Privacy & Data Breach

Policies & Procedures

This document was last reviewed and updated on: **07 January 2023**

Objectives

This policy outlines how Shelter Bay Financial collects, uses, shares and protects the personal information that we require to perform our business.

It includes our Enterprise Privacy Framework and establishes Shelter Bay policies, standards and practices for privacy management to protect Personal Information, meet our regulators' expectations and achieve our business objectives.

In establishing our privacy policies, standards and procedures, we consider "best practice" approaches for privacy management, in addition to meeting legal and regulatory requirements.

Key Principles

In handling Personal Information, we adhere to the following 10 principles:

Accountability – We are responsible for Personal Information under our control and establish this policy for managing privacy across all of Shelter Bay US operations. We have designated individuals who are responsible for monitoring compliance with these principles, our policies, practices and procedures and the expectations of our regulators.

Identifying purposes – We are transparent about our privacy practices and clearly identify the purposes for which we collect, use, retain and disclose Personal Information.

Consent – We obtain implicit or explicit consent from individuals regarding the collection, use and disclosure of their Personal Information. We may obtain consent in writing, verbally, electronically or through an authorized representative. Consent may also be implied.

Limiting Collection – We limit the collection of Personal Information to that which is necessary for the purposes we identify, and we collect it fairly and lawfully.

Use, disclosure, and retention – We do not use, disclose or retain Personal Information for purposes other than those for which we collect it, except with permission, or as permitted or required by law. We restrict the disclosure of Personal Information to those who have a need for, and the legal right to, the information. This may include our employees, licensed representatives, agents, agencies or service providers who need the information to perform their duties.

It may also include some of our business areas and subsidiaries who, from time to time, may offer or promote other financial products, benefits or services, or those of select third parties, that we believe may be of interest to our members and customers. We may also have joint marketing or distribution agreements with other financial institutions that may offer or promote products that we believe may be of interest to our members and customers.

In some instances, our subsidiaries, employees, service providers, representatives, reinsurers, and any of their service providers may be located in other jurisdictions. Personal Information may then be subject to the laws of those other jurisdictions.

We aim to keep Personal Information only as long as necessary and will destroy or delete it in a manner that is appropriate for the sensitivity of the information and the media in which it is stored or retained, and as required by law.

Accuracy – We make reasonable efforts to keep Personal Information accurate, complete, and up-to-date as is necessary for the purposes for which we use it.

Safeguarding information – We classify Personal Information and take reasonable measures to protect it by administrative, physical and technical security safeguards, as appropriate for the sensitivity of the information. We make every reasonable effort to prevent any loss, misuse, disclosure or modification of Personal Information, as well as any unauthorized access to Personal Information.

Openness – We make information about our privacy policies and practices readily available to individuals, subject to any exceptions permitted by law.

Individual Access – Upon written request, we inform individuals of the existence, use and disclosure of their Personal Information and give them access to it, subject to those exceptions permitted by law. Individuals may verify the accuracy and completeness of their information and have it amended as appropriate.

Inquiries and complaints – Shelter Bay Chief Privacy Officer for the enterprise is located at our corporate head office in Toronto, Canada. The AVP, North America Compliance and Privacy Officer, is designated with responsibility for privacy management for Shelter Bay North America business and will establish mechanisms for handling privacy questions, concerns or complaints.

Introduction

Shelter Bay Financial (Shelter Bay) maintains the privacy and security of individuals' personal information while collecting, using and disclosing personal information in compliance with applicable laws.

We support the rights of individuals or their authorized representatives to access, correct or delete information, subject to any restrictions in applicable laws. We will not collect, use or disclose personal information except as described to you in this privacy policy.

Information we collect

We generally obtain your personal information when you submit an application or other forms, and from your transactions and interactions with us.

This information may include:

- Personal data, such as your name, address, email address, telephone number, date of birth, social security number or citizenship.
- Financial data, such as your income and banking information.
- Health related data, such as health and medical information or information about your lifestyle and habits.
- Data about your interactions with us, such as when you visit our websites, applications, social media sites or when you call our service centers.

We collect personal information about you, including information that directly or indirectly identifies you, from the following sources:

- Directly from you: Such as information we receive from you on applications for products or services or other forms you complete, via telephone calls with you, or information you provide to us online. For example, when you apply for an insurance product with Shelter Bay, we may collect your name, mailing or email address, social security number and/or information about your health, assets or income.

- Indirectly from you: Such as from your use of our products and services, information about your transactions with us, our affiliates or others, or information we collect or observe when you use or interact with our websites or social media sites. For example, we may collect information such as online identifiers including location data, your Internet Protocol (IP) Address, or information about your web browser and pages accessed.

