submit a written or oral request to the *Organization*. This request must be accompanied by sufficient details to identify the personal information in question and to validate the identity of the applicant.

The *Organization* responds to requests for access and correction within the time limits prescribed by Bill 25. When a request for access is received, the *Organization* provides the person concerned with a copy of his or her personal information in an understandable format, unless otherwise permitted or required by law. The *Organization* ensures that procedures for accessing and correcting personal information are clear, transparent and easily accessible to the individuals concerned. It undertakes to provide adequate support and to respond to all questions and concerns related to access and correction of personal information.

6.10 Tenth principle - The possibility of lodging a complaint concerning non-compliance with the Principles

Any individual may address a challenge concerning the *Organization*'s compliance with the above principles. Complaints concerning non-compliance with these Principles should be addressed to the *Privacy Officer*.

7. Training and awareness-raising

Employee training and awareness regarding the protection of *Personal Information* are crucial to the *Organization*'s ability to ensure compliance with the Principles set out in the Policy, as well as its legal and contractual obligations regarding the protection of *Personal Information*. Accordingly, the *Organization* operates a training and awareness program. The *Organization* is committed to providing its employees with training on the protection of personal information, current legislation and related internal policies. This training is designed to make employees aware of the importance of confidentiality and security of personal information, and to provide them with the knowledge they need to handle it properly.

8. Policy maintenance

The *Organization* ensures that it maintains, measures, analyzes, evaluates and conducts periodic reviews of the Policy, related procedures and its *privacy* practices. Updates are therefore made as needed, taking into account legislative, technological and operational changes, as well as best practices in data protection. The *Organization* ensures that a *regulatory* watch is kept to take proper account of any changes in this area.

The Policy must be reviewed at least annually by the *Organization's* Audit Committee. Significant changes to the Policy shall be communicated to those concerned in an appropriate manner, and the *Organization* shall make the most recent version of the Policy available to employees in the manner deemed appropriate, as well as on its website.

9. Application

The Organization shall put in place mechanisms to evaluate the adoption and effectiveness of the Policy, its guidelines and any other documents derived therefrom. These mechanisms ensure continuous improvement in the protection of the *Organization*'s *Personal Information.*

Compliance with the Policy is mandatory for all employees. Employees who fail to comply are subject to disciplinary measures ranging from disciplinary notice to termination of employment, or to the contractual measures and penalties provided for consultants and suppliers, which may include contract termination and claims for damages. Additional training and awareness may also be provided in the event of failure to comply with the Policy.

10. Organization of the protection of personal information

10.1 Responsibilities of the *Organization's* Board of Directors

- Approve strategic orientations for the protection of *Personal Information.*
- Approve the Policy and any other important policies deriving from it, including any amendments, and support their application throughout the *Organization.*
- Stay informed of the *Organization'*s level of maturity and the risks relating to data protection. *Personal information.*
- Ensure that sufficient resources are allocated to enable the *Organization* to comply with the *Regulations on* an ongoing basis.

10.2 General Manager

The General Manager is the chief operating officer of the *Organization* and, more broadly, of the *Organization* as a whole, and as such is accountable under *ARPPIPS for the protection of the personal information* of the sectors making up the *Organization*.

The General Manager is authorized by the *Organization*'s Board of Directors to delegate all or part of this function by means of a written delegation of the *Privacy Officer* function attached as Appendix A to this Policy.

10.3 Responsibilities of the Privacy Officer

The Privacy Officer (hereinafter "the Officer") is mandated to assist the *Organization's Audit Committee* in the governance of the various issues related to the impact of the digitization of the economy on its activities with regard to the protection of *Personal Information* within the *Organization*. The Privacy Officer integrates his approach in synergy with the *Organization'*s information security and business continuity approach.

The person in charge monitors the implementation of the Policy, develops an action plan to manage risks in an organized manner, and follows up to ensure continuous improvement in the management of personal information within the *Organization*.

For the purposes of fulfilling his or her mandate, the Manager has executive and/or decision-making powers in relation to:

- Coordination of reporting, monitoring and analysis of employee compliance, for reporting to the *Organization's Audit Committee*.
- The establishment of a mechanism for assessing the *Organization'*s compliance with the *Regulations, at* the frequency and with the metrics and tolerance thresholds it determines.
- Approval and coordination of *waiver* requests.
- Coordinating responses to regulatory bodies.
- Coordinate the draft, review, approval and modification of policies, directives and any other document concerning the protection of personal information.
- The establishment of a method for documenting decisions and actions taken within the scope of its mandate, particularly with regard to risk acceptance, remediation and follow-up.
- Generally make recommendations to the *Organization's Audit Committee* on any matter falling within its mandate.

