ACM Privacy Policy

1. General

This section outlines general principles and (non-securities related) legal requirements, regarding client and former client privacy and the confidentiality of client's and former client's information, that govern the Company's conduct. In this section, the term "**client**" includes Unitholders and former Unitholders.

2. Principles of Privacy Law

The following are the principles of fair information practices incorporated into the *Personal Information Protection and Electronic Documents Act* (Canada) ("**PIPEDA**"). Every business that carries on "commercial activities" (defined broadly) is subject to the application of PIPEDA as it relates to the collection, use and disclosure of personal information (information about an identifiable individual, with the exception of the name, title, business address and business telephone number of an employee of an organization) ("**Client Information**"). PIPEDA only applies to information about human beings.

The Company is required to comply with PIPEDA in all of its business practices that involve personal information about individuals, as opposed to institutional, clients.

Protecting personal information provided to us by clients and using, disclosing and retaining it in accordance with PIPEDA is a key value of the Company.

The following set of guidelines, based on the ten principles in Schedule 1 to PIPEDA, supplement the Company's Privacy Policy. A copy of the Company's Privacy Policy may be obtained from the CCO.

Principle 1 – Accountability

All Company Personnel are responsible for Client Information (and confidential information about the Company) to which they have access as a result of their relationship with the Company and for compliance with the Company's Privacy Policy. The CCO is responsible for the Company's compliance with PIPEDA.

All inquiries or concerns regarding the use of Client Information, including information that has been transferred by the Company to a third party (for example, for processing), must be directed to the CCO**,** as the first point of contact at the Company. The CCO will then take the necessary action, including escalating inquiries or concerns to the UDP as appropriate. The CCO may also bring in other departments of the Company, as necessary, to assist in resolving the inquiry or concern.

Principle 2 - Identifying Purposes

The purposes for which Client Information is collected and used must be identified, documented and disclosed to clients at or before the time their information is collected.

The Company is only permitted to collect, use, disclose and retain Client Information to the extent necessary to fulfill the purpose for which the information was collected.

Before the Company may use Client Information for a purpose not previously identified to the client, the new purpose must be identified and documented, and the CCO must approve in writing the new purpose and the means to obtain client consent. Unless the use is required by law, client consent must be obtained before his or her information may be used for the new purpose.

The Company collects Client Information for the following purposes:

(a) Assessing the eligibility of an individual to invest in units of the Funds;

(b) Providing services to clients in relation to their investment in the Funds;

(c) Verifying creditworthiness of clients;

(d) Maintaining records for the Funds;

(e) Complying with statutory and regulatory requirements (such as establishing the identity of each client);

(f) Providing clients with the best possible service and protecting the Company and its clients from error and fraud; and

(g) For any other purpose related to the products and services of the Company or its affiliates to which clients may consent, including to provide Fund information and updates.

Principle 3 – Consent

Knowledge and consent of clients are required for the collection, use and disclosure of Client Information.

The consent obtained by the Company will generally be express consent, with notice of the purposes of collection and other relevant information being provided to clients in subscription agreements or similar documents, Client Information Forms or through the Company's Privacy Policy.

Subject to restrictions imposed by law or under a contract and reasonable notice, consent may, at any time, be withdrawn by a client. The Company must inform clients where there are implications of withdrawing or refusing their consent.

Principle 4 - Limiting Collection

As mentioned above, Client Information is not to be collected indiscriminately. The amount and the type of Client Information collected must be limited to that which is necessary for the purpose of the collection identified to the clients by the Company.

Principle 5 - Limiting Use, Disclosure and Retention

Caution should be exercised in regard to the disclosure of Client Information. In general, Client Information should only be disclosed for the purpose for which it was collected, with the express consent of the client or as required by law. If there is any doubt, the Company Personnel should speak to the CCO prior to disclosing Client Information. In some circumstances, for example where it is necessary in connection with the provision of a service and client consent has been obtained, the Company may disclose Client Information to an affiliate, the Funds or financial service providers, such as banks and others involved in financing or facilitating transactions by the Company or operations of the Company.

As mentioned, the Company may be required by law to disclose Client Information to taxation and regulatory authorities and agencies. In this regard, the Company may have to file with the appropriate securities commission, a report that includes Client Information such as the client's name and address, the types of securities issued, the date of issuance and the purchase price of securities issued to the client. Such information is collected indirectly by securities regulators, under the authority granted to them in securities legislation, for the purposes of the administration and enforcement of the legislation. For a description of additional circumstances under which the Company may disclose Client Information without the client's knowledge or consent, see section 5 of PIPEDA.

