Société portuaire
du Bas-Saint-Laurent
et de la Gaspésie
Québec

Personal Information Governance and Information Security Policy

June 2026

Société portuaire du Bas-St-Laurent et de la Gaspésie *(SPBSG)*
603 Avenue Saint-Jérôme PO box 222, Matane, Quebec G4W 3N1 | Tel.: 418 562-7094

Effective date: June 16, 2026	Adopted: June 16, 2026	Resolution no.: 2026-06-04
Deadline for review: 3 years	Revised: —	Policy Administrator: President and Chief Executive Officer

Contents

1 Introduction 3
2 Objectives 3
3 Roles and Responsibilities 3
3.1 Board of directors 3
3.2 President and Chief Executive Officer 4
3.3 Management 4
3.4 Privacy Officer 5
3.5 Data owners 5
3.6 Employees and contractors 5
4 Data Collection 5
4.1 Online presence 6
4.2 Human resource management 6
4.3 Handling complaints 6
4.4 Public consultations and surveys 6
5 Retention 7
6 Use 7
7 Disclosure 7
8 Destruction 7
9 Individual Rights 7
9.1 Right of access 7
9.2 Right of rectification 7
10 Complaints 7
11 Training 8
12 Information Security 8
12.1 Objectives 8
12.2 Responsibilities 8
12.3 Access control 8
12.4 Protection of personal information 8
12.5 Education 9
12.6 Compliance assessment 9
12.7 Incident management 9
13 Adoption, Review and Effective Date 9

Personal Information Governance and Information Security Policy

1 Introduction

The Société portuaire du Bas-St-Laurent et de la Gaspésie inc. (the "Authority") is subject to the *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* (the "Access Act"). The purpose of this policy is to ensure compliance with the legal framework of the Access Act.

The Authority recognizes the complementary nature of personal information protection, information security and confidentiality.

This policy sets out the rules governing the handling of personal information within the Authority. It defines the roles and responsibilities of the Authority's employees with regards to the entire life cycle of personal information, from its collection to its destruction.

The policy is intended for all individuals employed by the Authority, including students and interns ("personnel" or "employees"). It also applies to any individual with whom the Authority entrusts personal information for the performance of a mandate or service contract ("contractors").

It applies to all personal information held by the Authority, including information retained by third parties, regardless of the medium on which they are retained, from their collection to their destruction.

All information regarding a natural person that directly or indirectly makes it possible to identify said natural person is personal information.

2 Objectives

This policy sets out to:

a) Establish the rules governing the personal information held by the Authority.

b) Define the roles and responsibilities of the Authority's employees throughout the life cycle of personal information.

c) Establish the categories of individuals who may use personal information in the execution of their duties.

d) Promote transparency and set out the Authority's commitments regarding the protection of personal information.

3 Roles and Responsibilities

3.1 Board of directors

The board of directors is responsible for:

3.1.1 Approving this policy and its methods of application.

3.1.2 Understanding the issues that pose a risk to the security of the Authority's information assets.

3.1.3 Reviewing, analyzing, and making recommendations or decisions on the reports submitted to it.

3.1.4 Ensuring the Chair delegates, in writing, responsibility for access to documents and the protection of personal information to a member of the Authority's management team.

3.1.5 Facilitating the performance of the Privacy Officer's duties.

3.1.6 Supporting the implementation and dissemination of this policy.

3.2 President and Chief Executive Officer

The President and Chief Executive Officer is responsible for:

3.2.1 Implementing and monitoring information security measures.

3.2.2 Advising and making recommendations to management in matters of security.

3.2.3 If delegated such a responsibility, serving as the officer responsible for access to documents and the protection of personal information (the "Privacy Officer"), as further described in Schedule A.

3.2.4 Ensuring employees implement and comply with best practices for **personal information** protection.

3.3 Management

Management is responsible for:

3.3.1 Establishing guidelines for the protection of personal information and information security, including the cybersecurity program, and for monitoring the implementation of said guidelines.

3.3.2 Approving employee access to personal information held by the Authority.

3.3.3 Ensuring that physical access to premises where records containing personal or sensitive information are located, including digital access to such information, is granted in accordance with the principle of least privilege.

3.3.4 Defining access rights to documents and computer directories (access management procedure).

3.3.5 Submitting and making recommendations to the board of directors on all matters of information security that require the board's attention.

3.3.6 Ensuring compliance with this policy and any related procedures and guidelines within their administrative unit.

3.3.7 Ensuring employees under their supervision collect, use, retain, disclose and destroy personal information safely.

3.3.8 Collaborating with the Privacy Officer on matters regarding the Authority's compliance with legislative, regulatory and administrative obligations for the protection of personal information.