- From third parties and other sources: Such as, from your insurance agent or broker, or from consumer reporting agencies and other third parties to process or administer products or services requested by you; or information we receive from health care providers, clinics, or other insurance companies. We may also collect information from the Medical Information Bureau or other persons that have records about you or your health. Outside sources, from whom we obtain information, may retain information and disclose it to other persons as required or permitted by law.

Why do we collect your information?

The primary purpose we collect your personal information is so that we may offer and deliver the products and services that you request and that are suited to your needs.

Collecting your personal information helps us to:

- determine your eligibility for our products and services
- promote and offer you a full range of products and services that may meet your needs or interests
- communicate with you about your and our products and services
- respond to your inquiries or complaints
- identify and mitigate potential losses to you and/or Shelter Bay, for example to verify your identity, to detect, prevent, or investigate fraud or security breaches
- hold fraternal and community events and activities and operate our branch system
- conduct industry or market research
- support and optimize user experience on our Sites and improve our products and services
- fulfill our legal and regulatory obligations

How do we use and share your information?

We use and share personal information only for disclosed purposes related to the products and services we offer, with your consent or as required or permitted by law. We may also use your information in a way that does not directly identify you.

For example, we may combine information about the nature or frequency of visits to our Sites and use or share aggregated information for statistical research or analysis, to optimize user experience and diagnose technical problems on our Sites, or other business purposes. We may share your information with our affiliates and licensed agents and agencies to provide you with a full range of our products and services. We may share your information with non-affiliated third-parties who help us conduct our business or who perform services on our behalf.

They are contractually obligated to use, protect and secure your information in accordance with our policies and standards or as permitted or required by law. They only have access to the information necessary to perform these services on our behalf and are prohibited from using the information for any purposes except performing the contract.

Shelter Bay does not sell your Personal Information.

How do we protect your information?

We strive to protect your personal information from the risk of loss, unauthorized access, disclosure, modification, or misuse. We comply with applicable laws and regulations and have implemented reasonable physical, electronic and procedural safeguards to protect your information that are appropriate for its sensitivity.

For example, we encrypt your personal information and we use advanced firewall technology and layered security tools to protect our environment. We restrict access to your personal information to those employees who need to know the information to provide or administer our products or services. We regularly train employees to keep your information safe.

Purpose and Scope – Information Security and Cyber Security

Shelter Bay Financial is committed to helping individuals and families achieve their financial security goals through an innovative portfolio of competitive life insurance, annuity and asset management products.

To meet its business objectives, Shelter Bay Financial collects, creates, stores, and uses information that is proprietary or belongs to members, customers, employees, associates and / or business partners.

This Policy applies to Shelter Bay Financial and all of its subsidiaries. All employees, associates, vendors, contractors, consultants, outsourced service providers, business partners and any other person who has been granted access to Shelter Bay Financials' Information and / or its Information Assets are responsible for complying with this Policy's principles and objectives.

Given their differing lines of business and regulatory environments, subsidiaries may enact and implement their own Information Security and Cybersecurity policies, standards, processes, practices and controls as long as they meet the principles and objectives set out in this Policy. Key terms used in this Policy are

defined in Appendix 1.

Policy Statement

Shelter Bay Financial is responsible for protecting all information it collects, creates, stores, and uses from all threats, whether internal or external, deliberate or accidental and in compliance with all applicable laws, regulations and contractual obligations.

The security of information and information assets is ensured by implementing adequate information security measures, in alignment with Shelter Bay Financial's business strategy and risk appetite.

Cybersecurity is an integral part of information security, and this Policy seeks to mitigate cybersecurity risks across the organization.

This Policy establishes the following baseline objectives:

Confidentiality - ensuring that information and data processing capabilities are protected from unauthorized access, change, disclosure or use.

Integrity - ensuring that information is not subject to malicious or accidental alteration and that system processes function correctly and reliably.

Availability - ensuring that information, including stored information and processing capabilities, are available to authorized users when needed. Each subsidiary will, as appropriate, establish their own Information Security Policy aligned to the objectives outlined above, which adheres to the principles and disciplines outlined below and meets local operating, legal and regulatory requirements. Key Principles and Disciplines Principles

Secure by default – Security must be a consideration throughout the lifecycle of Information and systems. This is to minimize the impact of vulnerabilities discovered during the use of the systems.

Adopt a risk based approach – Information security risks are treated in a consistent and effective manner. Risk treatment typically should involve choosing one or more options including: mitigating, accepting, avoiding and transferring risk.

Prioritize based on criticality and business impact - Prioritize information security resources based on criticality and business impact of the integrity, availability and / or confidentiality of Information.

Monitor and improve information security - Monitor changing threat landscape and improve Information security techniques on an ongoing basis in response to that changing landscape.