The Company will not sell client information.

Client Information will be retained for a period of seven years following the end of the client relationship. After seven years, all client documentation will be destroyed in a manner commensurate with its sensitivity unless there are securities laws or other legal requirements that require its retention.

The Company may transfer Client Information to service providers under contract to the Company that provide accounting, legal, tax preparation and like services. The Company remains responsible for Client Information while it is in the hands of third party service providers. The Company will protect the information (and the Company) by requiring in its contractual relationships with its service providers that the service providers afford Client Information the same level of protection as it is given by the Company.

Principle 6 – Accuracy

Client Information must be as accurate, complete, and up to date as necessary for the purposes for which it is to be used and will only be routinely updated where necessary for those purposes.

Where a client demonstrates that Client Information under the Company's control is inaccurate or incomplete, the CCO should take a copy of proof of the accurate or complete information and oversee the process taken by the Company to update this information in a timely manner.

Principle 7- Safeguards

Client Information will be protected against loss, theft, unauthorized access, use, disclosure, copying, or modification by safeguards appropriate for sensitive information.

Client Information (and confidential information of the Company) will be retained in a designated secure area or electronic database.

Some examples of the safeguards used to protect Client Information include:

(a) Physical Measures: i.e. locking filing cabinets in which Client Information is stored and restricting access to offices in which Client Information may be accessible; and ensuring care in the disposal or destruction of Client Information;

(b) Organizational Measures: i.e. security clearance is required for anyone entering areas in which Client Information is accessible and access to Client Information is restricted to personnel who "need to know" the information to provide a service; regular training and reminders to Company Personnel of the importance of safeguards; contractually requiring any service provider to provide comparable security measures; and verifying the identity of a caller and their right to access information prior to disclosing Client Information; and

(c) Technological Measures: i.e. passwords for computer terminals.

Company Personnel are individually responsible for ensuring the confidentiality, appropriate use and protection of all Client Information to which they have access.

The Company will periodically review and update its security policies and controls as technology changes to ensure ongoing security of Client Information.

The Company may refuse to disclose certain information relating to its security policies and controls where disclosure of such information would negatively impact the integrity of the security policies and controls.

Principle 8 – Openness

Clients have a right to access the Company's Privacy Policy which includes information about its management of Client Information including contact information for the Privacy Officer and the means by which a client may gain access to and request the correction of his or her Client Information being held by the Company.

Principle 9 - Individual Access

On request, a client shall be informed of whether or not the Company is holding his or her Client Information, the use to which it has been put by the Company and the organizations to which it has been disclosed or the type of organizations to which it may have been disclosed where more precise information is not available.

Requests for access must be made in writing. Access to a client's own Client Information will be provided except where doing so would likely reveal personal information about a third party that cannot be severed from the Client Information. Access may also be withheld where:

(d) The Client Information is protected by solicitor-client privilege;

(e) Providing access would reveal confidential commercial information;

(f) Providing access could reasonably be expected to threaten the life or security of another individual;

(g) The Client Information was collected without consent because obtaining consent could have compromised the availability or accuracy of the information and the information is required for investigating the breach of a contract, federal or provincial law;

(h) The information was generated in the course of a formal dispute resolution process; or

(i) The information is required to be kept confidential under other applicable laws.

The Company will endeavour to respond to requests for access within 30 days unless responding in that time frame would unreasonably interfere with its business or information necessary to make a decision on access is not available in that time frame. In such cases, the Company may extend the time for responding to an access request by 30 days or the period that is required to convert Client Information into an alternative format. The Company will give notice to the client where it requires an extension and include the reasons for the extension as well as advice that the client may make a complaint to the Office of the Privacy Commissioner of Canada ("**OPC**") in respect of the extension. It is important for the Company to respect the time lines, as a failure to respond to an access request within the time lines will be deemed to be a refusal of the request.

If a client has a sensory disability, the Company will provide access to Client Information in an alternate format as agreed upon with the client. The Company will be afforded reasonable time in order to convert the Client Information into the alternative format.

