PRIVACY POLICY

Compliance Officer: Kam Ho (Kinson) Lai

DECEMBER 1, 2021

NOVELLA WEALTH CORPORATION
#270 – 10691 Shellbridge Way, Richmond BC V6X 2W8

Table of contents

SECTION 1 – APPOINTMENT OF A COMPLIANCE OFFICER

SECTION 2 – POLICIES AND PROCEDURES

1. PRIVACY AND OUR BUSINESS

1.1 General Provisions

1.2 Ten Privacy Principles

2. CONCERNS AND GENERAL INQUIRIES OR REQUESTS

2.1 Privacy Choices

2.2 Misuse of Personal Information

2.3 Privacy Breach Process

2.4 Mandatory Data Breach Reporting under PIPEDA

2.4.1 Notification to affected individual(s)

2.4.2 Notification to regulators

2.5 Future Preventions

2.6 Record Keeping

2.7 Responsibilities

3. OBTAINING VALID, INFORMED CLIENT CONSENT

3.1 New Uses/Access to Client Information

3.2 Supplier Contracts

3.3 Business Transactions Consent Exception

3.3.1 Buy/Sell Agreements

3.3.2 Agent of Record (AOR) Changes

4. COLLECTION OF PERSONAL INFORMATION

4.1 Recording client telephone calls

5. USE, DISCLOSURE AND RETENTION

5.1 Secure disposal

5.2 Record retention

6. SAFEGUARDS

6.1 Technological Safeguards

6.1.1 Encryption, antivirus, and firewalls

6.1.2 Screensavers, user ID, and passwords

6.1.3 Secure email

6.2 Physical Safeguards

6.2.1 Office design

6.2.2 Computers and consumer devices

6.2.3 Desks and files

6.3 Communicating confidential information with others

6.3.1 Voicemail

6.3.2 Caller authentication

6.3.3 Email

6.3.4 Faxes

6.4 Organizational safeguards

6.4.1 Authorization and limiting access on a “need-to-know” basis

6.4.2 Confidentiality agreements

7. ADOPTION OF POLICIES AND PROCEDURES

SECTION 3 – TRAINING PROGRAM

SECTION 4 – SELF-REVIEW

SECTION 5 – REVIEWS AND AMENDMENTS TO THE COMPLIANCE PROGRAM FOR PRIVACY

PRIVACY POLICY

SECTION 1 – APPOINTMENT OF A COMPLIANCE OFFICER

The Compliance Officer (CO) is responsible for:

- The implementation, monitoring, updating, and carrying out the compliance program which includes:
    - Policies and procedures
    - Training and awareness
    - Program self-review/assessment
- The privacy breach process, and client inquiries and complaints
- Reporting new risks, existing risks, monitoring and any legislative/regulatory changes that will impact the compliance program on a regular basis to senior decision makers within the practice

The CO should have the authority and resources necessary to discharge their responsibilities effectively. The CO should hold a senior position within the practice that enables them to have direct access to senior decision makers. The CO may delegate certain duties to other employees/staff; however, the CO retains responsibility for the implementation of the compliance program.

The below person has been appointed to the position of CO:

Name: Kam Ho (Kinson) Lai

Position: President & Founder

Date: January 1, 2022

Address: 270-10691 Shellbridge Way

Richmond, BC V6X 2W8

SECTION 2 – POLICIES AND PROCEDURES

1. PRIVACY AND OUR BUSINESS

Clients provide personal information that is essential to the practice's business. Protecting this information is important to maintaining client trust and confidence. The federal privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and Alberta, British Columbia and Quebec provincial privacy laws govern the collection, use and disclosure of personal information, as well as business information unless it's classified as "business contact information". This includes business title, business telephone number and email, and information that's used in relation to the individual's employment, business, or profession.

The practice is responsible for personal information under its control and for taking appropriate steps to safeguard the personal and confidential information in its possession. In some situations, this will mean adopting new business practices to safeguard personal information.

The practice makes information regarding its policies and procedures available to the public and abides by the privacy guidelines of the companies it represents (Company).

1.1 General Provisions

Through its policy on the protection of personal information, the Company reaffirms its commitment to protect such information and to comply with the laws and regulations that govern their management.

Although we have implemented protection measures that we deem appropriate, we cannot claim to be absolutely protected from a breach regarding the protection of personal information.

In this context, we believe it necessary to adopt measures that are to be applied in the case of a violation (breach) regarding the protection of personal information.

