SCHEDULE D: PRIVACY POLICY

BACKGROUND AND POLICY

This privacy policy has been developed to comply with Canada's *Personal Information Protection and Electronic Documents Act* ("*PIPEDA" or the "Act"*) and the British Columbia *Personal Information Protection Act*. PIPEDA sets out rules for the collection, use and disclosure of personal information in the course of commercial activity as defined in the Act.

The Ten Principles of PIPEDA Summarized

The ten principles of PIPEDA that form the basis of this Privacy Policy are as follows:

1. Accountability: organizations are accountable for the personal information they collect, use, retain and disclose in the course of their commercial activities, including, but not limited to, the appointment of a Chief Privacy Officer;

2. Identifying Purposes: organizations are to explain the purposes for which the information is being used at the time of collection and can only be used for those purposes;

3. Consent: organizations must obtain an Individual's express or implied consent when they collect, use, or disclose the individual's personal information;

4. Limiting Collection: the collection of personal information must be limited to only the amount and type that is reasonably necessary for the identified purposes;

5. Limiting Use, Disclosure and Retention: personal information must be used for only the identified purposes, and must not be disclosed to third parties unless the Individual consents to the alternative use or disclosure;

6. Accuracy: organizations are required to keep personal information in active files accurate and up-to-date;

7. Safeguards: organizations are to use physical, organizational, and technological safeguards to protect personal information from unauthorized access or disclosure.

8. Openness: organizations must inform their clients and train their employees about their privacy policies and procedures;

9. Individual Access: an individual has a right to access personal information held by an organization and to challenge its accuracy if need be; and

10. Provide Recourse: organizations are to inform clients and employees of how to bring a request for access, or complaint, to the Chief Privacy Officer, and respond promptly to a request or complaint by the individual.

This Privacy Policy applies to Fort Capital Securities Limited's ('FCSL') Board of Directors, employees and contracted employees. As well, FCSL has third-party service providers sign confidentiality agreements prior to any transfer of an individual's personal information in the course of providing related information and/or services.

DEFINITIONS

“Business contact information” means information that would enable an individual to be contacted at a place of business and includes name, position name or title, business telephone number, business address, business email or business fax number. Business contact information is not covered by this policy or PIPEDA.

“Chief Privacy Officer” means the individual designated responsibility for ensuring that FCSL complies with this policy and PIPEDA. This person is the CCO who is Duncan Baird.

"Data base" means the list of names, addresses and telephone numbers of clients and individuals held by FCSL in the forms of, but not limited to, computer files, paper files, and files on computer hard-drives.

"Express consent" means the individual signs the contract, or other forms containing personal information, authorizing FCSL to collect, use, and disclose the individual's personal information for the purposes set out in the contract.

"Implied Consent" means the organization may assume that the individual consents to the information being used, retained and disclosed for the original purposes, unless notified by the individual.

“Personal Information” means information about an identifiable individual including name, age, home address and phone number, social insurance number, marital status, religion, income, credit history, medical information, education, employment information. Personal information does not include contact information (described below).

“Significant harm” includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

"Third Party" means a person or company that provides services to FCSL in support of the programs, benefits, and other services offered by FCSL.

PURPOSES OF COLLECTING PERSONAL INFORMATION

Unless the purposes for collecting personal information are obvious and the client voluntarily provides his or her personal information for those purposes, we will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.

We will only collect client, customer, member information that is necessary to fulfill the following purposes:

- To verify identity;
- To identify client preferences;
- To understand the financial needs of our clients;
- To open and manage an account;
- To deliver requested products and services;
- To deliver a high standard of service to our clients; and
- To meet regulatory requirements.

Consent

We will obtain client consent to collect, use or disclose personal information (except where, as noted below, we are authorized to do so without consent).

Consent can be provided orally, in writing, electronically, through an authorized representative or it can be implied where the purpose for collecting using or disclosing the personal information would be considered obvious and the client voluntarily provides personal information for that purpose.

Subject to certain exceptions (e.g., the personal information is necessary to provide the service or product, or the withdrawal of consent would frustrate the performance of a legal obligation), clients can withhold or withdraw their consent for FCSL to use their personal information in certain ways. A client's decision to withhold or withdraw their consent to certain uses of personal information may restrict our ability to provide our services. If so, we will explain the situation to assist the client in making the decision.

Limiting Collection

Personal information collected will be limited to the purposes set out in this Privacy Policy, FCSL contracts, and/or other documentation.