The *Privacy Officer* is also responsible to:

- Ensure compliance with and implementation of the Policy, *Guidelines* and applicable *Regulations* by putting in place the necessary mechanisms to monitor the evolution of the deployment of *privacy* practices.
- Carry out day-to-day risk management, make progressive adjustments and spot-check adherence to the Policy.
- Support the deployment of applicable *directives* by allocating human, financial and technological resources.
- Support the conduct of *Privacy Impact Assessments* in *accordance* with applicable *Directives and Regulations.*
- Report periodically to the Audit Committee on *privacy* issues and risks, including non-compliance and related action plans.
- Capture and report to the Audit Committee risks that are above the established tolerance threshold.
- Analyze and approve all *waiver* requests.
- Provide ongoing training to ensure proper performance of responsibilities.
- Any other responsibility assigned by the *Regulations* and *Directives.*

Subject to the prior approval of Executive management, the *Privacy Officer* is authorized to sub-delegate in writing, in whole or in part, his or her responsibilities to a designated person, using a document substantially similar to the Privacy Officer Sub-Delegation Document attached as Appendix «B» to this Policy.

10.4 Sector responsibilities

Each sector, in collaboration with the *Privacy Officer*, is responsible for:

- Support the Privacy Officer in reporting to the Audit Committee.
- Put in place the human, financial and technological capabilities required to implement *privacy* protection practices (the "how-to").
- Sectors are responsible for monitoring compliance with this Policy, the *Directives* and other documents derived from it, as well as with the *Regulations.*

Appendix «A»

Model

Delegation of the Privacy Officer function

WHEREAS the *Act to* modernize legislative provisions respecting the protection of personal information, LQ 2021, c. 25, assented to on September 22, 2021, brings amendments to the Act respecting the protection of personal information in the private sector, RLRQ c. P-39.1 ("**ARPPIPS**") which will come into force progressively until September 2024.

WHEREAS section 3.1 of ARPPIPS, which will come into force on September 22, 2022, makes all legal entities responsible for protecting the personal information they hold.

WHEREAS this article also specifies that the person with the highest authority within the company must ensure compliance with and implementation of the Privacy Act, and that this person is responsible for the protection of personal information.

WHEREAS within Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc., the General Manager is the person with the highest authority.

WHEREAS, the aforementioned article also provides that this function may be delegated in writing, in whole or in part, to any person.

***

Therefore, in accordance with the above provision and in my capacity as General Manager of Norseco s.e.c./ W.H. Perron / 9406-5299 Québec Inc., I hereby delegate the entire function of Privacy Officer and the related powers to Mr. Benoit Plante, IT Manager.

This delegation also includes the responsibility for Mr. Benoit Plante, *IT Manager* to report to the Audit Committee and to me, upon request, and in accordance with the *Privacy Policy*, on privacy risks within Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc.,on mitigation measures taken and on the status of related work.

The powers and responsibilities hereby delegated may also be sub-delegated in whole or in part, in writing, in accordance with the terms and conditions set forth in the ARPPIPS and subject to the prior authorization of the undersigned.

SIGNED at Laval this 28th day of September, 2023.

Christian Chartrand
General Manager

Appendix «B»

Sub-delegation of the Privacy Officer function

WHEREAS the *Act to modernize legislative provisions respecting the protection of personal information*, LQ 2021, c. 25, assented to on September 22, 2021, brings amendments to the *Act respecting the protection of personal information in the private sector*, RLRQ c. P-39.1 ("**LPRPSP**") which will gradually come into force until September 2024.

WHEREAS section 3.1 of PHIPA, which comes into force on September 22, 2022, makes all legal entities responsible for protecting the personal information they hold.

WHEREAS this article also specifies that the person with the highest authority within the company must ensure compliance with and implementation of the Privacy Act, and that this person is responsible for the protection of personal information.

WHEREAS within Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc., the General Manager is the person with the highest authority.

WHEREAS, the aforementioned article also provides that this function may be delegated in writing, in whole or in part, to any person.

WHEREAS on *[date of Initial Delegation]*, the position of Privacy Officer for Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc., and the related powers were delegated to me by *[name of signatory of Initial Delegation]* (the "Delegation").