1.2 Ten Privacy Principles

i. ***Accountability***

The Company is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the company's compliance with the following principles.

ii. ***Identifying Purposes***

The purposes for which personal information is collected shall be identified by the company at or before the time the information is collected.

iii. ***Consent***

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

iv. ***Limiting Collection***

The collection of personal information shall be limited to that which is necessary for the purposes identified by the company. The information shall be collected by fair and lawful means.

v. ***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 for as long as necessary for the fulfillment of those purposes.

vi. ***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.

vii. ***Safeguards***

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

viii. ***Openness***

The company shall make readily available to individual with specific information about its policies and practices relating to the management of personal information.

ix. ***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.

x. ***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.

2. CONCERNS AND GENERAL INQUIRIES OR REQUESTS

Procedure

Any concerns, general inquiries or requests related to privacy and the practice are forwarded to the practice's compliance officer. The compliance officer will review and acknowledge requests within 24 hours or if away, redirect appropriately for handling. The client will be updated on the compliance officer's progress regarding the concern with complete documentation of the concern and related activities kept in the client file.

The practice's compliance officer forwards any privacy concerns, general inquiries or requests related to the company's products and services to that company's chief compliance officer.

2.1 Privacy Choices

Under privacy laws, clients have the right to request access to their personal information held in client files maintained by either the practice or the company and to challenge its accuracy, if need be.

Procedure

i. Clients may request access to their information with a written requisition. We must respond to this request as quickly as possible, but no later than thirty (30) days after the receipt of the request.

ii. Clients may withdraw their consent at any time by contacting our Compliance 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.

iii. Clients may file complaints about our privacy procedures as well as a breach in our privacy policy.

a) Complaints should be received in writing and forwarded to the Compliance Officer.

b) The Compliance Officer will contact the client and obtain all details.

c) The Compliance Officer will then review the circumstances of the complaint and determine if there is reason to alter the existing privacy policy.

d) 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:

i. If it would reveal personal information about another individual unless there is consent or a life-threatening situation.

ii. 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 during a formal dispute resolution process.

2.2 Misuse of personal information:

Procedure

Any misuse of personal information or potential breach of security safeguards relating to the company's products and services are reported immediately to the company's chief compliance officer by the practice's compliance officer.

2.3 Privacy breach process

A privacy breach occurs when there is the loss of unauthorized access to or unauthorized disclosure of personal information resulting from a breach of security safeguards. A privacy breach also includes information that is retained in ways which are not in accordance with applicable privacy legislation, such as retaining information that is no longer needed for the identified purpose.

Examples of privacy breaches:

- Copies of client personal information statements are stolen from a vehicle.
- Advisor laptop is lost/stolen, and it contains client personal information.
- Client information on an advisor's computer hard drive is compromised/hacked.
- Client information not emailed to the intended recipient either internal or external.
- Client information going to the wrong address (someone else opening the mail).
- Release of personal information without proper authorization or use of personal information without proper consent.
- Keeping inactive customer information for longer than the retention period.

Policy

Suspected breaches, complaints or any other concern relating to a privacy issue, whether they involve an individual or a supplier, are reported immediately to the practice's compliance officer and/or the company. The practice's compliance officer will assess, contain, remediate, and help enhance controls to prevent the breach from reoccurring in the future.

Procedure/Containment

Lost, stolen or hacked electronic devices:

- Engage the practice's IT support.
- Scan computers for malware before accessing systems again.
- Immediately contact the company's service desk to have systems passwords changed.
- File a report with the police.
- Change other system passwords (e.g., online banking).

Lost or stolen paper documents (e.g., policy contracts, applications, client files):

- Notify the practice's compliance officer, the company's chief compliance officer, and the practice's regional director/business services manager if applicable.
- Report stolen materials to the police.

Misdirected emails:

- Recall email immediately.
  - If not successful, contact unintended recipient to obtain written confirmation that email has been deleted.
- Notify the practice's compliance officer, the insurance company's compliance officer, and the practice's management if applicable.

Incident / breach determination and assessment

1. Answer the following questions:
    a. Was personal information involved? Is there proof / likelihood or is it indeterminable that personal information was involved?
    b. Has an unauthorized disclosure or transfer of an individual's personal information occurred? Unauthorized disclosure, whether it is intentional, inadvertent or because of criminal activity, constitutes a privacy breach.
    c. Was personal information collected or used without authorization?
2. If the answer to questions above is "yes", a privacy breach has occurred.
3. Complete risk assessment questions:
    a. Assess the situation

i. Type/Sensitivity and amount of personal information data elements disclosed (e.g., bank account number, SIN, health information/claims data)
ii. To whom was the information disclosed/who obtained it
iii. Number of individuals affected
iv. Was the information fully recovered
v. Time Lag from incident discovery to remediate
vi. Written Confirmation that there was no disclosure or misuse of duplication
vii. Potential harm to the individual (e.g., identity theft, fraud or other harm including pain and suffering or loss of reputation) or no known harm of affected individuals
viii. Potential Street Value of Data
ix. Was the personal information compromised in a malicious manner i.e., was this targeted or a technical/human error?
x. The incident is because of a systematic problem, or a similar incident previously occurred
xi. Whether or not the individuals affected have been notified
xii. The impacted individual is vulnerable (e.g., a minor)
xiii. Expectation that the Privacy Commissioner may receive complaints or inquiries (e.g., public awareness)

b. Considering the sensitivity of the information involved and the probability that the information will be misused determine if the breach poses a "real risk of significant harm" to any individual whose information was involved in the breach ("affected individuals").
    i. Based on the risk assessment conducted in section 3a, is there a real risk of significant harm?