Use of Personal Information

Personal information will be used for only those purposes to which the individual has consented with the following exceptions, as permitted under PIPEDA:

- the organization has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law and the information is used for that investigation;
- an emergency exists that threatens an individual's life, health or security;
- the information is for statistical study or research;
- the information is publicly available;
- the use is clearly in the individual's interest, and consent is not available in a timely way;
- knowledge and consent would compromise the availability or accuracy of the information, and
- collection is required to investigate a breach of an agreement.

Disclosure and Transfer of Personal Information

We will only use or disclose client personal information where necessary to fulfill the purposes identified at the time of collection [or for a purpose reasonably related to those purposes such as:

- To contact our clients directly about products and services that may be of interest;

We will not use or disclose client, customer, member personal information for any additional purpose unless we obtain consent to do so.
We will not sell client, customer, member lists or personal information to other parties.

PIPEDA permits FCSL to disclose personal information to third parties, without an individual's knowledge and consent, to:

- a lawyer representing FCSL;
- collect a debt owed to FCSL by the individual or client;
- comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction;
- a law enforcement agency in the process of a civil or criminal investigation;
- a government agency or department requesting the information; or
- as required by law.

PIPEDA permits FCSL to transfer personal information to a third party, without the individual's knowledge or consent, if the transfer is simply for processing purposes and the third party only uses the information for the purposes for which it was transferred. FCSL will take measures to provide, by contractual or other means, that the third party protects the information and uses it only for the purposes for which it was transferred.

Retention of Personal Information

If we use client, customer, member personal information to make a decision that directly affects the client, customer, member, we will retain that personal information for at least one year so that the client, customer, member has a reasonable opportunity to request access to it.
We will retain client, customer, member personal information only as long as necessary to fulfill the identified purposes or a legal or business purpose.

Accuracy

We will make reasonable efforts to provide that client personal information is accurate and complete where it may be used to make a decision about the client or disclosed to another organization.

Clients may request correction to their personal information for accuracy and completeness clarifications. A request to correct personal information must be made in writing and provide sufficient detail to identify the personal information and the correction being sought.

If the personal information is demonstrated to be inaccurate or incomplete, we will correct the information as required and send the corrected information to any organization to which we disclosed the personal information in the previous year. If the correction is not made, we will note the clients' correction request in the file.

Safeguards

Use of Safeguards

We are committed to ensuring the security of client personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.
The following security measures will be followed so that client personal information is appropriately protected:

- the use of locked filing cabinets;

- physically securing offices where personal information is held;
- the use of user IDs, passwords, encryption, firewalls;
- restricting employee access to personal information as appropriate (i.e., only those that need to know will have access;
- contractually requiring any service providers to provide comparable security measures; and
- employees and/or Board of Directors are required to sign a confidentiality agreement binding them to maintaining the confidentiality of all personal information to which they have access.

We will use appropriate security measures when destroying client's personal information such as shredding documents and deleting electronically stored information. We will continually review and update our security policies and controls as technology changes regarding ongoing personal information security.

Breaches of Security Safeguards

Under PIPEDA, FCSL is required to report to the Office of the Privacy Commissioner ("OPC") and the individual whose information has been breached, any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The report is contained herein as Schedule 1.

The individual's notification will be conspicuous and shall contain sufficient information to allow the individual to understand the significance of the breach and any steps they can take to mitigate/reduce harm among other prescribed information. The notification shall be given directly to the individual as soon as feasibly possible.

In determining the real risk of significant harm FCSL will consider:

- the sensitivity of the personal information involved in the breach;
- the probability that the personal information has been, is being or will be misused; and
- any other prescribed factor.

See Schedule 2 for further detail.

If a breach occurs, FCSL will also notify any other organization or government institution of the breach if FCSL believes that the other party may be able to reduce the risk of harm that could result from it.

Record Keeping of Breaches

FCSL will keep and maintain a record of every breach involving personal information under its control, even if there is no obligation to report or give notice of the breach (i.e. the breach does not create a "real risk of significant harm" to an individual).

The record will contain any information that enables the Commissioner to verify the firm's compliance with the breach reporting and notification obligations. The firm will maintain the record for 24 months after the day on which it determines that the breach has occurred (and may retain same longer to comply with other legal requirements) and will provide the record to the Commissioner on request.

