INTERNAL PRIVACY and BREACH POLICY

Fernhill Financial Corporation ("Fernhill")

Summary

These privacy policies and procedures outline Fernhill's commitment to privacy and explains the principles that guide us in protecting the privacy and confidentiality of personal information. In addition, the policy also outlines the procedures to be followed in the event of a breach of privacy.

All staff, including directors, officers, employees, licensed representatives and other persons or third parties who act for, or on behalf of, Fernhill, are required to comply with this privacy policy and procedure. Staff members must ensure this is communicated to all interested parties and that they take all necessary means to limit, without delay, any violation they are made aware of and to immediately report privacy breaches to the Privacy Officer responsible for the protection of personal information as defined in our privacy principles noted below.

The objective is to ensure that:

(a) Fernhill is compliant with regulatory and self-regulatory requirements regarding Privacy ("Regulations");

(b) A client's Privacy is handled in a professional manner, in a secure environment and appropriately monitored;

The Privacy Officer

(1) **Jared Webb** is hereby designated as the Privacy Officer and is responsible for the application of this policy and,

(2) all inquiries/complaints shall be directed to **Jared Webb** as the Privacy Officer.

Privacy Training

Fernhill requires and provides initial and ongoing privacy training for all staff to ensure compliance with the Canada's Personal Information Protection and Electronic Documents Act "PIPEDA."

Fernhill's Commitment

Our clients are our business. Fernhill is entrusted with some of the most sensitive personal information. We respect that trust and want our clients to be aware of our commitment to protect the information they provide in the course of doing business with our firm.

We collect personal information in compliance with applicable laws and ethical business practices in order to provide services and to conduct business. We limit the information that we collect to that which is necessary for, or related to, these purposes.

Fernhill abides by these **Ten Privacy Principles**. These Principles are based on the federal government's privacy legislation, the *Personal Information Protection and Electronic Documents Act*

1. Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

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.

3. Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.

4. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfillment of those purposes.

6. Accuracy: Personal information shall be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used.

7. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness: An organization shall make readily available to individuals, specific information about its policies and practices relating to the management of personal information.

9. Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Information Collection and Use

Fernhill collects the information required to complete the task for which it is engaged, whether that is insurance, money products or financial plans.

Personal information is information that refers to you specifically. We will use fair and lawful means to collect your personal information. We will only collect information that is pertinent and consistent with the purposes of the collection. Whenever practical, Fernhill will collect the required information directly from the client, or from their authorized representative(s), in completed applications and forms, through other means of correspondence, such as the telephone, mail or the internet, and through their business dealings with the firm.

What Fernhill needs to know and why

Fernhill collects information from you and about you, only with your consent, or as required or permitted by law. In general, Fernhill will collect personal information such as your name, address, telephone number(s) or other identifying information, such as your Social Insurance Number (SIN) or date of birth.

The type of additional information that the firm gathers will depend on the type of product or service involved. The information gathered may be financial, which would include such information as place of employment, annual income, assets and liabilities. It may be investment or advice related, requiring information on such things as your financial goals and retirement plans. If the client is applying for insurance or group insurance benefits, it may also include health information or lifestyle related information, such as their occupation, travel history and plans, driving record or criminal record.

Consent

The consent is for Fernhill to establish a file and collect and maintain personal, medical & financial information and is to be signed by the client and placed in their file.

Protection of Personal Information

With access to client information, Fernhill understands the need to keep the information protected and confidential. Our procedures clearly communicate that we are to use the information only for the intended purpose(s).

All employees of Fernhill are required to sign a confidentiality agreement upon commencement of employment.

Retention of Personal Information

We will only keep client's personal information in our records for as long as it is needed to fulfill the identified purposes, or as required or permitted by law.

Privacy Choices

Clients may request copies of our privacy policies and procedures at any time.

Clients may request access to their information. We will respond to this request as quickly as possible, but no later than 30 days after the receipt of the request.

Clients may withdraw their consent at any time by contacting the Privacy Officer. However, they will be made aware that failure to provide adequate information may prevent Fernhill from completing the task for which we were engaged.

Clients may file complaints about our privacy procedures as well as a breach in our privacy policy. Complaints should be received in writing and forwarded to the Privacy Officer. The Privacy Officer will contact the client and obtain all details. The Privacy Officer will then review the circumstances of the complaint and determine if there is reason to alter the existing privacy policy. Insurance carriers should be notified of any complaint involving their clients/products.

Exception to client access

Organizations must refuse an individual access to personal information:

- if it would reveal personal information about another individual unless there is consent or a life-threatening situation
- if the organization has disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct the organization to refuse access or not to reveal that the information has been released. The organization must refuse the request and notify the Privacy Commissioner. The organization cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Privacy Commissioner was notified of the refusal.

Organizations may refuse access to personal information if the information falls under one of the following:

- solicitor-client privilege
- confidential commercial information
- disclosure could harm an individual's life or security
- it was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner must be notified)
- it was generated in the course of a formal dispute resolution process.