2.4 Mandatory data breach reporting under PIPEDA

- When the practice considers that a breach is posing a real risk of significant harm, it must notify affected individuals and report to the Office of the Privacy Commissioner of Canada (the Commissioner) or provincial regulators where required as soon as feasible, even if only one individual is impacted.

- The practice must notify any other organization/company that may be able to mitigate harm to affected individuals.

2.4.1 Notification to Affected Individual(s)

A notification provided by the practice to an affected individual with respect to a breach of security safeguards must contain:

a. a description of the circumstances of the breach.
b. the day on which, or period during which, the breach occurred or, if neither is known, the approximate period.
c. a description of the personal information that is the subject of the breach to the extent that the information is known.
d. a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach.
e. a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
f. contact information that the affected individual can use to obtain further information about the breach.

Form and content of the notice:

The content and form of the notice will vary depending on the breach and the notification method chosen, and should contain the following elements, if applicable:

- a brief description of the breach and the moment when it happened.
- a description of the personal information in question.
- a brief description of the measures taken to control or reduce prejudice.
- the measures taken by The Company to help the persons and the measures that they can take for themselves to avoid or reduce the risk of prejudice and to further protect themselves (For example: arrangements for credit watch; information on how to change one's social insurance number, health insurance number, driver's license; fraud prevention tools).

- contact information for a The Company staff who can answer questions or provide more information.

Other persons to advise

To evaluate the need to report a privacy violation, the following factors must be considered:

- any applicable law requiring the notification.
- the type of personal information in question, including the information that was communicated, it if can be used to commit a theft and/or a misappropriation of identity and if there is a reasonable risk of prejudice arising from the leak of this information, including non-financial losses.
- the number of persons affected or concerned by the breach.
- whether the affected or interested persons have been advised or not.
- if we must reasonably deduce that the privacy commissioner's office will receive complaints or requests for information concerning the violation.

It is also important to consider advising the following persons, if necessary:

- the police, in case of theft or criminal activity.
- insurance companies or other pursuant to contractual obligations.
- professional corporations or other regulatory agencies if standards so require.
- financial institutions, including insurance companies to the extent that their help is required to communicate with the affected or interested persons.
- any other person.

2.4.2 Notification to Regulators

- Report to the Commissioner using the PIPEDA breach report form
- British Columbia – legislation recommends notification to the Privacy Commissioner if there is a real risk of significant harm. See BC's privacy breach checklist for the reporting.
- Alberta – Office of the information and privacy commissioner of Alberta (OIPC)

- Quebec – notify the Autorité des marchés financiers (the "AMF") of any breach of personal information that will jeopardize the interests or rights of consumers and the institution's reputation.

2.5 Future Prevention

Once immediate measures have been taken to lessen the risk associated with the breach, the person responsible for the protection of personal information and/or the team in charge of the investigation must investigate the causes of the incident and establish a prevention plan, if necessary, taking the following elements into account:

- a verification of physical and technical security.
- a review of policies and procedures and their update.
- a review of training practices for staff and agents.
- a review of provider practices.

Finally, a self-verification of the plan must be carried out at the end of the process to determine if it meets expectations or not.

2.6 Record keeping

Keep records of all privacy breaches for 24 months and provide it to the Commissioner upon request.

2.7 Responsibilities

2.7.1 Management

The company management adopt the present procedure and name the person responsible for the protection of personal information as responsible for the application and implementation of the procedure.

2.7.2 Compliance Officer

Person responsible for the protection of personal information coordinates all investigations regarding a breach and sets up an investigative team. Keeps management aware of activities on a regular basis and seeks their approval when necessary.

Ensures that the present procedure is delivered and communicated to all staffs.

2.7.3 Management staff members

Management staff members respect the present procedure and ensure it is communicated to all staffs.

They take all necessary means to limit, without delay, any violation they are made aware of and immediately report it to the person responsible for the protection of personal information. At their request, the management staff is part of the team in charge of the investigation.

2.7.4 Staffs

Staffs respect and comply with the present procedure. They advise their superior immediately or, if they cannot, the person responsible for the protection of personal information, of any breach. They take necessary measures to limit it immediately. At the request of the person responsible for the protection of personal information, they are part of the team in charge of the investigation.

