PRIVACY POLICY

Policy Objectives

Vior Inc. ("**Vior**" or the "**Corporation**") is responsible for protecting and managing Personal Information (as defined below) in its possession. By adopting the Privacy Policy (the "**Policy**"), Vior undertakes to protect, keep confidential and preserve the rights of the Persons Concerned (as that term is defined below). Employees, directors, officers and consultants of the Corporation (collectively and individually, "**Employee**") must diligently comply with the principles set out in the Policy and the procedures it puts in place and, where applicable, perform the tasks it assigns to him or her.

The Policy establishes the principles governing the collection, protection, use and disclosure of Personal Information within its scope.

1. Definitions

1.1 "**Privacy Impact Assessment**" or "**PIA**" refers to the process of considering all factors that will have a positive or negative impact on the privacy of the Persons Concerned. Those factors are:

a) compliance of an information technology project or communication with the legislation applicable to the protection of Personal Information and compliance with the principles underlying it;
b) identification of the risks of a breach of privacy caused by the project or the communication and assessment of their impacts;
c) implementation of strategies to avoid such risks or reduce them effectively.

1.2 "**Confidentiality Incident**" means:

a) access to Personal Information not authorized by law;
b) the use of Personal Information not authorized by law;
c) the disclosure of Personal Information not authorized by law; or
d) the loss of Personal Information or any other breach of the protection of such information.

1.3 "**Person Concerned**" means any natural person to whom Personal Information relates. Without limiting the generality of the foregoing, Persons Concerned include Employees, job applicants, members of management, visitors and internal customers.

1.4 "**Personal Information**" means any information held by Vior that allows a natural person to be identified directly or indirectly. Personal Information may include, but is not limited to, a person's name, mailing address, telephone number, email address, Internet (IP) address, age, gender, marital status, health information, social insurance number, financial situation, credit card data and credit history.

1.5 "**Necessary Personal Information**" means Personal Information comprising what is absolutely necessary to fulfil a legitimate, important and real purpose to which its collection relates where there are no other solutions that are less intrusive to the privacy of the Persons Concerned, and the useful effect of the collection is greater than the harm likely to be caused to them.

1.6 "**HR Information**" means any Personal Information relating to the Employees, applicants, trainees, temporary workers or retired Employees of Vior.

1.7 "**Commercial Transaction**" means the alienation or rental of all or part of Vior. or its assets, a change to its legal structure by merger or otherwise, the obtaining of a loan or any other form of financing by it or security taken to guarantee one of its obligations.

2. Scope

2.1 This Policy applies to all Employees of Vior.
2.2 This Policy applies to all Vior sites.
2.3 The provisions of this Policy may also be applied to any person employed by an external partner performing work for Vior or investors, where the Corporation holds such person's Personal Information. It therefore also applies to our on-site contractors.
2.4 The Policy determines the principles and internal procedures aimed at ensuring Vior's compliance with the obligations imposed by the following normative instruments:

a) *Civil Code of Québec,* CQLR, c. CCQ-1991.
b) *Act respecting the protection of personal information in the private sector,* CQLR, c. P-39.1, as amended by the *Act to modernize legislative provisions as regards the protection of personal information,* SQ, 2021, c. 25 *(*hereinafter: the *"***Amended Privacy Act**");
c) *Act to establish a legal framework for information technology,* S.Q. 2001, c. C-1.1.
d) *Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunication,* S.C. 2010, c. 23.
e) *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5, *(*hereinafter*:* the *"***PIPED Act***"). Note that this Act will be repealed and amended by An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts,* Bill C-27 (tabled and 1st reading - June 14, 2022), 1st Sess., 44th Parl. (Can.).

