PRIVACY MANAGEMENT POLICY

Objective

Individuals expect their Privacy to be respected and their Personal Information to be protected by the organisations with which they interact. The key objective of this Policy is to establish minimum requirements to ensure that Asteron Life Limited ("Asteron") manages all Personal Information in a manner that is compliant with the applicable Privacy laws and Asteron policies and standards.

Asteron will also maintain the following customer facing policies:

- Asteron Privacy Policy, which provides general information to customers about how Asteron collects, uses, discloses, manages and enables access to customer Personal Information.
- Consumer Data Right (CDR) Policy, which provides general information about how Asteron manages CDR Data and how a customer can access and correct the CDR Data, and how they may complain.

Asteron may incur penalties for breaches of Privacy laws, including fines and liability for compensation. Privacy breaches may also lead to significant reputational damage. This Policy also establishes minimum requirements for Asteron's processes for reporting a Notifiable Privacy Breach in New Zealand.

Application

This Policy applies to all Employees and Officers when handling Personal Information held by Asteron, including CDR Data that is Personal Information and Credit Related Information.

Where Asteron relies on a Third Party to manage Personal Information on Asteron's behalf, Asteron will ensure that the Third Party complies with the requirements of this Policy and all statutory, regulatory and legal obligations as applicable.

Policy Statements

1. Asteron is open and transparent about its Privacy arrangements

Asteron is accountable for all Personal Information under its effective control and is open and transparent about how it manages Personal Information. In addition to the provision of Privacy Statements referred to below, Asteron's Privacy Policy, is available on the Asteron website, provides general information about how Asteron manages Personal Information of customers.

2. All Personal Information must be collected in a lawful manner

Personal Information about an Individual is to be collected only when it is relevant and necessary for Asteron's activities and only through lawful means. Sensitive Information is collected when it is reasonably necessary for one or more of Asteron's functions or activities and with the Individual's Consent, whether express or implied. Individuals must have the option of anonymity or the use of a pseudonym, unless identification is required by law, or their use is impracticable.

3. Appropriate Disclosures are to be provided to Individuals when collecting Personal Information

Appropriate disclosures must be made to the Individual in accordance with New Zealand privacy laws.

A single disclosure document covering Asteron's activities should be adopted, subject to the following exceptions:

— activities that require different Disclosures;

— A brand or marketing strategy that requires multiple Disclosures; and

4. All Personal Information collected must be Used and Disclosed in accordance with the Disclosure Documentation

Asteron will not Use or Disclose Personal Information for purposes other than those for which it was collected as outlined in corresponding disclosure documentation, except:

— Asteron may Use and Disclose the Personal Information for a secondary purpose only if that secondary purpose is directly related to a purpose of collection; or

— With the Consent of the Individual; or

— As otherwise required or authorised by law.

When Using Personal Information (other than Sensitive Information) for Direct Marketing purposes, Asteron must provide Individuals with appropriate opt-out mechanisms.

5. Asteron will provide the means for Individuals to access their Personal Information where it is lawful to do so

The Asteron Privacy Policy outlines relevant details on how Individuals can obtain access to, and seek correction of, their Personal Information. This also includes information about how the Individual may complain about a Privacy related issue.

Where a request is refused, Asteron will advise the Individual in writing with an explanation of the refusal and information on the recourse available.

6. The protection of Personal Information must adhere to Asteron's risk appetite and security protocols

Asteron will identify and appropriately manage Privacy related risks within the parameters of Asteron risk appetite and security protocols when dealing with Personal Information, including any Disclosure to Third Parties, whether based in the relevant jurisdiction or overseas. This includes:

— Completing Privacy Impact Assessments (**PIAs**) to identify and ensure appropriate action is taken to manage the Privacy related risks and impacts associated with any new initiatives or changes to existing processes relating to products, platforms, or customers involving the collection, use or disclosure of any Personal Information;

— Establishing appropriate processes to ensure the ongoing data quality and integrity of Personal Information held by Asteron, including processes for reviewing, updating and correcting an Individual's Personal Information upon request;

— Ensuring appropriate processes are in place to protect Personal Information from misuse, interference and loss, as well as unauthorised access, modification or disclosure in accordance with the Security Management Policy, associated security standards, and the IT Acceptable Use Policy;

— Ensuring appropriate processes are in place for training, monitoring and overseeing Third Parties, where they deal with Personal Information on Asteron's behalf, to ensure that they comply with Privacy obligations applicable to Asteron;

— Establishing appropriate processes for timely identification, reporting and remediation (where applicable) of Privacy incidents, including regulatory notifications where required;

— Establishing appropriate processes for permanent De-Identification and/or Destruction of Personal Information once it is no longer required for Asteron's functions or activities; and

— Maintaining adequate monitoring, oversight and reporting arrangements to evaluate the continued effectiveness of Privacy management processes and systems.