2.7.5 Team in charge of the investigation

The persons appointed by the person responsible for the protection of personal information to be part of the investigation team must participate in each of the steps described in detail in the present policy.

3. OBTAINING VALID, INFORMED CLIENT CONSENT

Consent is considered valid only if it is reasonable to expect that individuals understand the nature, purpose and consequences of the collection, use or disclosure of their personal information to which they are consenting.

Policy

At the beginning of a relationship with a client, the practice will obtain client consent for the collection, use and disclosure of their personal information and notify them of potential out-of-country storage.

When collecting information from clients and prospects, explain the purposes behind the collection of this information and provide information about the practice's privacy policies.

Only disclose personal information about clients to another person or company if verbal or written consent from the client has been obtained or if otherwise allowed or required to do so by law. If information is sensitive, written consent should be obtained.

The practice will recommend other professionals or advisors to clients if the client asks or if the client may benefit from such services. The practice never provides any client names or other information to third parties to market their services unless the client has first been informed and consented.

Procedure

Review the *Privacy commitment and your client file* form with the client, keeping the signed copy in the client file for future reference. Cover the:

- Purposes for the collection,
- Who has access - staff access, other advisors?
    - This covers a short-term or temporary absence from the practice. At times when the practice is unable to provide service to clients for an extended period and help from another advisor or new administrative support person is required
- Use of external suppliers (e.g., information processors which includes client relationship managers and cloud-based storage services)
    - Likelihood that information will be stored outside Canada and is subject to regulation, including public authority access laws in that country
- Sharing spousal information consent; joint files and access to that information
- Individual's ability to always withdraw consent

3.1 New uses/access to client information

Policy

The practice will obtain client consent if the purpose for the collection, access, use and disclosure of the client's personal information changes.

Procedure

Review the new purpose, access, use and disclosure with the client and keep a copy of the new consent in the client file.

If a client objects to a transfer or new access, the client has the right to:

- Request that his/her information not be disclosed
- Request a new advisor
- Receive the names of other advisors to contact or be provided with the name and number of the regional director where they can request another advisor

3.2 Supplier contracts

Policy

The practice requires client consent prior to transferring client information to a supplier and retains control of the information when transferring personal information to a supplier for processing.

Information transfers to suppliers for processing, including cloud computing, is done for a variety of reasons including information storage, processing, or manipulating client personal information.

Procedure

Before entering into, substantially amending or renewing a contractual arrangement with a supplier, the practice assesses whether or not the supplier has appropriate safeguards in place to protect client information.

The practice will check with its legal counsel before agreeing to the terms of the supplier and keep a printed copy of the agreement for the practice's records.

Assessment considerations:

Business experience: Evaluate the supplier's experience and technical competence to implement and support the planned activities.

- How long has the supplier been in business? A new supplier may not have a sufficient track record to allow the practice to judge its processes and procedures as they relate to the safeguarding of information.

Reputation: Assess how long the supplier has been in the market and their market share.

- Obtain references to assess reputation? References from current users can help gauge the supplier's reputation.

Information security:

- What is their experience in handling sensitive personal and financial information?
- Does the supplier have a documented privacy policy in accordance with privacy legislation?
- Do they have a documented and current physical security policy or information security policy?
- Confirm with the supplier that the data they store, as well as data in transmission, is encrypted.

Incident reporting: Review the supplier's incident reporting and management programs to ensure they have clearly documented processes for identifying, reporting, investigating and escalating incidents. Ensure the supplier's escalation and notification process meet the practice's expectations.

- Does the supplier agree to notify the practice within 48 hours or less if there is a data security breach that may involve client information?
- If a security breach is suspected, is there support from the supplier for an investigation? Are access logs maintained and provided on demand?

Contingency planning:

- Does the supplier have backup and recovery processes? Will the practice be able to access files if the supplier shuts down? What will the practice do if the supplier loses the client files? Does the practice have a backup?

Out-of-country notification:

- Does the supplier hold data outside of Canada or do individuals outside Canada have access to the data? Information held in other countries may not have the same safeguards as in Canada and may not follow privacy requirements. Attempt to use a supplier that stores information in Canada, or the practice will notify clients that their information will be stored outside of Canada.

Review the supplier's licensing agreement carefully: It is a contract, and by clicking "I agree" or by downloading any software, you may inadvertently expose information stored at the site to undue risk if the proper safeguards of information are not adhered to.

The service provider must not involve any other third parties and/or data sharing, data pooling or access rights to clients' sensitive information, unless this is specifically mentioned in the service supplier's agreement.

