Barrage attaches great importance to the confidentiality and security of personal information.

This policy is established in accordance with the following regulations: *Personal Information Protection and Electronic Documents Act* (Federal), *Act Respecting the Protection of Personal Information in the Private Sector* (Quebec), *Personal Information Protection Act* (Alberta) and *Personal Information Protection Act* (British Columbia).

Federal law applies in provinces where local law does not exist, for example in Ontario. In provinces where there is a specific law, the provincial law applies.

This Policy:

- is available at all times on the Barrage Capital website.
- is supplemented by the *Digital Data Privacy Policy* which governs the management of digital data collected on the Barrage Capital website. This second policy is also available on the Barrage Capital website.
- is also supplemented by the following internal procedures:
    - Security Incident Management Policy,
    - Procedure in the event of a leak of personal data,
    - Procedure for requesting access to personal information,
    - Procedure for requesting de-indexing and deletion of personal information,
    - Procedure for destroying and anonymizing personal information.

Principles governing the protection of personal information

1 - Responsability

Barrage is responsible for the personal information under its management.

Barrage designates the Chief Compliance Officer as the Privacy Officer (hereinafter, the “Officer”).

For any requests or questions regarding this Policy, please contact the Officer at 514-903-7243 or by email at info@barragecapital.com.

The role of the Officer covers the following points:

- Ensure that Barrage complies with the legislative provisions regarding the management and protection of personal information.

- Ensure that Barrage has implemented the necessary measures to protect the confidentiality of the personal information held.
- Receive information requests, access to files and complaints, and deal with them in a timely and satisfactory manner.
- See that all staff are trained and aware of the protection of personal information.

More specifically, the tasks of the Officer are:

- Approve the policies and practices regarding personal information that the company must establish and implement.
- Participate in privacy factor assessments concerning certain information or electronic service delivery systems and suggest measures to ensure the protection of personal information processed within these systems.
- Record any communication (made without consent) to a company or public body that could mitigate the damage caused by a confidentiality breach and take part in the assessment of the damage caused by a confidentiality breach.
- Record and communicate to clients and relevant organizations any confidentiality breaches.
- Receive and respond to requests for access and rectification as well as requests related to data portability and the right to be forgotten.

2 – Definition of personal information

For the purposes of this policy, we will use the definition contained in the *Act Respecting the Protection of Personal Information in the Private Sector*, which defines as follows:

“any information which relates to a natural person and allows that person to be identified.”

3 – Determination of the purposes for collecting information

The purposes for which Barrage collects personal information are:

- To enter into an employment contract.
- To provide portfolio management services.

These purposes are specified to the individual before or at the time the personal information is collected.

4 – Consent

All individuals must be informed and consent to any collection, use or communication of personal information concerning them.

The consent of the individual concerned will be explicit and without any deduction on the part of Barrage. It will meet the following criteria:

- Free: expressed without conditions, constraints, or promises.
- Informed: formulated with awareness of its scope.
- Specific: authorizing the disclosure of personal information for a given purpose.
- Time-limited: valid for the duration required to achieve the purposes for which it is requested or for the duration prescribed by the regulations (whichever is longer).

Consent from potential clients is obtained verbally and that of clients is obtained in writing in the file opening form.

The only time Barrage will collect or disclose personal information without consent of the person concerned will be in circumstances required by law.

5 - Limitation of collection

Barrage can only collect the personal information necessary for the purposes determined and must proceed in an honest and lawful manner.

Barrage collects only the type and amount of protected information that it needs in an essential way for its activities and for the purposes set out during the collection:

For potential clients and clients

Personal information collected from customers will be used only for the purposes of providing services of Portfolio Management. The information requested is required under:

- Securities regulations (know your client, insider declaration).
- Anti-money laundering regulations specifically regarding the identity of account holders and source of funds.
- Tax regulations.
- Criminal regulations.
- Administration of the account by the trustee.
- The eventual transfer of assets from another financial institution.

For employees

The personal information collected will be used within the framework of the employment contract between Barrage and the employee.

6 – Limitation of use, communication and retention

Personal information must not be used or communicated for purposes other than those for which it was collected unless with the consent of the person concerned or as required by law. Personal information should not be retained by Barrage longer than necessary for the fulfillment of the identified purposes.

Use

Personal information is used only by persons who need this information in the performance of their duties relating to the portfolio management mandate and personnel management. They will in no case be used for purposes that are not relevant in this context.

Communication

Barrage communicates confidential information only to the external parties necessary for the exercise of its activities: regulatory authorities and service providers such as trustees, auditors and communication platforms. When Barrage uses these external parties, it ensures that the protection of personal information meets confidentiality requirements.

Barrage does not sell personal information or client lists to anyone. The discretionary portfolio management agreement provides that the identity of the client is not revealed to third parties, unless authorized by him.

Retention

Barrage will not retain personal information beyond prescribed retention periods, regardless of the medium used.

The retention period shall not exceed the longer of the following deadlines:

- The duration necessary to fulfil the authorized purposes, or
- The deadlines prescribed by legal requirements.