Prior to the release of Client Information, the CCO must confirm the identity of the client by reviewing two pieces of photo identification. Photo identification must be presented to the CCO in original form, or alternatively, a photocopy will be accepted where a notary or lawyer has declared in writing that they have reviewed the original identification. Written documentation of this review will be retained by the CCO.

The Company will inform the client in writing if it refuses his or her request for access, setting out the reasons for the refusal and the right of the client to complain to the OPC. Information that is the subject of a complaint must be retained by the Company until the client's rights are exhausted.

The Company will process access requests. The costs of these access requests, if any, will be paid by the client, but may be waived by the Company in its sole discretion. As such, prior to proceeding with such access request, the Company will inform the client that submits an access request of the approximate cost of the access request and will obtain approval to proceed from the client.

Specific rules apply in regard to requests for access to information provided to government agencies for purposes including law enforcement and all such requests should be directed to the CCO.

Principle 10 - Challenging Compliance

A client may address any concerns with respect to the Company's compliance with the above principles or the Company's Privacy Policy to the CCO.

The Company has procedures regarding client complaints which Company employees must explain to clients if concerns about Client Information management are raised. The complaint process to be followed is that outlined in section **[XIV]** "Complaints").

As mentioned above, clients have the right to challenge the accuracy and completeness of their Client Information and to have it amended as appropriate.

Breach of Security Safeguards Reporting

The Company has an obligation to notify individuals in cases of a breach of security safeguards and report to the OPC if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. Additionally, the Company notifying an individual in the event of a breach must also notify any other organization that may be able to mitigate harm to affected individuals and must maintain a record of any data breach that the organization becomes aware of.

A report of a breach of security safeguards to the OPC must be in writing and contain:

- a description of the circumstances of the breach and, if known, the cause
- the day on which, or the period during which, the breach occurred;
- a description of the personal information that is the subject of the breach;
- an estimate of the number of individuals in respect of whom the breach creates a real risk of significant harm;
- a description of the steps that the organization has taken to reduce the risk of harm to each affected individual resulting from the breach or to mitigate that harm;
- a description of the steps that the organization has taken or intends to take to notify each affected individual of the breach; and
- the name and contact information of a person who can answer, the OPC's questions about the breach on behalf of the organization.

The Company shall also notify the affected individuals of a breach. The notification shall contain sufficient information to allow the individual to understand the significance of the breach to them and to take steps, if any are possible, to reduce the harm that could result from it or to mitigate that harm. The content of the notification provided by the Company to an individual affected by a breach of security safeguards must contain:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred;
- a description of the personal information that is the subject of the breach;
- a description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm;
- a description of the steps that the affected individual could take to reduce the risk of harm resulting from the breach or to mitigate that harm;
- a toll-free number or email address that the affected individual can use to obtain further information about the breach; and information about the organization's internal complaint process and about the affected individual's right to file a complaint with the OPC.

The Company may also include in the notification to individuals affected sources of information designed in protecting against identity theft (e.g. online guidance on the OPC website and Innovation, Science and Economic Development Canada website).

The manner in which the Company gives notification to individuals may be conducted either through direct or indirect notification. Direct notification is to be given to the affected individual; (i) by email or any other secure form of communication if the affected individual has consented to receiving information from the Company in that manner; (ii) by letter delivered to the last known home address of the affected individual; (iii) by telephone; or (iv) in person. Indirect notification may be given to the affected individual by the Company if giving direct notification would cause further harm to the affected individual, if the cost of giving direct notification is prohibitive for the Company or if the Company does not have contact information for the affected individual (or if the information that it has is out of date). When indirect notification is used, the Company will either post a conspicuous message posted on the Company's website for at least 90 days, or by means of an advertisement that is likely to reach the affected individuals.

The Company shall keep and maintain a record of every breach of security safeguards involving personal information under its control for 24 months after the day on which the Company determines that the breach has occurred and the record must contain information pertaining to the breach that enables the OPC to verify compliance. The breach report to the OPC may be used by the Company as a record of the breach of security safeguards. Failure to report breaches as prescribed by PIPEDA or to keep required records will subject the Company to monetary penalties.

References

Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (Canada)
Section 5 of the *Personal Information Protection and Electronic Documents Act* (Canada)
Sections 10.1 through 10.3 of the *Digital Privacy Act*
Sections 2 to 6 of the *Breach of Security Safeguards Regulations*