Ensure that the supplier:

- Limits use of the information to the purpose specified to fulfill the contract
- Limits access to data to individuals who need access to fulfill the contract
- Limits disclosure of the information to what is authorized by the practice or required by law
- Refers any access requests or complaints relating to the information transferred to the practice
- Returns or securely disposes of the transferred information upon completion of the contract
- Reports on the adequacy of its personal information security/control measures and allows your organization to audit the third party's compliance with the contract as necessary

Understand:

- How to terminate the agreement with the supplier and ensure data is purged or returned. A supplier that does not remove or return information may present a risk to a client's information and therefore to the practice.
- The limitations of the service supplier's liability

3.3 Business transactions consent exception

Business transactions include, for example, the sale of a business, a merger or amalgamation of two or more organizations or any other prescribed arrangement between two or more organizations to conduct a business activity.

Policy

The practice transfers personal information where necessary to determine whether to proceed with a transaction, or to complete a transaction. The information must be used or disclosed solely for purposes related to the transaction, safeguarded appropriately, returned, or destroyed when no longer needed for that purpose and the affected clients must be notified that their personal information has been transferred to another organization.

Procedure

When receiving personal information, the practice will enter into an agreement to use or disclose the information for the sole purpose of the transaction, to protect it and to return or destroy the information if the transaction does not proceed. If the transaction proceeds, the practice will notify affected clients that their personal information has been transferred to another organization.

3.3.1 Buy/sell agreements

Policy

The practice will use, disclose, and protect client information during the valuation process and when seeking a buyer for the book of business or looking to purchase a book of business.

Procedure

The practice limits identifying client information on documents shared with third parties and contacts legal counsel to draft a suitable confidentiality agreement that should be signed by third parties involved in the process of valuing the book for potential sale or purchase.

3.3.2 Agent of Record (AOR) changes

Policy

For client initiated AORs, the practice assumes consent to transfer access to the client's information and files, if applicable to the new advisor.

4. COLLECTION OF PERSONAL INFORMATION

Policy

When collecting personal information:

- Limit the amount and type of the information gathered to only what is necessary, for the identified purposes.
- Take reasonable efforts to ensure client and prospect information held in client files is accurate and is updated or corrected as needed.
- Take appropriate measures to ensure that information collected is used for the purposes identified and that it's not used for another purpose or disclosed to a third party without the client's or prospect's consent, except as may otherwise be allowed by law.

4.1 Recording client telephone calls

Policy

Any recording of client calls involves the collection of personal information and therefore requires the caller's consent.

Procedure

- Recording may only take place with the individual's consent. If the caller objects to the recording, provide the caller with meaningful alternatives and if the caller continues to refuse, cease recording the conversation immediately and destroy any recordings that may have been created.
- Only record calls for specified purposes.
- The individual must be informed that the conversation is being recorded at the beginning of the call and will ensure the individual is advised as to the purposes for which the information will be used.
- Ensure compliance with applicable privacy legislation.
- If a copy of the client file is requested, provide the recording or transcription of the recording of calls with the client.

5. USE, DISCLOSURE AND RETENTION

Policy

Personal information is not, without consent, used or disclosed to a third party for any purpose other than that for which it was collected, unless such use or disclosure is required or allowed by law.

The practice retains personal information only if necessary to fulfill the identified purpose or as otherwise required or allowed by law and is solely responsible for the safe keeping of this material and for maintaining its confidentiality.

Personal information that is no longer required to fulfill the purpose(s) identified when collected is securely destroyed or erased.

5.1 Secure disposal

Policy

- When paper materials containing any client or prospect personal information are to be destroyed, this is done by shredding, not recycling.
- Information is deleted from all business technology before the technology is destroyed. Storage devices must be destroyed when being disposed of to ensure the information is not retrievable.
- When disposing of or destroying personal information, take appropriate measures to prevent unauthorized parties from gaining access.
- When disposing of equipment or devices used for storing personal information (such as filing cabinets, computers, diskettes, and audio tapes), take appropriate measures to remove or delete any stored information or otherwise to prevent access by unauthorized parties.

5.2 Record retention

Policy

The practice's clients, files and records are maintained for at least any minimum period required by law.

6. SAFEGUARDS

Policy

Appropriate safeguards must be taken in the storage and disposal of client information. Anyone working for or contracted with the practice is required to follow the procedures outlined in this section.

Procedure

The practice uses technology, physical and organizational safeguards to protect client personal information from theft or misuse, as well as unauthorized access, disclosure, copying, use or modification.