7 – Accuracy

Personal information must be as accurate, complete and up-to-date as required by the purposes for which it is used.

The personal information used by Barrage must be as accurate as possible and complete in order to minimize the possibility that erroneous information is used to make a decision about a client or employee.

In particular, certain personal information concerning the financial situation of clients may have an impact on the management of their assets. Clients must inform Barrage of changes to their file.

Barrage will update this information, when necessary, to meet the identified purposes, or upon notification by the person concerned if any information is inaccurate or out of date.

8 – Security measures

Personal information must be protected by security measures corresponding to their degree of sensitivity.

The necessary measures are put in place on the physical, administrative and technological levels in order to prevent loss, theft, consultation, communication, copying, use, modification, destruction or any other unauthorized use.

In all cases, the information is kept in a safe place, protected against unauthorized access and kept only for the time necessary. These measures apply regardless of the form in which it is stored.

Personal information communicated to third parties under contractual agreements must specify the confidential nature of this information and the purposes for which it is intended.

All Barrage employees who have access to personal information are required, as a condition of employment, to respect the confidentiality of such information.

9 – Transparency

Barrage must make available to any person in an easily accessible manner precise information on its policies and practices concerning the management of personal information. This policy will be given to anyone who requests it.

10 – Access to personal information

Barrage must inform any person who so requests of the existence of personal information concerning them, of their use and of the fact that they have been communicated to third parties, and allow them to consult it. It will also be possible to contest the content of the information and have it amended as appropriate.

Upon written request to the person responsible for the protection of personal information, any person concerned may consult their file. In order to ensure the protection of personal information, a client or an employee may be required to provide sufficient information for Barrage to provide access to the file in a secure manner.

Barrage will provide the personal information requested within a reasonable time (maximum 30 days). The information will be provided in an understandable and complete manner.

This right of access and modification covers:

- The right to consult the file free of charge.
- The right to have incorrect information corrected free of charge.
- The right to obtain a copy of the file for a reasonable fee covering the costs incurred in this regard, including the person concerned will be notified beforehand.
- The right to obtain the list of third parties to whom Barrage has or could communicate personal information for the exercise of its activities.

In certain circumstances provided for by the regulations, Barrage will not be able to provide the information requested. The reasons will be communicated to the applicant.

11 – Possibility of filing a complaint against non-compliance with the principles

Anyone must be able to complain about non-compliance with these principles by contacting the person responsible for enforcing them.

If a person concerned wishes to file a complaint relating to the exercise of the rights resulting from this policy or to any situation related to the protection of personal information, he may do so by contacting the designated person in charge.

Any complaint will be studied carefully in order to ensure an adequate treatment. The person will be informed of the outcome of the investigation into their complaint. If the complaint is justified, Barrage will take the appropriate measures as soon as possible, including modifying its policies and procedures if necessary.

In the event of a disagreement with Barrage in the exercise of the rights set out herein, the person concerned may contact the Office of the Privacy Commissioner of Canada.

12 – Breach of security measures

Barrage has the obligation to report to the Privacy Commissioner of Canada any breach of security measures (unauthorized communication, loss of personal information or unauthorized access to it) involving personal information under its control if it is reasonable to believe, in the circumstances, that the breach of security safeguards creates a "real risk of serious harm to an individual.

Serious harm includes bodily harm, humiliation, damage to reputation or relationships, financial loss, identity theft, adverse effect on credit reports, damage to or loss of property, and loss of employment or business opportunities or professional activities.

Factors relevant to determining whether a breach of security safeguards poses a real risk of serious harm include:

- the degree of sensitivity of the personal information involved in the breach of security safeguards and,
- the likelihood that these have been misused or are in the process of being misused.

Barrage keeps a record of all personal information security breaches it manages whether or not there is a real risk of serious harm. In other words, every breach of security measures must be logged.

Barrage is required to notify the person concerned of any breach of the security measures relating to personal information concerning him and under his management, if it is reasonable to believe, in the circumstances, that the breach presents a real risk of serious harm to them.

For more details, it is possible to consult the documents on the website of the Office of the Privacy Commissioner of Canada.

13 – Disclosure of the Policy

Barrage undertakes to make this policy available on request and to publish it on its website.

14 – Application by employees

All Barrage employees must respect and apply personal information management policies and procedures.

15 – Privacy Impact Assessment

In order to fully understand the importance of managing personal information, Barrage Capital conducted a Privacy Impact Assessment. This analysis concludes the current IT system includes sufficient security standards to protect personal information.

16 – Destruction and anonymization

Barrage has implemented the following policies regarding the destruction and anonymization of personal data.

17 – List of authorized partners

Barrage must frequently share, request or transfer personal information of clients to the following business partners :

- CIBC-Mellon;
- FundSERV;
- Other financial institutions with client authorization;
- Canadian regulators, including AMF, OSC and FINTRAC.

18 – Crisis management

Barrage undertakes to set up a crisis management team for any major incident that has caused a breach in the security of personal information.

This crisis management team could notably be made up of an internal manager, external consultants, and/or the police services.