

BP Wealth & Insurance Inc.
P.O. Box 360
5104A – 50 Ave
Cold Lake, AB T9M 1P1
1-888-594-1857
www.bpgs.ca



Excalibur Executive Planning Inc.
#1350 – 5555 Calgary Trail NW
Edmonton, AB T6H 4P9
1-888-594-1857
www.excaliburplanning.com



Excalibur Executive Planning Inc./BP Wealth & Insurance Inc. /BP Group Solutions or BPGS Privacy Policy

Objective

To ensure that:

- a) **Excalibur Executive Planning Inc./BP Wealth & Insurance Inc./BP Group Solutions or BPGS** is in compliance with regulatory and self-regulatory requirements regarding Privacy (“Regulations”);
- b) **Excalibur Executive Planning Inc./BP Wealth & Insurance Inc./BP Group Solutions or BPGS** Client’s Privacy is handled in a professional manner, in a secure environment and appropriately monitored.

Policies

Person(S) Responsible:

- 1) _____ is hereby designated as responsible for the application of this policy;

Our Commitment

At **Excalibur Executive Planning Inc./BP Wealth & Insurance Inc./BP Group Solutions or BPGS** our Advisors and our clients are our business. As a financial services Company, we are trusted with some of our clients most sensitive personal information. We must respect that trust and need our clients to be aware of our commitment to protect the information they provide in the course of doing business with us.

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

- 1. Accountability:** An organization is responsible for the 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. Identification 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 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 purpose for which it is to be used.
7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitive of the information.
8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices 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.

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 employees of **Excalibur Executive Planning Inc./BP Wealth & Insurance Inc./BP Group Solutions or BPGS**. This policy also applies to all consultants and third party contracted by **Excalibur Executive Planning Inc./BP Wealth & Insurance Inc./BP Group Solutions or BPGS**.

The Privacy Officer

_____ is the privacy officer and all inquiries /complaints shall be directed to him.

Information Collection and Use

We collect the information required for us to complete the task for which we are engaged, whether that is insurance, or money products. The information collected may be per individual products or group products. Group products would include the collection of employee personal information. Examples of what could be collected are on the next page.

This information may include:

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)
Bankers(s)
Bank information
Investment advisor and account information
Financial Statements
Medical Information

Organization 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 federal or provincial law (the Privacy Commissioner must be notified)
- It was generated in the course of a formal dispute resolution process.

Privacy Breach

- Should we become aware of a privacy breach, we will review our privacy policy and amend as required.
- If necessary, the affected client/s will be notified as well as the insurance carrier.
- If necessary, we will notify our E&O insurance carrier

Consent

The Consent for us to establish a file and collect and maintain personal information is to be signed by the client and placed in their file.

Protection of Personal Information

As the principal, management and employees of **Excalibur Executive Planning Inc./BP Wealth & Insurance Inc./BP Group Solutions or BPGS** we are granted access to client information and must understand the need to keep the information protected and confidential. Our training procedures clearly communicate that we are to use the information only for the intended purpose(s).

Staff will be required to sign a confidentiality agreement upon commencement of employment.

Retention of Personal Information

We will retain our complete client files for a minimum period of seven years. Any files where there were complaints or legal issues will be kept indefinitely.

Privacy Choices

Clients may request of our privacy policies and procedure at any time

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

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

Clients may file complaints about our privacy procedure 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 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.

Schedule "A"

Office Safeguards

- Disclaimer on all emails, 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 desk
- No discussion of client files outside the office
- Empty shredding file weekly
- Lock shredding bin
- Password protected screensavers on all computers
- Any inquiry should be directed to the Privacy Officer
- All file 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, SIN #, DOB, etc. to confirm identity
- Employee 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
- Fax is set up to keep faxes in memory when office is closed
- Office is locked and alarmed and professionally monitored
- Complaint logs are maintained
- Certificates of Destruction are received and shredded