3.3.9 Taking appropriate measures in the event of a violation of this policy or of personal information protection rules by an employee or contractor under their supervision.

3.3.10 In collaboration with the Privacy Officer, educating employees and contractors under their supervision of the importance of protecting personal information.

3.3.11 Ensuring employees and contractors under their supervision participate in Authority-provided training sessions relating to the protection of personal information.

3.4 Privacy Officer

The Privacy Officer is responsible for:

3.4.1 Advising management on matters of security, taking into account any risks to the Authority and its mitigation strategies.

3.4.2 Advising the owners of personal information or sensitive personal information on the best practices implemented by the Authority to ensure the protection of their personal information.

3.4.3 Implementing cybersecurity measures and ensuring the monitoring thereof.

3.4.4 Applying the access management procedure, as instructed by management.

3.4.5 Ensuring the implementation of the rules of use of technology and the compliance thereof.

3.5 Data owners

Data owners are responsible for:

3.5.1 Ensuring that the personal information for which they are the designated owner is classified in a manner that adequately governs its use, processing, retention, distribution, protection, and destruction.

3.5.2 Ensuring that personal information is only accessible by authorized systems and individuals, through the access management procedure.

3.5.3 Reporting to the President and Chief Executive Officer and to the Privacy Officer any suspected or confirmed security incidents (including confidentiality incidents), or any potential breaches involving the personal information for which they are the designated owner.

3.6 Employees and contractors

Employees and contractors are responsible for:

3.6.1 Complying with this policy and application guidelines, whether on Authority premises or elsewhere.

3.6.2 Protecting the confidentiality of the information they have access to (including personal information) and only accessing personal information when required for their work.

3.6.3 Recognizing that they have no guarantee of confidentiality in their electronic communications.

3.6.4 Taking responsibility for any actions made using their account, i.e., not sharing their access code and passwords.

3.6.5 Using a strong, complex password (composed of lower- and upper-case letters, special characters and numbers) and not sharing it.

3.6.6 Not retaining, on any paper or electronic medium other than those authorized by the Authority, any personal information obtained in the course of their duties, and continuing to maintain its confidentiality.

3.6.7 Participating in any education and training activities in matters of personal information protection made available to them by the Authority.

3.6.8 Reporting all suspected or confirmed security incidents (including confidentiality incidents), or any potential breaches (security breaches, wrongful use of confidential information, etc.) to their superior and to the Privacy Officer.

4 Data Collection

The Authority collects only the personal information necessary to carry out its activities, including the operation, maintenance, upgrading and developing of port infrastructure, the management of its online presence (website and portal), human resource management, handling complaints, and public consultations and surveys.

4.1 Online presence

The Authority collects the personal information that website and portal users share with it (e.g., audience statistics, contact information, and information regarding port services).

4.2 Human resource management

The Authority collects only the personal information necessary to evaluate candidates for recruitment purposes. This data is usually shared by candidates. The Authority collects the personal information required to manage employee records.

4.3 Handling complaints

The Privacy Officer collects the personal information shared with them by individuals filing complaints in order to handle their privacy complaints. This information generally includes their contact details and the subject of their complaint.

4.4 Public consultations and surveys

In the scope of its activities, the Authority may collect personal information during public consultations or surveys.

For all public consultation and surveys, the Authority must:

4.4.1 Comply with applicable legislation.

4.4.2 Assess the necessity of holding a public consultation or survey.

4.4.3 Obtain valid and reliable results from its surveys and public consultations.

4.4.4 Avoid collecting personal information where possible, and prioritize data collection for aggregated statistics, excluding personal information.

4.4.5 Destroy personal information as soon as the purpose for which it was collected has been fulfilled.

4.4.6 Use the protection measures established in Schedule B.

4.4.7 Where consultations and surveys are conducted by a third party, ensure the Authority is the data owner of the resulting data by entering an agreement with the third party that includes the provisions established in Schedule B.

4.4.8 Following the survey or public consultation, take the necessary steps identified in Schedule B.

5 Retention

The Authority's employees and contractors must ensure the confidentiality of personal information when carrying out their duties in accordance with section 3.6 above.

If there are any doubts regarding the confidentiality of data or questions regarding the management of personal information, employees and contractors must speak with their manager or the Privacy Officer.

6 Use

The Authority's employees must only use personal information for the purposes for which it was collected. Any other use must be authorized in advance by the employee's manager or the Privacy Officer. The manager or Privacy Officer must ensure that any such use complies with applicable legislation and, where required, that the consent of the individual concerned has been obtained.

7 Disclosure

The Authority's employees and contractors must not disclose any confidential personal information to a third party without the consent of the individual concerned, except where permitted under the Access Act.