3. Roles and Responsibilities

3.1 Corporate Secretary:

a) ensures the protection of Personal Information by exercising the functions attributed by the Privacy Act to the "person in charge of the protection of personal information", (hereafter "**Privacy Officer**") unless all or part of them have been delegated in writing to another officer of the Corporation.;
b) is responsible for protecting the Personal Information of senior management and of Board of Directors.
c) sees that the Employees for whom he is responsible comply with this Policy by ensuring that it is known and applied by all of them;
d) approves the Personal Information policies and practices the company must establish and implement;
e) participates in PIAs and any risk study related to the protection of Personal Information when required by applicable law;
f) participates in the management and reporting of Confidentiality Incidents; and
g) establishes procedures for processing complaints involving privacy issues.

3.2 Human Resources/Finance:

a) endorses the inherent obligation to protect the integrity, availability and confidentiality of the information and files handled by the Chief Executive Officer;
b) is responsible for establishing the necessity of HR Information and Personal Information related to the receiving of visitors, as applicable;
c) ensures that only authorized persons within Vior who have a legitimate need to know, have access to the Personal Information of Employees, contractors and investors;
d) provides education and training to ensure that Employees are aware of Vior's obligations with regard to the protection of Personal Information and the best practices to adopt to protect them;

e) participates in PIA concerning certain information or electronic service delivery systems and suggests measures to protect Personal Information processed within the framework of those systems;
f) receives and responds to requests for access and rectification as well as requests related to data portability and the right to oblivion (deletion of information, where possible – e.g. on the recruitment platform);
g) protects all confidential information, including HR Information, entrusted to it, as well as the tools and techniques used by Vior's Human Resources Department; and
h) in collaboration with the person responsible for IT Services, sets up and ensures the validity of administrative and technical controls in order to limit access to Personal Information to staff who need to have access to it for legitimate reasons.

3.3 Information Technology:

a) management is responsible for establishing appropriate technical and organizational measures to safeguard Personal Information and ensure the security of our information systems. These responsibilities are delegated to an IT services firm for implementation and ongoing support;
b) management ensures that procedures are in place – carried out by an IT services firm - to regularly test, analyze and evaluate the effectiveness of technical and organizational measures to keep Personal Information secure; and
c) management oversees the the evaluation of existing and prospective technological solutions, relying on the expertise of an IT services firm to ensure alignment is established with this Policy..

3.4 Employees:

a) keep their file and Personal Information up to date;
b) use the means in place to protect their Personal Information (e.g. using a strong password, locking their session, etc.); and
c) if they need employment confirmation or references or otherwise need to provide Personal Information, the employees fill out the forms to give the employer authorization.

4. Principles Applicable to Consent

The general principles related to consent defined in this section apply to the collection, use or disclosure of Personal Information. These principles must be integrated into Vior's internal processes.

4.1 Any consent required from a Person Concerned must be manifest, free and informed.
4.2 Any consent required from a Person Concerned must be given for specific purposes and in such a way that the Person Concerned understands the nature, purposes and consequences of the collection, use and disclosure of Personal Information.
4.3 When the request for consent is made in writing, it must be presented separately from any other information provided to the Person Concerned.
4.4 Depending on the nature and sensitivity of the Personal Information, consent may be express (such consent may be given verbally, in writing or electronically) or implied (for example, where the Person Concerned voluntarily provides Personal Information).
4.5 To the extent reasonable, the acceptance of any policy of Vior that requires the consent of the Person Concerned with regard to the collection, use and disclosure of Personal Information concerning him is explicit and recorded.
4.6 When the consent of the Persons Concerned should be requested by partners or suppliers, Vior contractually ensures that they are aware of their duties with regard to the quality of the consent they must obtain prior to disclosing Personal Information to Vior.

5. Collection of Personal Information

5.1 Definition. Collection is the operation by which Personal Information is collected (e.g. forms, surveys, Web analytics tools), created (e.g. internal identifier) or inferred (e.g. statistical attendance profile).

5.2 Principles. Vior applies the following principles regarding the collection of Personal Information:

a) Determine the purposes of collecting it before proceeding;
b) Limit the collection of Personal Information to the minimum necessary to achieve the identified purposes;
c) Request consent prior to collecting Personal Information by applying the principles set out in section 5;
d) Minimize inaccuracies in Personal Information that is collected by providing mechanisms for the Persons Concerned to examine and correct their records.

