PRIVACY POLICY

My Commitment

As a financial advisor, I am trusted with some of my clients' most sensitive personal information. I must respect that trust and need my clients to be aware of my commitment to protect the information they provide in the course of doing business with me.

Principles of PIPEDA

There are 10 principles that I must follow to be in compliance with PIPEDA.

1. **Accountability**
   I am responsible for personal information under my control and I am the designates individual accountable for the my compliance with the following principles.

2. **Identifying Purposes**
   The purposes for which personal information is collected shall be identified by me 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 me. 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**

I shall make readily available to individuals specific information about my 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 me for compliance purposes.

Applicability

The Act is applicable to personal information only. However, it has been suggested that in keeping with the spirit of the law, PIPEDA should also be applied to information obtained on closely-held corporations which would be most, if not, all of our corporate clients. This policy applies to all myself and any of my employees, if applicable. This policy also applies to all consultants and third parties contracted by me.

The Privacy Officer

I am responsible for these policies & procedures, however I also report to various designated compliance staff at the various insurance MGAs through which I place my life insurance business. In those cases, the designated Policy Officer of each of those insurance MGAs should be reached for inquiries/compliants.

Information Collection and Use

I collect the information required for me to complete the task for which I was engaged, whether that is insurance, money products or financial plans.

This information may include, but are not limited to:

Name
Date of Birth/Date of Death
Social Insurance Number
Home Address(s)
Work Address(s)
Telephone Number(s), Fax Number(s)
Email Address(s)
Marital Status
Financial Income/Expense Info
Lawyer(s)
Banker(s)

Bank information
Investment advisor and account information Financial Statements
Medical Information

Consent

The consent for me to establish a file and collect and maintain personal information is done using the Privacy Protection Notice which is to be signed by the client and placed in their file.

Protection of Personal Information

As a Financial Advisor I am granted access to client information and must understand the need to keep the information protected and confidential. My training procedures clearly communicate that I am to use the information only for the intended purpose(s).

Any staff I may hire will be required to sign a Confidentiality Agreement upon commencement of employment.

Retention of Personal Information

I will retain my completed client files for a minimum period of seven years. Any files where there were complaints or legal issues will be kept indefinitely.

Destruction of Personal Information

As a Financial Advisor that has client personal information in its control, I do not simply throw it away in the trash. I securely disposes of it.

My goal is to irreversibly destroy the media which stores client personal information so that personal information cannot be reconstructed or recovered in any way. When going through the process of disposal, I also destroys all associated copies and backup files.

Privacy Choices

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

Clients may request access to their information. I must 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 me of the designated Privacy Officer at the insurance MGA with which I do business. However, they will be made aware that failure to provide adequate information may prevent me from completing the task for which I was engaged.

Clients may file complaints about my privacy procedures as well as a breach in my privacy policy. Complaints should be received in writing and forwarded to the Privacy Officer at the insurance MGA with which I do business. 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

I 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 I have disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct me to refuse access or not to reveal that the information has been released. I must refuse the request and notify the Privacy Commissioner. I 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.

I 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.

Privacy Breach

A privacy breach involves improper or unauthorized collection, use, disclosure, retention or disposal of personal information. A privacy breach may occur within an institution of off-site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

Where a privacy breach occurs, I am required to:

1. Notify individuals about security breaches which pose a real risk of significant harm, except where prohibited by law;
2. Report breaches of security safeguards to the Office of the Privacy Commissioner involving personal information that pose a real risk of significant harm;
3. Notify other organization or government institutions that may be able to mitigate harm; and
4. Keep records of all privacy breaches for 24 months.

Examples of situations that could result in the disclosure of, or access to, personal information by unauthorized parties are:

- The theft, loss or disappearance of equipment or devices containing personal information;
- The sale or disposal of equipment or devices containing personal information without purging prior to sale or disposal;
- The transfer of equipment or devices without adequate security measures;
- The use of equipment or devices to transport or store personal information outside the office for telework or off-site work arrangements without adequate security measures;
- The inappropriate use of electronic devices to transmit personal information, including telecommunication devices;
- Intrusions that result in unauthorized access to personal information held in office buildings, file storage containers, computer applications, systems, or other equipment and devices;
- Low level of privacy awareness among employees, contractors or other third parties that handle personal information;
- Inadequate security and access controls for information in print or electronic format, on site or off-site;
- The absence of provisions or inadequate provisions to protect privacy in contracts or in information-sharing agreements involving personal information;
- Insufficient measures to control access and editing rights to personal information, which may result in wrongful access to, and the possible tampering with, records containing personal information;
- Phishing or the use of deceptive tactics to trick an individual into providing their personal information either directly or by going to a fake web site. For example, an individual pretending to perform system maintenance calls an employee to obtain his or her security password; and
- Pharming or the use of a fake copy of an official web site to redirect to a malicious web site in order to steal information without the users knowledge. This method takes advantage of the weaknesses in the Data Network System (DNS). For example, an individual accesses what he or she believes is an official web site and submits personal information as requested by the site. The individual is unaware that he or she has been redirected to a fake copy of the official web site.