Prior to disclosing any confidential personal information to a third party, the Authority's employees and contractors must consult their manager. The manager may consult with the Privacy Officer.

Some information may be disclosed to third parties pursuant to service agreements that the Authority enters with said third parties.

8 Destruction

The Authority's employees and contractors must securely destroy personal information once it is no longer required for the purposes for which it was collected, in accordance with the retention periods set out in the Authority's retention schedule and record management policies.

9 Individual Rights

9.1 Right of access

Individuals whose personal information is held by the Authority have the right to be informed of the existence of such information and to receive a copy of it, subject to the limitations and conditions set forth in the Access Act.

9.2 Right of rectification

Individuals concerned about incorrect, incomplete or ambiguous personal information, or information that has been collected, disclosed or retained in violation of the Access Act may request to have their information corrected, subject to the limitations and conditions set out in the Access Act.

10 Complaints

If individuals believe their personal information is being handled in violation of this policy or applicable legislation, they may file a complaint by submitting a written request to the Privacy Officer, who must respond to the complaint and investigate within a reasonable time. The Privacy Officer may take one or more of the following measures:

- Ask the complainant to clarify their complaint and provide help to do so.
- Decide to open an investigation assessing the merits of the complaint.
  Ask the complainant for permission to share their complaint or other content with another service in order to obtain the information needed to assess the merits of the complaint.
- Ask to meet with the complainant for any of the reasons mentioned above.

Once the complaint has been filed and assessed, the Privacy Officer must notify the complainant, within a reasonable time, of the results of the assessment and the corrective measures to be implemented, if applicable.

11 Training

As part of its operations, the Authority is committed to training and educating its employees and contractors regarding the protection of personal information and the rules in place to ensure compliance with its Privacy Policy. Ongoing awareness and training are essential to ensuring the protection of information.

Employees and contractors receive training on the protection of personal information as part of the onboarding process. The Authority also ensures its training is periodically reviewed and kept up to date.

12 Information Security

12.1 Objectives

This section of the policy covers information security. Its purpose is to protect corporate information from internal and external threats, ensure the confidentiality, integrity and availability of information, and comply with applicable privacy regulations.

12.2 Responsibilities

In general, information security applies to all administrators, managers, employees, suppliers, business partners, contractors, clients, or any other person who accesses, uses, saves, transports, or discloses the Authority's information assets. It applies to all of the Authority's information assets throughout their entire life cycle, regardless of their form, medium, location, or the means of disclosure used to transmit them, whether they are retained by the Authority itself or by a third party. For greater clarity and without limiting the foregoing, examples include various tangible and intangible media used to process, transmit, or retain information assets: paper, software, databases, networks, videos, or audio recordings.

The Privacy Officer is responsible for implementing protection measures, and employees and contractors must comply with security rules and procedures.

12.3 Access control

Access to information is restricted to authorized individuals based on their role and need to know. Employees and contractors must be identified and authenticated prior to being granted access to information. They must use strong passwords and change them regularly.

12.4 Protection of personal information

Personal information must be protected against loss, destruction, alteration and unauthorized use. In order to restrict access to authorized individuals, sensitive and confidential personal information must be classified and centralized.

The Authority implements the following technological, physical and organizational security measures to protect its information assets:

12.4.1 It keeps an updated inventory of key information assets and identifies critical assets that require enhanced protection.

12.4.2 It designates an officer (data owner) for each critical asset and asset containing personal information.

12.4.3 It performs an annual information security risk assessment and establishes required security measures.

12.4.4 It implements adequate physical security measures to protect information and equipment.

12.4.5 It implements adequate IT security measures to protect information and equipment, such as security configuration settings, password settings, logging and alerts.

12.4.6 It controls access to information assets through its IT Administrator, in accordance with management directives.

12.4.7 It ensures compliance with PCI Security Standards Council requirements for protecting payment card information.

12.4.8 It provides adequate training on the risks and impacts of security breaches to users, depending on their degree of access to information assets.

12.4.9 It encourages the reporting of actual or suspected security incidents (including confidentiality breeches).

12.4.10 It securely manages IT systems, for example by implementing patches and firewalls.

12.4.11 It monitors information asset use and IT systems, in compliance with applicable legislation and regulations.

12.4.12 It implements physical security measures (locked filing cabinets, alarm systems) to protect records containing sensitive information.

12.4.13 It performs regular backups to ensure the recovery of personal information in the event of an incident.

12.4.14 It destroys information in a secure and timely manner.

12.5 Education

Employees and contractors must be made aware of security risks and best security practices. The Authority provides them with regular training and they are required to familiarize themselves with this policy. Awareness campaigns are also implemented to keep employees and contractors up to date with the latest security threats.