5.3 Means.

a) Vior collects certain HR Information from applicants for jobs posted on the company's website in the career section. Vior is committed to posting the Privacy Policy in compliance with the Amended Privacy Act.
b) Once hired, additional HR Information is collected to build and process the employee's file and to process payroll and other benefits.
c) Vior also collects Personal Information about contractors and visitors to the site, for security reasons and in the event of an emergency.
d) Vior collects the categories of Personal Information described in Appendix 3, on the categories of Persons Concerned that are specified in order to achieve the purposes identified therein. This Appendix shall be completed and updated on a regular basis during the implementation of this Policy.

6. Use of Personal Information

6.1 Definition. In this Article 6, the term "use" includes any operation performed internally by an Employee. This can be the organization, structuring, adjustment, modification, extraction or consultation of Personal Information, or any other type of operation involving Personal Information where it is carried out by an Employee.

6.2 Principles. With respect to the use of Personal Information, Vior applies the following principles:

a) Each Employee who uses Personal Information is bound by confidentiality obligations and has received adequate training;
b) Employees who use Personal Information may only have access to the Personal Information necessary to perform their duties;
c) The Employee will incur sanctions in the event of contravention, improper use or use for purposes other than the exercise of his or her duties;
d) Such penalties are made known to the Employee before the Personal Information is used.

6.3 Types of use of Personal Information.

a) The Personal Information held by Vior is used to process an employee's file, payroll and benefits, medical file, security and in the event of an emergency, as specified in Appendix 3.
b) Where reports are submitted (e.g. training, labour reports, etc.), the Personal Information is anonymized so the Person Concerned cannot be identified directly or indirectly.

7. Disclosure of Personal Information

7.1 Definition. Disclosure consists of voluntarily transmitting, transferring or making Personal Information available to a third party for them to carry out any transaction, regardless the means of communication used or the disclosure of Personal Information to the third party. For greater clarity, it is not relevant whether the third party can view or become aware of the Personal Information for the transfer, transmission or making available to be considered a disclosure.

7.2 Principles.

1) Vior limits the amount and types of Personal Information disclosed to what is necessary for the purposes for which the disclosure is made.
2) Vior keeps a record of disclosures.
3) Vior has set up requirements related to subcontractors and discloses Personal Information transparently and securely.
4) Personal Information is disclosed either after obtaining the consent of the Person Concerned or with legal authorization to make the disclosure without the consent of the Persons Concerned.

7.3 Disclosure of Personal Information authorized by law without the consent of the Persons Concerned

Who?	Description and Purpose	Measures
Subcontractors	Vior enters into contracts with suppliers and subcontractors to provide service to the Corporation	The contract obliges subcontractors in particular to: • only use the Personal Information necessary to provide the service; • refrain from disclosing or communicating Personal Information without Vior's written consent; • implement strict security measures; • allow Vior to audit those measures; • notify Vior immediately of a Confidentiality Incident. • destroy Personal Information at the end of a contract; • set up automatic mechanisms and/or procedures that ensure that the results of requests for modification, deletion or opposition relating to Personal Information are carried out by subcontractors.
Third party for a commercial transaction	Vior Inc. may sign a contract with a third party (including investors) to carry out a commercial transaction.	The contract requires that the third party: • use only the Personal Information necessary to carry out the commercial transaction; • set up strict security measures; • refrain from disclosing or communicating Personal Information without Vior's written consent; • notify Vior immediately of a Confidentiality Incident;

Who?	Description and Purpose	Measures
		• destroy the Personal Information if the transaction is not carried or if it is no longer necessary for it to be carried out.
Legitimate authorities	Vior may be required to provide Personal Information to comply with an order or decision by a court, including a valid search warrant, or regulatory authority.	The laws governing these authorities require them to set up measures to keep Personal Information confidential.
Vior's attorneys	In order to ensure its defense or assert its rights, Vior may, in certain cases, disclose Personal Information to its attorneys.	Both the law and the mandate letters that Vior signs with its attorneys require that they keep all Personal Information it discloses to them confidential.