Records must contain any information that enables the OPC to verify compliance with breach of security safeguards reporting and notification requirements in sections 10.1(1) and (3) of PIPEDA, including requirements to assess real risk of significant harm.
Records, at minimum, will include:

- date or estimated date of the breach;
- general description of the circumstances of the breach;
- nature of information involved in the breach;
- whether or not the breach was reported to the Privacy Commissioner of Canada/individuals were notified; and
- sufficient details for the OPC to assess whether the firm has correctly applied the real risk of significant harm standard and otherwise met its obligations to report and notify in respect of breaches that pose a real risk of significant harm

Openness

FCSL will endeavour to make its privacy policies and procedures known to the individual via this Privacy Policy as well as the firm's *Privacy Statement*, contained herein as Schedule 3.

Individual access

Clients have a right to access their personal information, subject to limited exceptions.
Exceptions to access that might apply include:

- information that is prohibitively costly to provide;
- information that contains references to other individuals;
- information that cannot be disclosed for legal, security, or commercial proprietary reasons, and
- information that is subject to solicitor-client or litigation privilege.

A request to access personal information must be made in writing and provide sufficient detail to identify the personal information being sought. A request to access personal information should be forwarded to the Chief Privacy Officer.

Upon request, we will also tell clients how we use their personal information and to whom it has been disclosed if applicable.

We will make the requested information available within 30 business days or provide written notice of an extension where additional time is required to fulfill the request.

A minimal fee may be charged for providing access to personal information. Where a fee may apply, we will inform the client of the cost and request further direction from the client on whether or not we should proceed with the request.

If a request is refused in full or in part, we will notify the client in writing, providing the reasons for refusal and the recourse available to the client.

Complaints/recourse

If an individual has a concern about FCSL' personal information handling practices, a complaint, in writing, may be directed to the Chief Privacy Officer.

Upon verification of the individual's identity, the Chief Privacy Officer will act promptly to investigate the complaint and provide a written report of the investigation's findings to the individual. Where the Chief Privacy Officer makes a determination that the individual's complaint is well founded, the Chief Privacy Officer will take the necessary steps to correct the offending information handling practice and/or revise FCSL' privacy policies and procedures. Where the Chief Privacy Officer determines that the individual's complaint is not well founded, the individual will be notified in writing.

If the individual is dissatisfied with the finding and corresponding action taken by FCSL' Chief Privacy Officer, the individual may bring a complaint to the Office of the Privacy Commissioner.

Schedule 1: PIPEDA Breach Report Form

https://www.priv.gc.ca/en/report-a-concern/report-a-privacy-breach-at-your-organization/report-a-privacy-breach-at-your-business/

Schedule 2: Assessing Real Risk of Significant Harm[3]

As an accountable organization, you should develop a framework for assessing the real risk of significant harm in order to assess breaches consistently.

The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include:

- the sensitivity of the personal information involved in the breach; and
- the probability that the personal information has been, is being, or will be, misused.

As a part of your assessment, you should consider the following:

i. **Sensitivity:**
   - PIPEDA does not define sensitivity. However, the concept of sensitivity of personal information is discussed in Principle 4.3.4 of PIPEDA which states:

     > *Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.*

   - Following a breach, to determine sensitivity, it is therefore important to examine both what personal information has been breached and the circumstances.

[3] https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_6

- Certain information may on its face be clearly sensitive. Other information may not be.
- The circumstances of the breach may make the information more or less sensitive. The potential harms that could accrue to an individual are also an important factor.

ii. **Probability of Misuse:**

Some questions you may wish to consider are:

- What happened and how likely is it that someone would be harmed by the breach?
- Who actually accessed or could have accessed the personal information?
- How long has the personal information been exposed?
- Is there evidence of malicious intent (e.g., theft, hacking)?
- Were a number of pieces of personal information breached, thus raising the risk of misuse?
- Is the breached information in the hands of an individual/entity that represents a reputation risk to the individual(s) in and of itself? (e.g. an ex-spouse or a boss depending on specific circumstances)
- Was the information exposed to limited/known entities who have committed to destroy and not disclose the data?
- Was the information exposed to individuals/entities who have a low likelihood of sharing the information in a way that would cause harm? (e.g. in the case of an accidental disclosure to unintended recipients)
- Was the information exposed to individuals/entities who are unknown or to a large number of individuals, where certain individuals might use or share the information in a way that would cause harm?
- Is the information known to be exposed to entities/individuals who are likely to attempt to cause harm with it (e.g. information thieves)?
- Has harm materialized (demonstration of misuse)?
- Was the information lost, inappropriately accessed or stolen?
- Has the personal information been recovered?
- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?