12.6 Compliance assessment

Information security compliance must be assessed regularly. Audits must be carried out to ensure rules and procedures are being followed. Regular reports must be prepared to keep management abreast of the state of information security.

12.7 Incident management

To minimize impact, security incidents (including confidentiality incidents) must be managed appropriately. A security and confidentiality incident management process exists to detect, analyze, remedy and prevent security and confidentiality incidents. All incidents must be reported to management and to the Privacy Officer. An assessment regarding the risk of serious injury caused by security and confidentiality incidents will determine whether other parties must be notified (employees, individuals whose personal information is involved, the *Commission de l'accès à l'information* [CAI], etc.). All confidentiality incidents must be reported in the Authority's confidentiality incident log.

By implementing these information security measures, the Authority can ensure the adequate protection of its sensitive information and maintain the trust of its partners.

13 Adoption, Review and Effective Date

This policy is to be reviewed every three (3) years from its date of adoption, or earlier if justified. It comes into effect as soon as it is adopted by the board of directors.

SCHEDULE A

Role of the Access to Information and Privacy Officer

- Ensure the implementation of and compliance with the provisions of the Access Act within the Authority.
- Ensure compliance with this policy and the Authority's legal, regulatory and administrative obligations regarding access to documents and the protection of personal information.
- Coordinate the Authority's actions in matters of access to documents and the protection of personal information.
- Support management and serve in an advisory, support and guidance role for the Authority's employees and contractors.
- Submit this policy to the board of directors for approval and ensure it is periodically updated.
- Identify and recommend the necessary tools to implement this policy.
- Collaborate with the IT and Record Management Administrator in implementing measures for the optimal protection of personal information.
- Ensure accountability for the protection of personal information.
- Handle complaints relating to the protection of personal information in accordance with the Access Act.
- Handle requests for access to documents and access to personal information, as well as correction requests in accordance with the Access Act.
- Conduct, in accordance with the Access Act, a privacy impact assessment for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, disclosure, retention or destruction of personal information. Such assessments must be conducted from the outset of the project and in respect of any disclosure of personal information outside Quebec. The Access to Information and Privacy Officer must also determine if the information to be disclosed will be adequately protected.

SCHEDULE B

Protection Measures

Where the person responsible for a survey or consultation (the "survey lead") collects personal information through a survey or consultation, the Authority must implement adequate protection measures.

The survey lead must:

a) Ensure that the survey or consultation is required.

b) Consult with the Privacy Officer on the minimum requirements for the protection of personal information when conducting surveys and consultations.

c) Carry out a preliminary ethics assessment of the survey or consultation, taking into account the sensitivity of the information involved, the purpose for which it is to be used, the volume of information, its distribution and the medium on which it will be stored.

d) Consult with the Privacy Officer regarding the possibility of obtaining the consent of individuals for the disclosure of their personal information to a third party conducting the survey (or consultation), taking into account the large number of people to be contacted or the need to contact specific individuals for the purposes of the methodology used or the validity of the results.

e) Ensure that information collected is required for the exercise of the Authority's functions or for the implementation of a program under its administration.

f) Ensure that the individuals involved are informed of:

- The Authority's contact details.
- The purpose for which the information is being collected.
- The categories of individuals who will have access to the information.
- The voluntary nature of the request.
- The consequences of declining to provide the requested information.
- Their rights of access and rectification as provided for in the Access Act.
- The fact that the information collected will not be added to any record that the Authority may hold on the individual concerned, and that participation in, or refusal to participate in, the survey will have no impact on their record or on any services the individual may receive from the Authority.

Agreement with a third party to carry out surveys and consultations

Where the survey lead engages a third party to conduct a survey or consultation:

a) Only the personal information required to conduct the survey must be disclosed to the third party.

b) The collection or disclosure of sensitive personal information must be avoided, unless a preliminary ethical assessment of the survey or consultation has been carried out.

c) The applicable requirements governing mandates and service contracts must be complied with, and the engagement documented in writing.

d) Appropriate security measures must be implemented by the third party to ensure the confidentiality of such information.

Following a survey

Following the survey, the survey lead must:

a) Ensure no personal information is retained by the third party engaged to conduct the survey.

b) Ensure the third party destroys all the information they hold and compiles a report on its destruction.

c) Continue to maintain the confidential nature of the personal information collected.

d) Ensure the information is accessible only to the individuals who require access for the performance of their duties.

e) Ensure the information is used only for the purposes for which it was collected and is not added to any other personal information file.

f) Ensure the information is retained in accordance with the retention period set out in the retention schedule and is destroyed in accordance with that schedule.

g) Ensure the survey or consultation reports of public interest produced by the Authority or on behalf of the Authority are shared on the Authority's website.