7.4 Disclosure of Personal Information outside the Province of Québec

5) **Jurisdictions.** Vior may disclose Personal Information outside of Québec to the following regions:
- Other provinces in Canada

6) **Procedure.**
- Before disclosing Personal Information outside Québec, Vior conducts a PIA.
- The PIA considers the following factors:
  - the sensitivity of the Personal Information;
  - the purpose of its use;
  - the measures taken to protect it;
  - the legal rules applicable in the State where the Personal Information will be disclosed.
- Vior will only disclose the information if this assessment shows that the Personal Information will be adequately protected according to generally accepted privacy principles.

8. Data conservation, Accuracy and Security

a) Personal Information for which Vior Inc. is Responsible

Personal Information held by Vior is stored securely, with strict access management (for authorized persons only).

Vior follows generally accepted industry standards to protect information submitted to it, both during transmission and once it is received. Appropriate physical, technical and administrative safeguards are maintained to protect Personal Information against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, misuse and any other unlawful processing of personal information in our possession.

See Appendix 1 for the legal retention periods for personal information held by Vior.

9. Contacting the Privacy Officer

To ask questions or make comments regarding this Privacy Policy or personal information, assert your rights, file a complaint or obtain information about Vior's policies and practices, contact the Privacy Officer by email at corporatesecretary@vior.ca or anonymously through the Tandem Team, a third-party provider for confidential, anonymous reporting services by telephone: 1-844-487-4729.

All anonymous reports will be treated sensitively and seriously, in the strictest confidence and in accordance with this Policy and all applicable laws and regulations.

10. Confidentiality Incident Management

10.1 Actions to be taken following a Confidentiality Incident

If Vior has reason to believe that a Confidentiality Incident involving Personal Information it holds has occurred, it must take reasonable steps to reduce the risk of harm being caused and to prevent other similar incidents from occurring. Vior must document any Confidentiality Incident in the register for that purpose.

A Confidentiality Incident could occur, for example, when:

- a person confirms the employment status of an employee or gives employment references without having received the employee's authorization;
- a staff member gives personal information to the wrong recipient;
- the organization is the victim of a cyber-attack: phishing, ransomware, etc.

10.2 Risk assessment

For any Confidentiality Incident, Vior must assess the risk of harm to the Persons Concerned. To do so, it must consider, among other things:

- the sensitivity of the information in question;
- the anticipated consequences of its use;
- the likelihood that it will be used for detrimental purposes.

The Privacy Officer may involve other people, suchas senior management or external consultants as needed.

If the analysis reveals a risk of serious harm, Vior must notify the *Commission d'accès à l'information du Québec* and the Persons Concerned who are affected by the Confidentiality Incident.

Otherwise, it must continue its work to reduce the risk of and prevent a similar incident from reoccurring in the future.

11. Policy Review

The Governance and Compensation Committee shall review this Policy periodically, as it deems appropriate, and propose recommended changes to the Board of Directors. All amendments will be brought to the attention of each Vior personnel upon becoming effective.

This Policy was adopted and ratified by the Board of Directors on August 13, 2025.