7. Asteron ensures adequate training of, and awareness by, its Employees of Asteron's Privacy management procedures

Asteron adequately informs Employees of its Privacy management procedures when dealing with Personal Information, by integrating Privacy compliance into staff training programs, with continuous education training undertaken on an annual basis. This training will ensure Employees understand their obligations when managing Personal Information and how, in turn, their own Personal Information is managed by Asteron.

8. Asteron will adhere to the requirements of the notifiable data/privacy breach requirements

Asteron will have processes in place to comply with the notifiable data/privacy breach. Asteron will review all privacy incidents in a timely manner to determine whether any individuals are likely to be at risk of serious harm as a result of a data/privacy breach. Where notifiable data/privacy breaches are identified Asteron will promptly notify the relevant regulatory body and affected individuals.

9. Asteron will adhere to the European Union (EU) General Data Protection Regulation (GDPR), to the extent it applies

The GDPR contains data protection requirements that applies to all businesses based in the EU, as well as those based outside the EU who offer products or services to, or otherwise monitor the activity of, people living in the EU. Consequently, some businesses covered by the New Zealand Privacy Act 2020 must also comply with the GDPR. As Asteron primarily offers financial products and services to customers in New Zealand only, the provisions of the GDPR will generally not apply. Policies and procedures that involve the design, implementation or management of processes and systems that handle personal data must have regard to GDPR requirements and when they may be triggered.

Role Accountabilities and Responsibilities

1. Employees and Officers

- Accountable for immediately reporting any potential or actual Privacy incidents to their leader or Risk and Compliance representative; and
- Responsible for ensuring the following:
  - Maintaining knowledge and understanding of, and always acting in accordance with, the processes relevant to their role and Function that have been developed to protect the Privacy of Individuals;
  - Promptly logging all identified Privacy incidents in GRC; and
  - Successfully completing mandatory compliance Privacy training on an annual basis.

2. Asteron CEO

- Accountable for implementing compliance management policies, frameworks and standards relating to privacy management and systems to effectively manage compliance obligations that arise within Asteron; and
- Responsible for ensuring the following:
  - Developing and maintaining adequate procedures and processes to ensure Personal Information is handled in accordance with this Policy and Asteron's Privacy obligations;
  - For CDR Data, developing and maintaining adequate processes to ensure compliance with the CDR regulation;
  - Ensuring Privacy is considered when identifying, assessing, and managing risk, as well as developing and monitoring controls for those risks;
  - Promoting Privacy compliance by integrating Privacy into staff training programs;
  - Regularly reviewing and maintaining Privacy Statements to ensure they are up to date and consistent with the Privacy Statement Template;
  - If applicable, regularly reviewing customer privacy disclosures were used in forms, call scripts or other collateral to ensure they remain fit for purpose;
  - Completing PIAs for initiatives that involve the collection, use or disclosure of Personal Information and meet the thresholds of the PIA Questionnaire; and
  - Establishing appropriate processes for:
    - Facilitating access to, and correction of, Personal Information;
    - Receiving and responding to Privacy enquiries and complaints; and
    - Managing Privacy incidents in line with the Asteron Incident Management and Breach Assessment and Reporting Standards and applicable Data/Privacy Breach Response Procedure.

3. Privacy Officer

- Responsible for ensuring the following:
  - Developing and maintaining Asteron-wide Privacy standards, guidelines, and training materials;
  - Regularly reviewing and updating the customer facing Asteron Privacy Policy and related supporting documents.

- In consultation with the Chief Risk Officer, Asteron, liaising with the relevant regulatory body on Asteron-wide Privacy matters;
- Providing guidance on the management of Serious or above Privacy incidents in accordance with the Incident Management and Breach Assessment and Reporting Standards; and
- The Privacy Officer must notify the Chief Risk Officer of any Privacy incident that may have an impact.