Containment of Privacy Breach

If a privacy breach occurs, I will take the following steps within 48 hours to manage and contain the situation as best it can:

1. **Freeze Everything**

   Take affected devices offline but do not shut them down or make any changes just yet. The goal here is to stop any ongoing activity by limiting communication to and from the impacted systems but not commit any action which might erase clues, contaminate evidence or otherwise inadvertently aid the attacker. In the case of virtual machines or

other systems you can snapshot, it is recommend doing so now so that you will have a recorded version of the system at the time the breach was occurring. You can analyze the snapshot later in an offline state.

2. **Ensure auditing and logging is ongoing**

Ensuring that existing system auditing remains intact and has been operational will be one of the most useful steps you can take to determine the scope of the breach and devise remediation methods. If auditing has been disabled (to cover someone's trail for instance), restore it before proceeding; it will also assist in establishing whether breach activity is ongoing and when the breach can be safely determined to have concluded.

3. **Change passwords or lock credentials**

Changing passwords or locking credentials is a common tactic in preparing to investigate a data breach since it will help ensure the cessation of said breach if it is ongoing, and data breaches commonly rely on compromised passwords and credentials. Make sure to apply this step to all involved accounts, whether confirmed or suspected.

4. **Determine the impact**

Now the investigation starts. Figure out what happened here; what information was accessed, what systems were compromised, and which accounts may have been utilized. You'll need the logs referenced in the prior step, as well as the tools discussed in step number two. Determine and establish the scope of the breach to formulate how to solve it.

5. **Determine how it happened**

It's not enough to remediate a data breach based on impact alone; you have to determine root cause or you may simply be slapping a temporary band-aid on the situation. Did someone erroneously give out their password? Was a system not patched for a particular vulnerability? Did someone plug an unauthorized laptop into the company network which then subjected the organization to malware? Or did an employee simply leave their unencrypted mobile device in a taxi cab and was then subjected to blackmail?

6. **Determine what needs to be done**

Now comes the step where you build out your remedy to seal the hull of the ship from the iceberg damage, so to speak. Establish whether you need to remotely wipe a stolen mobile device, update software, change network firewall rules, segregate subnets, run antimalware scans, increase logging and alerting or some other technical steps, get these planned out. Then enact them immediately.

7. **Communicate the details to the appropriate internal personnel**

   It's not just technical steps you need to worry about. There's also the communication and notification process. Who do have to involve to let them know the breach occurred, how it occurred, what details were involved, and what has to be done?

8. **Make public announcements and prepare for responses**

   This is never going to be the most fun of these steps, but quite likely it will be up to someone to make a public announcement, perhaps in the form of a press conference, series of emails, social media announcements, website announcements or any other form of communication which exists between the company and the outside world.

   Make sure to describe what the organization has done to remedy the breach, what it intends to do in the future, and what (if any) steps customers should take to protect themselves, such as by changing passwords, contacting credit card companies or placing fraud alerts.

   If possible, establish a hotline or name a specific group/contact information to address customer concerns regarding this breach so they can answer questions and provide guidance.

Evaluate Risks Associated with Privacy Breach

Personal data passes through many areas of a business, and it needs to be kept secure at all times, whether it's saved on a database, in hard-copy form and stored in an office, or being transferred to or from third parties. Each area has its own risk and below is a list of some of the most prominent risks:

1. **Web application vulnerabilities**, including injection flaws (which allow attackers to copy or manipulate data) and sensitive data exposure (which allows attackers to gather sensitive information).
2. **Operator-sided data leakage**, which consists of any failure to prevent the leakage of information containing or related to user data.
3. **Insufficient data breach response**, such as failing to inform affected data subjects about a possible breach or data leak.
4. **Insufficient deletion of personal data**, i.e. not deleting data subjects' information after a set period of time or when it is no longer necessary.
5. **Non-transparent policies, terms and conditions**, such as failing to provide sufficient information on how data is collected, stored and processed.
6. **Collection of inessential data**, including descriptive or demographic information that's not needed for the purposes of the system.
7. **Sharing data with a third party** without obtaining the data subject's consent.