Foster a security-positive culture – Raise security awareness among users to make information security a key part of 'business as usual'. Ensure users have the skills required to protect critical or classified Information and systems.

Provide timely and accurate information on security performance - provide information as necessary to demonstrate that information security expectations are being met and where not put forward plans for remediation.

Disciplines

Information Security is a critical aspect of Shelter Bay Financial's internal control framework and is incorporated into all aspects of our business practices and operations.

Shelter Bay Financial strives to ensure that appropriate measures are implemented in accordance with recognized industry standards to maintain the security of its Information, Information Assets and processing facilities. The following security disciplines must be observed as a minimum.

Cybersecurity

Cybersecurity risks are prudently managed in a manner that is consistent with this Policy and applicable regulatory requirements. Appropriate policies, standards and processes must be in place to protect business critical Information by identifying, preventing, detecting and responding to attacks.

Access Control

Access to Information is provided only in accordance with business needs. It must be restricted to only authorized individuals and access to Information is based on Need-to Know and Least Privilege principles. Access privileges are authorized by the appropriate Information Owner(s).

Training & Awareness

Appropriate training and education is provided to all Shelter Bay Financial employees and associates at least annually regarding relevant information security policies, standards and procedures, range of threats, appropriate safeguards and employee / associate responsibilities.

Risk Management

Implementation of information security controls and safeguards must be based on risk assessments. Risks must be assessed and controlled by considering the potential threats and likelihood of each threat to Information compared to Shelter Bay Financial's risk appetite.

Human Resources

Employees, associates, contractors and third-party staff must be appropriately qualified for the level on which they are permitted to access Information and understand their responsibilities in doing so. Access permission to Information must be removed once employment or association is terminated.

Incident Response

Employees and associates are to be appropriately trained and equipped to detect, report, and respond to adverse events, providing the foundation for effective Information Security and Incident Management. All employees and associates have an obligation to report actual or suspected breaches of information security.

Information Classification

Information Owners, or their delegates, must classify all Information Assets within their control to ensure that:

- Information is reviewed about its potential for loss to Shelter Bay Financial in the event of accidental or intentional disclosure.
- Information is reviewed with regard to the protection and security of the personal information of Shelter Bay Financial's clients, individual employees and associates.
- Responsibilities of Information Owners are articulated and accepted.

Physical and Environmental Security

Appropriate physical security measures must be defined, implemented, and managed in all locations to protect Shelter Bay Financial's Information and Information Assets.

Communications and Operations Management

Protection of information systems and processing facilities is ensured by implementation of appropriate security measures and operating procedures in service delivery, system planning and acceptance, network security management, communication mechanisms and information exchange.

Business Continuity Planning

Shelter Bay Financial must plan for continuity and contingencies covering business critical systems, processes and infrastructure. The continuity planning must be based on risk assessments focusing on operational risks and be tested on at least an annual basis to ensure adequacy. Business continuity process programs must address information security and cybersecurity requirements.

Compliance

All employees and associates must comply with this Policy, including all information security standards, procedures and regulations. Non-compliance with the Policy could result in disciplinary action, up to and including termination of employment, association or services.

Third Party Access

All external contractors, service providers or suppliers who maintain, access, store or otherwise handle Shelter Bay Financial information and information assets must be contractually required to implement reasonable safeguards to adhere to the objectives and principles of this Policy at a minimum.

Data Breach

A data breach is defined as any unauthorized access, use, disclosure, or destruction of personal information. Personal information includes, but is not limited to, names, addresses, phone numbers, email addresses, financial information, medical history, avocations and identification numbers.

Procedures for Responding to a Data Breach:

STEP 1: NOTIFY STAFF AND OTHER CUSTODIANS

- Notify appropriate staff of the breach, including the chief privacy officer or other staff member responsible for privacy.
- Depending on the nature or seriousness of the privacy breach, you may need to contact senior management, the patient relations representative, and technology and communications staff.
- If the breach involves an electronic system shared between multiple custodians, notify all affected custodians.

STEP 2: IDENTIFY THE SCOPE OF THE BREACH AND TAKE STEPS TO CONTAIN IT

- Identify the scope of the breach, including individuals or organizations who may have been involved with or are responsible for the breach, and the nature and quantity that is affected.
- Retrieve any copies of that have been disclosed.
- Ensure that no copies have been made or retained by anyone who was not authorized to receive the

information.
- Record the person's contact information in case follow-up is required.

Determine whether the breach would allow unauthorized access to any others, for instance if it is on a shared system. Take whatever steps are appropriate, such as changing passwords and identification numbers and/or temporarily shutting down your computer system.