Schedule 3: Privacy Statement

Privacy Policy & Information Gathering

A privacy policy is a declaration of what information is collected from website visitors and how that information is used. We have adopted 10 Privacy Principles (listed below) based on the federal legislation to ensure that clients' information is protected.

FCSL will disclose information to third parties such as custodians, banks, trustees and other service providers only to enable them to fulfill their service obligations to the firm and its clients. For example: opening accounts, managing accounts, record keeping, tax statement production, processing instructions and executing client transactions.

(1) What information do we collect?

We may collect, store and use the following kinds of personal data:

(a) information about your computer and about your visits to and use of this website (including your IP address, geographical location, browser type, referral source, length of visit and number of page views]);
(b) information relating to any transactions carried out between you and us on or in relation to this website;
(c) information that you provide to us for the purpose of registering with us;
(d) information that you provide to us for the purpose of subscribing to our website services, email notifications and/or newsletters;
(e) any other information that you choose to send to us.

(2) Cookies

A cookie consists of information sent by a web server to a web browser, and stored by the browser. The information is then sent back to the server each time the browser requests a page from the server. This enables the web server to identify and track the web browser.

We may use cookies on the website. We will use the session cookies to keep track of you whilst you navigate the website. We will use the persistent cookies to enable our website to recognize you when you visit. Session cookies will be deleted from your computer when you close your browser. Persistent cookies will remain stored on your computer until deleted, or until they reach a specified expiry date.

We use Google Analytics to analyse the use of this website. Google Analytics generates statistical and other information about website use by means of cookies, which are stored on users' computers. The information generated relating to our website is used to create reports about the use of the website. Google will store this information. Google's privacy policy is available at: http://www.google.com/privacypolicy.html. Most browsers allow you to reject all cookies, while some browsers allow you to reject just third party cookies. For example, in Internet Explorer you can refuse all cookies by clicking "Tools", "Internet Options", "Privacy", and selecting "Block all cookies" using the sliding selector. Blocking all cookies will, however, have a negative impact upon the usability of many websites, including this one.

(3) Using your personal data

Personal data submitted on this website will be used for the purposes specified in this privacy policy or in relevant parts of the website.

We may use your personal information to:

- administer the website;
- improve your browsing experience by personalizing the website;
- enable your use of the services available on the website;
- supply to you services via the website;
- send statements, emails and communication materials to you;
- send you general (non-marketing) communications;
- send you email notifications which you have specifically requested;
- send to you marketing communications relating to our business which we think may be of interest to you by post or, where you have specifically agreed to this, by email or similar technology (you can inform us at any time if you no longer require marketing communications); and
- deal with enquiries and complaints.

(4) Disclosures

We may disclose information about you to [any of our employees, officers, agents, suppliers or subcontractors] insofar as reasonably necessary for the purposes as set out in this privacy policy.

In addition, we may disclose information about you:

(a) to the extent that we are required to do so by law;
(b) in connection with any legal proceedings or prospective legal proceedings;
(c) in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk).

Except as provided in this privacy policy, we will not provide your information to third parties.

(5) Security of your personal data

We will take reasonable technical and organizational precautions to prevent the loss, misuse or alteration of your personal information.

We will store all the personal information you provide on our secure (password- and firewall-protected) third-party servers. All electronic transactions you make to or receive from us will be encrypted using 128-bit SSL technology.

Data transmission over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

You are responsible for keeping your password and user details confidential.

(6) Policy amendments

We may update this privacy policy from time-to-time by posting a new version on our website. You should check this page occasionally to ensure you are happy with any changes.

We may also notify you of changes to our privacy policy by email.

(7) Your rights

You may instruct us to provide you with any personal information we hold about you. You may instruct us not to process your personal data for our own marketing purposes by email at any time.

(8) Third party websites

The website contains links to other websites. We are not responsible for the privacy policies or practices of third party websites.

(9) Updating information
Please let us know if the personal information which we hold about you needs to be corrected or updated.

(10) Contact

If you have any questions about this privacy policy or our treatment of your personal data, please write to us by email to contact@fortcapital.ca or by post to:

Fort Capital Securities Limited
1010-510 Burrard Street
Vancouver, BC, Canada, V6A 3A8
Telephone: 1-604-681-2353