APPENDIX 1
RETENTION OF PERSONAL INFORMATION

Type of document/information	Applicable law	Period
Group insurance	*Act respecting insurance*, RSQ c A-32.	No prescribed time limit. Unless there are specific provisions in the Employee'scontract Recommendation: When no retention period is prescribed, it is still prudent to keep these documents for at least three years.
File of terminated employees	*Civil Code of Québec*, SQ 1991, c 64, art 2925.	Three years. Corresponds to the prescription period for civil actions.
Medical record	*Act respecting occupational health and safety*, RSQ c S-2.1, s 127 (5).	No prescribed time limit. Recommendation: Seven years after the end of employment.
Claim files under the *Act respecting industrial accidents and occupational diseases*	*Act respecting industrial accidents and occupational diseases*, RSQ c A-3.001.	No prescribed time limit. Recommendation: keep these documents permanently because of claims that may arise long after employment ends.
Information used to carry out a pay equity plan or to assess the maintaining of pay equity in the Company Content of any postings	*Pay Equity Act*, R.S.Q., c. E-12 001 (sections 14.1 and 76.8)	Six years after posting the results.
Training (training programs and agreements, training invoices and contracts)	*Regulation respecting eligible training expenditures*, RRQ 1981, c D-8.3, r 3, s 4.	Six years after the last year to which the information relates.
Company pension plan	*Supplemental Pension Plans Act*, RSQ c R-15.1.	Permanently. If the employee is eligible for a pension.
Payroll register and related documents	*Regulation respecting a registration system or the keeping of a register*, RRQ 1981, c N-1.1, r 6, s 2.	Seven years.
Register for tax purposes and back-up documents (accounting records, etc.)	*Tax Administration Act*, CQLR c A-6.002, s. 35.1; *Income Tax Act*,	Seven years after the last year to which they relate or after the tax return is filed (i.e. seven years).

Type of document/information	Applicable law	Period
	RSC 1985, c 1 (5th Supp.), s 230 (4).	
Records of employment and other documents relating to contributions/deductions and claims	*Employment Insurance Act*, SC 1996, c 23, s 87 (3) and s 87 (4).	Six years after the end of the year in respect of which the records were kept or until a decision is rendered (including the expiry of the deadline to appeal) in a dispute under section 90 or 91 of the Act.
Québec pensions (registers of contributor information)	*Act respecting the Québec pension plan*, RSQ c R-9, s 66.	No prescribed time limit. Recommendation: at least seven years after the end of the fiscal year in which employment ended. This corresponds to the four-year prescription for any assessment by the Minister (under section 66 of the Act).
Documents covered by a request for access or rectification	*Act respecting the protection of personal information in the private sector,* CQLR c P-39.1, s 36.	No prescribed time limit. However, when personal information is the subject of an access request that is denied by the company, it must be kept for the time required to allow the person in question to exhaust the remedies provided for in the Act.

APPENDIX 2
COMPLAINT PROCEDURE

If an individual believes that an event that contravenes the principles set forth in this Policy has occurred, he or she should contact our Privacy Officer (corporatesecretary@vior.ca) in writing or report an event anonymously by telephone through the Tandem Team at 1-844-487-4729.

The Privacy Officer or delegate acknowledges and coordinates follow-up to inquiries and complaints, and ensures that responses meet the privacy requirements and are provided in a timely manner.

Investigations

All Confidentiality Incident complaints are investigated. If a complaint is found to be justified, Vior strives to resolve it promptly. If necessary, policies and practices are modified so the situation does not reoccur.

The investigation includes an examination of the facts which make it possible to analyze the complaint using various means:

- examination of the file of the person concerned (information both in the database and on paper);
- examination of the Privacy Policy;
- discussion with Employees who have dealt with the person in question or worked on the file; and
- consultation of any other source or documents likely to provide relevant information.

Acknowledgment and response

When it is impossible to respond to a request for information or to resolve a complaint immediately, Vior's Privacy Officer informs the person of the status of the request or complaint and indicates the approximate date the applicant will receive a reply. If a complaint is reported anonymously, such anonymous reports will be forwarded by the Tandem Team directly to the Privacy Officer and Chair of the Audit Committee.

Follow-up

The Privacy Officer or delegate will contact the applicant if necessary to ensure that the matter has been satisfactorily resolved.

If the resolution of the complaint requires that Vior change its policies and practices, the Privacy Officer or his delegate will ensure that the necessary changes are made.

Oversight of privacy complaint procedures

The Privacy Officer or their delegate periodically reviews the complaints procedure to ensure that a fair, appropriate and prompt mechanism is in place. They also keep a complete register of all communications and complaints received regarding the protection of Personal Information.