8. **Outdated personal data**, including incorrect or bogus data, or the failure to update data when it's no longer correct.
9. **Missing or insufficient session expiration**, i.e. failing to effectively enforce session termination. This might result in an organisation collecting additional data without the user's consent.
10. **Insecure data transfer**, i.e. failing to provide data transfers over secure channels or to put in place mechanisms limiting the leak surface.

Prevention of Privacy Breach

To prevent a privacy breach, I should:

- Take privacy into account before making contracting decisions or entering into information-sharing agreements. I should include adequate privacy protection provisions, such as a requirements to immediately notify the proper authorities of a privacy breach;
- Provide regular and ongoing training to employees, managers and executives to ensure that they are aware of the requirements of these policies and procedures;
- Ensure that personnel working off-site are aware of their privacy and security responsibilities. This means ensuring that appropriate measures are taken to safeguard the personal information they handle off-site;
- Establish clear administrative controls that restrict access and editing rights to records containing personal information to only those employees who have a legitimate need to know, and for me to put in place appropriate audit trails to ensure that these administrative controls are functioning as intended;
- Use cryptography (encryption) to protect sensitive personal information stored in a computer or a portable storage device or being transmitted through email, on a company network, a wireless network, or across the Internet;
- Establish clear procedures for the use of wireless devices;
- As a general rule, do not send personal information by facsimile unless absolutely necessary. If you must fax personal information, consider the safeguards recommended by the Office of the Privacy Commissioner of Canada for faxing personal information;
- Purge all equipment and other electronic devices containing personal information before selling, disposing of, or transferring such equipment or devices;
- Empty security containers such as file cabinets, safes or mobile shelving units and ensure that no classified or protected material is left inside before selling or transferring them;
- Take precautions against "phishing" and "pharming":
    - Ensure that requests for personal information are valid and that individuals asking for personal information are who they claim to be;
    - Refuse to provide personal information in response to an unsolicited telephone call, fax, letter, email attachment or Internet advertisement;
    - Be on the lookout for clues indicating that a website may be fraudulent (i.e., spelling errors, unusual advertisements, or portions of the site that do not work properly);

    - Check the lock icon at the bottom of your browser to ensure that you are sending personal information over a secure connection; and
    - Verify the phone number and call the individual to determine validity if you have any concerns.
- Notify the Privacy Officer immediately of situations where personal data is at risk of being compromised and a potential privacy breach may occur.

Examples of best practices in managing privacy breaches include:

- Preliminary assessment and containment;
- Full assessment;
- Notification (to affected individuals and internal management where required);
- Mitigation and prevention;
- Notification to the Privacy Officer; and
- Sharing of lessons learned.

Should I become aware of a privacy breach, I will review my privacy policy and amend as required, as well as maintain a record of all privacy breaches.

- The record should include information as to the nature and extent of the breach, the type of personal information involved, the parties' involved, anticipated risks, steps taken or to be taken to notify individuals, any remedial action taken and whether the investigation determined it to be a material privacy breach.
- Records documenting privacy breaches should not contain personal information.

Notification of Privacy Breach

I will notify individuals whose personal information has been wrongfully disclosed, stolen or lost.

- I will notify all affected individuals whose personal information has been, or may have been, compromised through theft, loss or unauthorized disclosure, especially if the breach:
    - Involves sensitive personal data such as financial or medical information, or personal identifiers such as the Social Insurance Number;
    - Can result in identity theft or some other related fraud; or
    - Can otherwise cause harm or embarrassment detrimental to the individual's career, reputation, financial position, safety, health or well-being.
- Notification should occur as soon as possible following the breach to allow individuals to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.
- Consult with the Privacy Officer and with law enforcement authorities to determine whether notification should be delayed to ensure that any possible investigation is not compromised.

- Care should be exercised in the notification process to not unduly alarm individuals, especially where the institution only suspects but cannot confirm that certain individuals have been affected by the breach.
- It is always preferable to notify affected individuals by letter (first class recommended), by telephone or in person, unless the individuals cannot be located or the number of individuals is so large that the task would become too onerous.

In such cases, I could post a conspicuous notice on its web site or on log-in screens used to access departmental data and/or use major local or national media (television, radio, newspapers and magazines). I should use electronic mail only when the individual has previously consented to the receipt of electronic notices.