6.1 Technological safeguards

Technology examples requiring safeguards can include:

- Computers – desktops, laptops, servers, and personal digital assistants (tablets/smartphones)
- Hardware and software
- Mobile devices
- Portable media –USB / thumb drives, CDs and DVDs
- Printers, scanners, fax machines and photocopiers with secure print options
- Email and internet services (e.g., cloud computing)

6.1.2 Encryption, antivirus, and firewalls

Policy

- Encryption and antivirus software and firewalls are installed and kept up to date on all business technology as means to ensure client data remains secure. This includes encryption of sensitive data while stored and in transit including transmission to backup servers.
- Business technology safeguards are reviewed on an annual basis and upgraded as necessary.
- When technology is unattended or is being transported, all devices are shut down (powered off). Logging off, locking, or leaving the device in standby or sleep mode could render additional security measures ineffective.

Security program details

Safeguards	Product	Last updated
Encryption		
Antivirus/Malware protection		
Firewall		

6.1.3 Screen savers, user ID and passwords

Encryption does not eliminate the need for strong passwords.

- Protect user ID and passwords and never share either with anyone.
- Pick strong passwords (use capitals, lowercase, numbers, and symbols with a minimum length of eight characters).

- Avoid using proper names and words found in dictionaries (e.g., insurance, password) and personal information, like family and pet names, birthdays, government ID numbers or words associated with hobbies and interests.

- Use password-protected screensavers to prevent unauthorized access to unattended computers.
- Lock computers by clicking on “lock computer” when away from your computer temporarily.

6.1.4 Secure email

Password protection

When dealing with sensitive information, emails containing personal information need to be secured by a file/document password, or where possible, be encrypted. File passwords should be provided by telephone.

Encryption options when sending email and attachments securely:

1. WinZip
2. Microsoft Office 2007 (Word, Excel, and PowerPoint)
3. Microsoft Office Outlook 2007, with the use of digital certificates
4. Office 2016/0365

6.2 Physical safeguards

Consideration is given to the following safeguards:

6.2.1 Office design

- Desks/workspaces are arranged out of the traffic flow within the office.
- Fax machines, photocopiers, printers, etc. are in areas where access is reasonably limited.
- Associates/staff dealing with sensitive client information are located, where possible, in an area where conversations will not be easily overheard.
- Personal client information files are located out of the traffic flow within the area.
- Locked file cabinets are used for files containing personal information.

6.2.2 Computers and consumer devices

Always take steps to protect against the theft of laptop computers and mobile devices by using an anti-theft security device (e.g., locking cable), whether at the office, at home, in a meeting room or hotel room, etc.

- Lock your device away in a secure place when not using it.
- To prevent theft, avoid leaving laptops in vehicles. If you must, keep your laptop in your trunk or another out-of-sight area.
- Shut down and power off your laptop – this will ensure that all applications have been properly closed.
- Log out of any websites or programs when you are finished using them. And remember, don't "save" your information so that you can automatically log in the next time – if your mobile device is lost or stolen, someone may be able to access your accounts or files.
- Computers and consumer devices (and if applicable associate/staff computers) are stored securely to prevent access during all absences (evenings, weekends, illnesses, and vacations).

Securing laptops

In the office during the day – Laptops are locked using a locking cable and securely anchored to an immovable piece of furniture or a secure docking station. The lock key is stored in a safe place away from the laptop.

When leaving work at the end of the business day – Laptops are stored in a locked cabinet or drawer, and the lock key is stored in a safe place away from the laptop.

Laptop security rules described above still apply when office doors are locked.

On the road:

- Be cautious of public Wi-Fi hotspots as someone may be eavesdropping on them. Avoid online banking, shopping, or accessing corporate resources from such connections. It's best to save sensitive transactions for when you're on a network that you trust.
- Also be wary of using your mobile device outside your home country. Eavesdropping and traffic analysis maybe more prevalent on a foreign network.
- While working, position laptops so only the user can see the personal information on the screen.

- Record laptop serial and model numbers and keep them in a separate location.
- Carry laptops in a discreet bag. Use a padded bag, such as a backpack, instead of the normal laptop tote, to transport a laptop securely and safely.
- Keep laptops out of sight by storing in car's locked compartment during travel to prevent theft.
- Never place laptops in a taxi or limousine trunk since most hired drivers do not lock their trunks.
- Never check laptops with hotels or airlines.
- After placing laptop on an airport's x-ray conveyer belt, watch the bag and don't let anyone cut ahead of you in line.
- At home or in a hotel room, secure laptops as you would at work. Have the locking cable on hand, lock the laptop down and store it out of sight.
- Card-access hotel rooms produce an accurate audit trail of who has visited the room and when. Metal keys can be lost and copied. If the hotel room uses metal keys, consider not leaving the laptop in the hotel room.

6.2.3 Desks and files

- Sensitive personal information or another client documentation should never be left unattended. When personal information needs to be accessible in paper format for active business purposes, all files and file contents should be placed so the contents are protected from the view of those who are unauthorized to see them.
- Ensure all sensitive personal information is secured in locked rooms, cabinets and/or desk drawers when not actively in use and that access is appropriately restricted.