- In a case of unauthorized access by an agent, consider suspending their access rights

STEP 3: NOTIFY THE INDIVIDUALS AFFECTED BY THE BREACH

- Shelter Bay requires custodians to notify individuals affected by a breach at the first reasonable opportunity. Notification can be by telephone or in writing.
- There are many factors to consider when deciding on the best form of notification. If unsure, contact Shelter Bay Management to discuss the most appropriate form of notification.
- There may also be exceptional circumstances where direct notification is not possible or may be detrimental to the individual. If this is the case, contact Shelter Bay Management to discuss these circumstances.
- When notifying individuals affected by a privacy breach, you should provide the following information:
    - Where appropriate, the name of the agent responsible for the unauthorized access
    - the date of the breach
    - A description of the nature and scope of the breach o a description of the information that was subject to the breach
    - The measures implemented to contain the breach, and
    - The name and contact information of the person in your organization who can address inquiries •
    - Notice to affected individuals must include a statement letting them know they are entitled to make a complaint to Shelter Bay Management.

STEP 4: INVESTIGATE AND REMEDIATE

Conduct an internal investigation to:

- ensure the immediate requirements of containment and notification have been met
- review the circumstances surrounding the breach, and
- review the adequacy of existing policies and procedures in protecting personal information

- Address the situation from a systemic basis; in some cases, program-wide procedures may warrant a review. For example, administrative or security controls on an electronic system may be insufficient and need to be updated or augmented
- If you have notified Shelter Bay Management of a breach, you will be asked to provide the details of your investigation and work with Shelter Bay Management to identify and commit to any necessary remedial action.
- Keep a log of all privacy breaches and identify a person responsible for maintaining the log. For each privacy breach, record:
    - the name of the employee or agent that caused the breach, where it is determined to be relevant, such as in the case of unauthorized access o the date of the breach
    - The nature, scope and cause of the breach
    - the number of individuals affected by the breach
    - a description of the personal information that was subject to the breach, and
    - a summary of the steps taken to respond to the breach.

- You may also be required to cooperate in any Shelter Bay Management investigation related to the breach.

You must keep track of and report privacy breach statistics to Shelter Bay Management.

STEP 5: Notify the Federal Privacy Commissioner & Insurance Carrier

- Notify the Federal Privacy Commissioner of the breach including only necessary and appropriate details as directed by the commissioner:

    - **Telephone**
      Monday to Friday from 9 am to 4 pm (ET)

      Toll-free: 1-800-282-1376
      Phone: 819-994-5444
      Fax: 819-994-5424
      TTY: 819-994-6591

      Individuals using the teletype writer service may leave a message and we will respond within three business days. You may also request an appointment for a live call via our online form or by leaving a message detailing your request.

    - **Mailing address**

      Office of the Privacy Commissioner of Canada
      30 Victoria Street
      Gatineau, Québec
      K1A 1H3

- Notify the insurance carrier that issued the policy.
    - Contact Customer Service to identify the appropriate carrier contact.
    - Once the appropriate contact is identified, provide a summary of particulars and actions taken to date.

HOW TO MINIMIZE THE RISK OF A PRIVACY BREACH

- Educate staff about the privacy rules governing the collection, use, disclosure, retention, transfer and disposal of personal information.
- Make sure policies and procedures are in place that comply with the privacy protection provisions and that staff are properly trained.
- Safeguard personal information when it is physically removed from the office or facility. Ensure that all laptops and personal devices are password protected and that data is encrypted.
- Ensure that no more personal information is collected, used or disclosed than is reasonably necessary to proactively lessen the impact of any privacy breaches.
- Ensure that you do not collect, use or disclose personal information if there is other information that will serve the intended purpose.
- Ensure that logging and auditing is in place on electronic systems containing health records. Make staff aware that the systems will be regularly audited.

Conduct a privacy impact assessment (PIA), where appropriate. The PIA helps determine whether new

technologies, information systems and proposed programs or policies meet basic privacy requirements.

Contact Information:

If you have any questions or concerns about this policy, or if you believe you may have been affected by a data breach, please contact the privacy officer at 1.888.498.5288

Inquiries and complaints

For complaints about how Shelter Bay Financial Corp handles, processes or manages your personal information, please contact [insert Organization contact]. Note we may require proof of your identity and full details of your request before we can process your complaint.

Please allow up to 90 days for Shelter Bay Financial Corp to respond to your complaint. It will not always be possible to resolve a complaint to everyone's satisfaction.

How to contact us

If you have a question or concern in relation to our handling of your personal information or this Policy, you can contact us for assistance as follows:

Email - tom@shelterbay.ca

Phone - 1.888.498.5288

Mailing Address:

Attention: Privacy Officer

Shelter Bay Financial Corp

33096 Whidden Avenue

Mission BC V2V2T2