Notification of affected individuals should include:

- A general description of the incident, including date and time;
- The source of the breach (an institution, a contracted party, or a party to a sharing agreement);
- A list of the personal information that has been or may have been compromised;
- A description of the measures taken or to be taken to retrieve the personal information, contain the breach and prevent reoccurrence;
- Advice to the individual to mitigate risks of identity theft or to deal with compromised personal information (e.g., Social Insurance Number);
- The name and contact information of the Privacy Officer at the insurance MGA with which I do business with whom individuals can discuss the matter further or obtain assistance;
- A reference to the effect that the Privacy Officer has been notified of the nature of the breach and that the individual has a right of complaint, when applicable; and
- I should also inform affected individuals of developments as the matter is further investigated and outstanding issues are resolved.

Clean Desk Policy

Employees, if any, are responsible for clearing their desks when they leave the office at the end of the business day and I am is responsible for providing access to a paper shredder and storage space. The office manager or the employee's supervisor must check the office at the end of the business day and confiscate or destroy any folders, papers or portable storage media an employee might have left out on their desk. Consequences for policy non-compliance is a verbal warning and termination if continual breach of policy after already having received a verbal warning.

E-mail Privacy Disclosure Sample

Myself, and any Employees I may hire, using an e-mail address are required to include the following privacy disclosure in their e-mail signature:

This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this email.

Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. Email transmission cannot be guaranteed to be secure or error-free, as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender, therefore, does not accept liability for any errors or omissions in the contents of this message which arise as a result of email transmission. If verification is required, please request a hard-copy version.

Office Safeguards

In an effort to ensure the privacy of our client information I have implemented the following safeguards:

- Disclaimer on all e-mails, faxes etc.
- Clean desk policy
- All confidential materials to be removed from view at end of day, lunch, break time, etc.
- No information in view of public, on desks
- No discussion of client files outside the office
- Empty shredding file daily
- Lock shredding bin
- Password protected screensavers on all computers
- Any inquiry should be directed to the Privacy Officer
- All filing cabinets to be locked
- All waste paper containing personal information to be shredded
- Any person, client or broker, must identify themselves by a broker code, Social Insurance Number, Date of Birth, etc. in order to confirm identity
- Employees must be furnished with a copy of the privacy policy and sign off acknowledging that they have read it
- Staff are required to sign a Confidentiality Agreement
- Office is locked and alarmed and professionally monitored
- Complaint logs are maintained
- Certificates of Destruction are received for shredded material

PRIVACY PROTECTION NOTICE

1. **Client Record and Personal Information:**
   The personal information collected about you for the purposes identified in this Privacy Protection Notice is held in a record called the "client record". The personal information in your client record may include your name, address and telephone number, social insurance number, birth date, driver's license, passport number, income, net worth, account holdings and the name, address and social insurance number of your spouse and beneficiary. Depending on the investment/insurance or service you request, additional personal information may be held in your client record. For example, if you have established a pre-authorized payment plan, your financial institution account number is recorded.

2. **Providing Your Information to Me:**
   When you completed an application form or otherwise opened an account through me, you provided me with personal information including, where applicable, personal information concerning your spouse and beneficiary. You may have also provided me with information when you gave instructions to me about insurance and/or investments you had or wished to have. I collect this personal information, hold it in your client record, use it and when needed, disclose it for the purposes identified in this Privacy Protection Notice.

3. **Collecting, Holding, Using and Disclosing Information in Your Client Record:**
   I may collect, hold and use the information in your client record. I may also collect personal information from, and disclose personal information to, third parties for the following purposes:

   a. Identifying you and ensuring the accuracy of information contained in your client record.
   b. Establishing and administering your account, determining, maintaining, recording and storing account holdings and transaction information in your client record.
   c. Providing you with investment account statements and other information related to any insurance policies held, which you may request as needed to service your account.
   d. Understanding your insurance and/or investment needs and eligibility for products and services and recommending particular products and services to meet your needs;
   e. Protecting you against error and fraud.
   f. Meeting the legal and regulatory requirements of various statutes including provincial securities legislation and federal money laundering regulations.
   g. Verifying information previously given by you with any other organization when necessary for the purposes provided in this Privacy Protection Notice.

4. I may collect personal information about you from third parties for the purposes identified in this Privacy Protection Notice. These parties include other financial institutions, insurance/segregated fund companies and others who represent that they have the right to disclose the information.

   I may disclose to third parties personal information about you for the purposes identified in this Privacy Protection Notice. These parties include the insurance MGA with which I do business, other financial institutions, account statement preparation and mailing companies, Canada Post, courier and document storage companies and insurance/segregated fund companies. Other third parties could include Canadian government agencies such as the Canada Revenue Agency.