Documents outside of business premises

Client information must be safeguarded whether in the office, car, or other location. Paper files containing personal information should be removed from the office only when necessary or required to appropriately service clients.

For tracking purposes, all files/documents are recorded before being removed from the premises for reference if lost or stolen. All associates/staff must be made aware of and comply with this requirement.

6.3 Communicating confidential information with others

- Never discuss clients in public places such as elevators, cafeterias, or restaurants.
- When sharing client or employee personal information on cellular phones, take precautions to avoid being overheard.
- When reading a client's personal information on public transit such as trains, planes or buses, position documents to prevent anyone else from reading them.

6.3.1 Voicemail

Messages left for clients should not contain personal information unless the client is informed in advance that the message may contain personal information. The client must also confirm that he/she wants this information to be provided on his/her voice message service.

6.3.2 Caller authentication

If a request is made by phone, it is necessary to authenticate that person before providing them with any personal information.

To authenticate the caller, the person must successfully answer three of the following questions. Always ask the questions in this order.

- Full name of owner(s)
- For person calling on behalf of the estate, ask for full name of the deceased owner
- For owner - in-trust for, ensure the caller's name matches the trustee's name on the system
- For power of attorney, caller must provide name of power of attorney that matches name on file in addition to the name of the policyowner
- Policy number
- Apartment number, street number, street name and city
- Date of birth of the life insured/annuitant
- Full name of life insured/annuitant

If the validation is not successful inform, the caller that the practice is responsible for protecting the privacy and confidentiality of personal client information and therefore cannot disclose any details without first validating that the caller is the person who should be receiving this information. Ask them to submit their request in writing.

6.3.3 Email

Messages should not contain personal information unless the client is informed of this in advance and has confirmed that he/she wants this information to be provided by email.

The following disclaimer is added to all email containing client personal information:

" This email may contain confidential information and is intended only for the named recipient and may be privileged. Distribution or copying of this email by anyone other than the named recipient is prohibited. If you are not the named recipient, please notify us immediately and permanently destroy this email and all copies of it. Internet email is not private, secure, or reliable. No member of the Novella Wealth is liable for any errors or omissions in the content or transmission of this email. Any opinions contained in this email are solely those of the author and, unless clearly indicated otherwise in writing, are not endorsed by any member of the Novella Wealth."

Email authentication

Sensitive information should not be communicated by email unless it's at the client's request. If a request is made by email, it's necessary to authenticate that person before providing personal information through email.

- Call the client and confirm they requested the information.
- Ensure the email is being sent to the correct recipient as names on address listings may be similar.
- Authenticate the client and obtain and document consent to communicate via email.
- Encrypt/password protect files when disclosure of identifiable client information is requested via email.

6.3.4 Faxes

Faxes should not contain personal information unless the client is informed in advance that the fax may contain personal information and has confirmed that he/she wants this information to be provided by fax.

The following disclaimer is added to the cover sheet of all faxes containing client personal information:

"The contents of this fax, including any attachment(s), are confidential and may be privileged. If you are not the intended recipient (or are not receiving this fax on behalf of the intended recipient), please notify the sender immediately and delete or destroy this fax without reading it, and without making, forwarding, or retaining any copy or record of it or its contents. Thank you."

Confirm fax number before sending client personal information

- Pay careful attention to the different long-distance prefixes (i.e., 1-866, 1-888, 1-800) and take time to confirm the fax number before hitting send. Personal or confidential information can easily be misdirected by using the incorrect long-distance prefix.
- For commonly used fax numbers, consider preprogramming your fax machine to avoid errors.
- Reconfirm the fax number before you hit send.
- Contact recipient once the fax is sent to confirm receipt.

6.4 Organizational safeguards

6.4.1 Authorization and limiting access on a "need-to-know" basis

- Authorization is only granted for access to personal information on a "need-to-know basis" (i.e., information required to perform defined job functions). Access to files (physical, system and electronic) is reviewed when associates/staff are hired or moved to a different job function.
- When an associate/staff member's employment is in the process of being terminated, access to client information, including electronic information from computers and all other material from work areas is suspended.

6.4.2 Confidentiality agreements

Employees are made aware of the importance of maintaining security and privacy of personal information. Where personal information is sensitive or where the potential consequences of improper disclosures are significant, the practice:

- Uses confidentiality agreements with employees
- Takes appropriate precautions to safeguard client information from third parties who may have access to the premises i.e., security, cleaning services and suppliers.
- Obtains, if appropriate, a non-disclosure agreement from the individual or corporation servicing the device if confidential information cannot be removed from a device before releasing it for repairs.