WHEREAS, subject to the prior agreement of its signatory, the Delegation provides for the possibility of sub-delegating, in whole or in part, the powers and responsibilities attached thereto, in accordance with the PPSA.

WHEREAS on *[date authorization for sub-delegation was obtained by the signatory of the original Delegation]*, the signatory of the Delegation authorized the sub-delegation of the powers and responsibilities of the Delegation to *[first and last name of designated RPRP], as* appears from the authorization attached hereto.

***

Therefore, in accordance with the above provision and the Delegation, I delegate the following powers and responsibilities to *[full name]*:

- List of delegated powers and responsibilities

This delegation is also accompanied by the responsibility for *[name and surname of designated person]* to report to the Audit Committee and to me, upon request and in accordance with the Privacy Policy, on the risks related to the protection of personal information within Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc., on the mitigation measures taken and on the status of related work.

SIGNED at _____this _____day of _____.

_____

Name: *(last name)*
Title : *(title)*

Appendix «C»

Information assets	Any information, *data* or *metadata* held by the *Organization* (as Owner or simple possessor), regardless of its medium (paper, electronic or other), as well as *Information Systems*.
IT assets	All the *Organization*'s technological systems and equipment used to *Processing*, use, storage, retention and communication of *Information Assets.*
Privacy	*Confidentiality* is the reserved nature of an item of information or a *Treatment*, access to which is restricted to only those persons authorized to know it for the purposes of the service, or to authorized entities or *Processes.*
Confidential	Characteristic of a file, *Document*, media or information, *Data*, or *Metadata*, which, by its nature or because of the requirements of the *Organization*, law and regulations, contracts, *Directives* or *Standards*, is and must be neither available to the public, nor disclosed to unauthorized persons, entities or *Processes.*
Retention	Defined as the continued possession, use or control of an *Information Asset,* including *Personal Information*, by the *Organization,* or a *Third Party* on behalf of the *Organization*.
Consultant	Usually refers to a non-employee who has access to an *Organization*'s *Information Asset* and performs a function normally assigned to an *Employee*. It differs from a service *provider* who can carry out activities remotely.
Derogation	The *process of applying* to the Privacy Committee to override a privacy requirement. A *Waiver* must be formally approved by the Privacy Committee following a *Risk* Analysis and the identification of compensatory measures.
Destruction	Refers to the action of physically *destroying* media or carriers containing *information assets in* a secure manner. Typically, this may involve shredding, disintegrating, incinerating, pulverizing or even melting the media or carrier. It is generally carried out by Service *Providers.*
Requests	All *Requests* for the exercise of a right (e.g.: right of access, rectification, updating, de-indexation, deletion, information, etc.) or complaints made by an individual pursuant to a law or regulation concerning the protection of *Personal Information with* respect to the *Organization*.

Directive	Derived from a policy and specifies its framework. May be a corporate or departmental *document*, and specifies the internal rules of conduct, the operational objectives to be achieved and the division of responsibilities between the various business units.
Document	Means the policies, *Directives, Standards, Processes,* Guides and *Procedures* detailing the *Organization's* structure, *Processes* and controls. *Documents* also include paper or digital copies.
Data	*Data* is a quantitative or qualitative fact, value or variable relating to a thing or an individual, which, taken on its own, may have no particular significance. *Data* can also be aggregated into a *Data* set.
Employee	Refers to any individual working on behalf of the *Organization*, regardless of status, employment (trainee, student or permanent/temporary employee).
Privacy Impact Assessment	An analysis that identifies and considers all factors that may have a positive or negative impact on the privacy of the persons concerned, and suggests strategies to avoid or mitigate the *Risks* identified. This definition also refers to the *Privacy Impact Assessments* provided for in sections 3.3, 17 and 21 of the PIPEDA.
Supplier	A *Supplier is* a natural or legal person who provides goods or services to the *Organization*. This includes, in particular, contractors and sub-contractors, *Partners* (business partners), service providers and representatives who usually use their own IT equipment. *Consultants* are expressly excluded from this definition.
LCAP	An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain practices that discourage commercial activity by electronic means, amending the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the *Privacy* Act and the Telecommunications Act, S.C. 2010, c. 23, commonly known as the "*Canadian Anti-Spam Act*".
LNE	Ontario *Employment Standards Act, 2000*, including electronic *monitoring* requirements added on April 11, 2022.
PIPEDA	*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c 5
LPRPSP	*Act respecting the protection of personal information in the private sector*, RLRQ c P-39.1
Safety (control) measure	In the context of a *Policy* or *Directive*, a concrete means which ensures, partially or totally, the protection of *Information Assets* against one or more Computer *Threats,* and whose implementation aims to reduce the probability of occurrence of these *Threats* or to minimize the resulting losses.