   When I transfer personal information to my service providers, I ensure by contractual means, that the transferred personal information is used only for the purposes for which the service provider

is retained. If you wish to withdraw consent to the continuation of this information sharing or discuss the implications of such withdrawal, please contact me through one of the means listed at the end of this notice. In some circumstances, legal requirements may prevent you from withholding consent. Your decision to withhold consent may limit my ability to deal with you and may also limit the products and services that I provide you, because the collection of information and the disclosure to certain third parties is a necessary part of making the product or service available to you.

Your personal information will not be shared with sales advisors of any other company without your consent.

5. **Using Your Social Insurance Number:**
   I am required by law to use your Social Insurance Number to facilitate required tax reporting to the Canada Revenue Agency. It may also provide the number to third parties engaged to provide income tax reports.

6. **Employees Who Have Access to Your Client Record:**
   If applicable, my employees may have access to your client record provided they have a specific need to know in connection with the purposes identified in this Privacy Protection Notice. Access is permitted only to the extent necessary for such purposes.

7. **Location of Your Client Record:**
   Your client records, in electronic or paper format, are kept at my office and/or the offices of the insurance MGA with which I do business. Paper records forming part of your client record may also be kept in secure offsite storage. Your client record may be transferred to other locations for disaster recovery purposes.

8. **Right to Access and Rectify Personal Information:**
   Except in limited circumstances prescribed by *the Protection of Personal Information and Electronic Documents Act (Canada)* and similar provincial privacy protection acts, you are entitled to access, through a written request, the personal information contained in your client record. You may verify this personal information and request that any inaccurate information be corrected. Please contact me through one of the means listed at the end of this notice. If your concerns have not been resolved to your satisfaction, you can contact the Privacy Officer at the insurance MGA through which I do business.

9. **Changes to Your Personal Information:**
   Please inform me promptly of any change in the personal information that you have previously provided. Contact information is provided below.

   I appreciate your business and promise to handle your questions or input regarding personal information in a prompt and courteous manner.

Advisor Name: _____

Advisor Phone Number: _____ Advisor Fax Number: _____

Advisor Email Address: _____

Advisor Business Address: _____

PRIVACY POLICY CONSENT

My Privacy Policy and Commitment to Protecting Your Privacy

I value your business and I thank you for your confidence in choosing me as your source for advice and products. As my client, you trust me with your personal information. I respect that trust and want you to be aware of my commitment to protect the information you share in the course of doing business with me.

Your Rights as they Pertain to Your Personal Information

- You have the right to know why an organization collects, uses or discloses your personal information.
- You have the right to expect an organization to handle your information reasonably and to not use it for any other purpose other than the one to which you consented.
- You have the right to know who in an organization is responsible for protecting your information.
- You have the right to expect an organization to protect your information from unauthorized disclosure.
- You have the right to inspect the information an organization holds about you and make sure it is accurate, complete and current.
- You have the right to expect an organization to destroy your information when requested or when no longer required for the intended purpose.
- You have the right to confidentially complain to an organization about how it handles your information and to the Privacy Commissioner of Canada if need-be.

How I Collect, Use and Disclose Your Information

When you do business with me, you share personal information, including sensitive medical information, which I keep in your file so that I may provide you with financial strategies, products and services that best meet your needs. I assume you consent for me to use this information in an appropriate manner. I may use and disclose this information in order to:

- Communicate with you in a timely and efficient manner
- Asses your application for investment, insurance and other services available to you by me
- Evaluate claims and underwriting risks when required
- Detect and prevent fraud
- Analyze business results
- Act as require or authorized by law

What I Will NOT Do With Your Information

I will not sell your information to anyone. Nor do I share your information with organizations outside of my relationship with you that would use it to contact you about their own products or services.

I Strive to Protect Your Personal Information

All employees, associated advisors and suppliers who are granted access to client records understand the need to keep this information protected and confidential. They know they are to use the information only for the purposes intended and this expectation is clearly communicated. I also established physical and systems safeguards, along with proper processes, to protect client information from unauthorized access or use.

Your Privacy Choices

You may withdraw your consent at any time (subject to legal or contractual obligations and on providing us reasonable notice) by contracting me or the Privacy Officer at the insurance MGA with which I do business. Please be aware that withdrawing your consent may prevent me from providing you with the requested products or services. I may occasionally use your personal information to advise you of products or services I believe may be of interest to you or fit your personal circumstances. If you would rather not receive this type of communication, please advise me or the Privacy Officer at the insurance MGA with which I do business.

I may be reached as follows:

Advisor Name: _____

Advisor Phone Number: _____ Advisor Fax Number: _____

Advisor Email Address: _____

Advisor Business Address: _____

Until advised otherwise, you have my consent to collect and maintain my personal information in my client file.

Signed this _____ day of _____, 20 _____.

Client Name: _____

Client Signature: _____