7. ADOPTION OF POLICIES AND PROCEDURES

Policies and procedures adopted on February 1, 2020.

SECTION 3 – TRAINING PROGRAM

All advisors and staff, permanent and temporary, are trained as outlined in this training program.

- Training is mandatory prior to the individual being given access to personal information.
- Training is an ongoing process with refresher training conducted annually or more frequently if needed based on changes to legislation, technology, service providers as well as new use/access to personal information, etc.
- The compliance officer facilitates and tracks completion of all training. Training is completed through circulation and review of the policies and procedures section of this compliance program which are reviewed as part of the program self-review to ensure materials are accurate and up to date.
- Completion of training is tracked and signed by each advisor and staff acknowledging completion. Records of completed training are retained in this section of the compliance program.
- Optional/additional training may include modules provided by insurers, circulation of insurer privacy communications and updates, news articles, industry communications and training modules etc.
- Staff not able to attend refresher training on the originally scheduled date(s) will need to have alternate arrangements made to meet this requirement.

Training completion tracking

Name	Type of training and content (initial training, ongoing, review of policies procedures and background information, module provided by insurer, etc.)	Date	Employee signature
Example - Cam Smith	*Initial training, review of policies procedures and background information*	*12/04/2020*	

SECTION 4 – SELF-REVIEW

Date completed: _____

Review completed by: _____

Signature of principal/advisor: _____

Accountability	Yes	No	Comments
Has the practice designated a person to oversee compliance with privacy legislation and is the name of the designated person available to a client on request?			
Has the practice implemented procedures to protect personal information?			
Has the practice communicated and trained staff about policies and practices?			
Does the practice understand that personal information should not be collected unless it's needed to fulfill the purpose identified?			
Does the practice understand that when providing third parties (e.g., computer consultants, cleaning staff, accountants, etc.) access to personal information, it must have contractual or other means to provide a comparable level of protection?			
Is the practice aware of and follow the company's privacy guidelines and strong business practices?			
Is the practice aware of and following the privacy guidelines and strong business practices of other insurance companies it represents?			
Does the practice understand insurer processes regarding privacy complaints and inquiries?			
Consent	**Yes**	**No**	**Comments**
Does the practice understand that it's responsible for obtaining consent for the collection, use and disclosure of personal information?			
Does the practice have a process in place to obtain consent from clients for the collection, use and disclosure of their personal information?			
Does the practice make a reasonable effort to tell the client how his/her information will be used or disclosed?			

Consent	Yes	No	Comments
Has the client or an authorized representative e.g., legal guardian, general power of attorney consented to the collection of information?			
Does the practice have a process in place to manage opt-out and withdrawal of consent (e.g., can track and respect the wishes of clients who have opted out)?			
Limiting collection	**Yes**	**No**	**Comments**
The practice only collects information that is necessary to fulfill the purpose(s) disclosed to the client.			
The information is collected by fair and lawful means.			
Limiting use, disclosure, and retention	**Yes**	**No**	**Comments**
Does the practice understand that if personal information is intended to be used for a purpose other than the one for which it was originally collected, this new purpose must be disclosed to the client and obtain his/her consent?			
Does the practice have guidelines and procedures for the retention of personal information?			
Has the practice taken steps to ensure that when disposing of or destroying personal information, unauthorized parties will not be able to access it?			
Accuracy	**Yes**	**No**	**Comments**
Does the practice have a process in place to ensure that the personal information collected and used is as accurate, complete, and up to date as is necessary for the purpose(s) for which it is to be used?			
Safeguards	**Yes**	**No**	**Comments**
Does the practice have security safeguards in place to protect against loss or theft, as well as unauthorized access, disclosure, copying, use or modification of personal information?			
Does the practice use an enhanced level of protection for sensitive information? Examples: • Physical measures (e.g., locking filing cabinets, restricted access to office, etc.) • Organization measures (e.g., limiting access on a "need-to-know" basis) • Technological measures (e.g., use of			

passwords and encryption)			
The practice has made advisors and staff aware of the importance of maintaining the confidentiality of personal information			
Openness	**Yes**	**No**	**Comments**
Clients can easily obtain information about the practice's privacy policies and practices.			
Individual access	**Yes**	**No**	**Comments**
The practice understands that clients have a right to request information about them held in files it maintains.			
The practice has a process in place if a client requests access to/her personal information.			
The practice understands that clients have a right to request information about them held in files maintained by the company.			
The practice knows the process if a client requests access to his/her personal information held at the company.			
Actions required:			

SECTION 5 – REVIEWS AND AMENDMENTS TO THE COMPLIANCE PROGRAM FOR PRIVACY

The present program was adopted on February 1, 2020.

The present program was revised and amended on [date]

Below is a summary of these amendments:

Document revision history

Date	What changed?	Reason for the change