Non-compliance	*Non-compliance* with a framework that is the subject of an action plan to implement a corrective action within a defined timeframe, when the *Risk* is medium, high or very high.
Standard (See *Standard*)	The *Standards* are a low-level description of how the *Organization* will implement its *Information Security* strategy. In other words, they are used to maintain a minimum level of effective security. They are also mandatory. *Standards* are derived from *Directives*. They may vary according to the business line, *Division* or *Subsidiary* concerned.
Organization	Refers to all sectors of Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc., Partenariat agricole QMO s.e.c. and Commandité QMO inc.
Regulatory body	Refers to the bodies designated in the *Organization's Privacy Policy* to oversee its application. This definition includes the Commission d'accès à l'information du Québec, the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner of British Columbia.
Partner	Individuals or groups of individuals who participate in the *Organization's* activities without holding the status of *Employees*, *Consultants* or *Suppliers*. In some cases, a *Partner*'s activities may require the use of *information assets* owned by the *Organization*.
Staff	Generic term used to refer to *Employees*, *Consultants* and *Suppliers* of the *Organization*.
PIPAAB	*Personal Information Protection Act*, SA 2003, c P-6.5
PIPABC	*Personal Information Protection Act*, SBC 2003, c 63
Privacy policy	*A document* that serves as a guide and framework for decisions regarding the protection of *Personal Information*. The policy sets out the *Organization*'s main principles and guidelines. It is approved by Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc. Board of Directors.
Security policy information	*A document* that serves as a guide and framework for decision-making. The policy sets out the *Organization's* main *principles* and guidelines in terms of *information security*. It is approved by Norseco s.e.c. / W.H. Perron / 9406-5299 Québec Inc. Board of Directors.
Procedure (See *Process*)	A *Procedure* describes and formalizes the tasks involved in implementing the *Process*. If the *Procedure* is not followed, the Output *Data* of the *Process* will not comply with the expected requirements: it specifies the what, how, when and who is involved. *Procedures* support *Directives*. They are generally approved by the departments concerned.

Process (See *procedure*)	A *Process is* a set of operations, which can be broken down into tasks, with a view to achieving a given result. A *Process* is a sequence of actions that are not sequential like a *Procedure*. It is defined by its transactional nature: "produce X" , "design Y", "transporting Z from A to B", "invoicing XYZ services", etc. *Processes* support the *Directives*. They are generally approved by the departments concerned.
Compliance program	Program to implement and execute a strategy for compliance and *risk* management of *personal information*
Regulations	Refers to the *privacy* laws and regulations applicable to the *Organization*. This definition includes *PIPEDA*, *PIPEDA*, the *Canadian Personal Information Protection and Electronic Documents Act*, the Personal Information *Protection and Electronic Documents Act, the Personal Information Protection and Electronic Documents Act, the Personal Information Protection and Electronic Documents Act, the Personal Information Protection and Electronic Documents Act, the Personal Information Protection and Electronic Documents Act,* the Personal Information Protection and Electronic Documents Act and their regulations.
Information	*Information* is *data* about something or someone. For example, a telephone number or a name is *information*.
Personal information	Consists of any *Information* concerning a natural person that directly or indirectly enables that person to be identified (e.g. surname, first name, postal address, telephone number, social insurance number, etc.).
Privacy Officer	Designates the manager responsible for ensuring compliance with and implementation of the *Division*'s Privacy Policy and *Regulations*. His or her mandate is set out in the *Division*'s Privacy Policy and *Regulations.*
Risk	Potential impact of an event that could adversely affect the *Organization'*s activities *or in* any way interfere with the fulfillment of its mandate. The assessment of a *Risk* level takes into account the plausibility of an event and the *Criticality* of its potential impact on the *Organization.*
Third party(ies)	Actor(s) or *Organization(s)* collaborating directly or indirectly with the *Organization* and having access to the *Information Assets*. *Third parties* include but are not limited to *Suppliers*, Vendors and *Consultants*.
Treatment (verb Treat)	Means any collection, use, disclosure, retention, *destruction* or other handling of *Personal Information.*
User	Any person who uses the *Organization'*s *information assets*, including but not limited to *employees*, trainees, *consultants* or *suppliers*.