4. CRO (Chief Risk Officer) Asteron

- Responsible for ensuring the following:
  - Promoting a Privacy aware culture that reinforces the importance of good Privacy management to minimise Privacy related risks throughout the Personal Information life cycle; and
  - Providing independent challenge and oversight of the Asteron's Privacy management practices to assist Asteron in meeting its Privacy obligations.

5. Internal Audit

- Responsible to provide independent review and oversight of the governance and controls that are in place to manage Privacy compliance.

Policy Exemptions

No exemptions apply to this Policy.

Policy Breaches

All Policy breaches must be recorded in GRC in accordance with the Incident Management Standard, with the Policy Owner notified. Non-compliance with this Policy may result in disciplinary action (including termination of employment).

To the extent that this Policy imposes an obligation on Asteron, it does not form a contractual term, condition or representation.

Key Terms

Applicable Privacy laws	Includes the Privacy Act 2020 and New Zealand Privacy Principles.
CDR Regime	Currently in development in Parliament. This policy will require a review when the New Zealand CDR regulation is finalised.
Consent	May be express or implied consent.
Data/Privacy Breach Response Procedure	A Data/Privacy Breach Response Procedure sets out the roles and responsibilities involved in managing a data/privacy breach. It describes the steps Asteron will take if a data/privacy breach occurs.

De-Identification	Personal Information is de-Identified if the information is no longer about an identifiable Individual or an Individual who is reasonably identifiable. De-Identified information is not Personal Information.
Destruction	Personal Information is Destroyed or disposed of when it can no longer be retrieved.
Direct Marketing	Involves the Use or Disclosure of Personal Information to communicate directly with an Individual to promote goods and services.
Disclosure	The act of making Personal Information known, accessible or visible to a related company within Asteron or to a Third Party.
Notifiable Privacy Breach	Means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely to do so.
Individual	A natural person and could include: — a potential or existing customer or Supplier; or — an employee or representative of a corporate customer or Supplier; or — a Third-Party claimant or witness involved in a claim.
Personal Information	Any information or an opinion about an identified Individual, or an Individual who is reasonably identifiable: — whether the information or opinion is true or not; and — whether the information or opinion is recorded in a material form or not. Personal Information also includes Sensitive Information and Credit Related Information. Examples of the types of Personal Information Asteron collects about Individuals include names, postal addresses, email addresses, phone numbers, file notes about likes and preferences. Personal Information includes Unsolicited Personal Information.
Privacy	The rights and obligations of Individuals with respect to the collection, Use, Disclosure, security, integrity, access, correction and Destruction of Personal Information.
Privacy Statement	A document that Discloses who the Individual is dealing with and some or all of the ways Asteron collects, uses, discloses and manages Personal Information of the Individual.
Sensitive Information	Privacy regime, Sensitive Information means: (a) information or an opinion about an Individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or

	(v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record, that is also Personal Information; or (b) health information about an Individual; or (c) genetic information about an Individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.
Third Party	Parties that are not related to Asteron and are contracted to provide services or products to Asteron.
Unsolicited Personal Information	The Personal Information that has been received by Asteron where no active steps were taken to collect. Examples of this occurring include employment applications or misdirected mail.
Use	Asteron Uses Personal Information when it handles and manages that information within its effective control. Examples include accessing, reading, searching of the Personal Information or transferring the Personal Information to other entities or making decisions based on the Personal Information.

Policies and Procedures

Asteron has a suite of policies in place to support privacy.

Policy, Framework, Standard, Guideline, Process etc.	Description
Data Breach Response SOP	This SOP sets out the actions that Management must take when a data breach is discovered it should be read in conjunction with the Notifiable Data Breaches Guideline and Breach Assessment and Reporting Standard. The SOP covers two common scenarios: 1. a cyber or data event affecting Personal Information; and 2. accidental loss, inappropriate access to or disclosure of Personal Information. Asteron use the Incident and Breach Response Guidelines and the Breach Management Standard.
Data Classification, Handling and Quality Assurance Standard	This Standard sets out the information classification process and articulates the role and responsibilities of the Supporting Data Custodian with respect to information classification. The Standard sets out the data handling requirements based on the information classification, including how to comply with the Standard. Data handling includes transmission, storage and disposal of data.
Data Governance Framework	This Framework applies to all Asteron critical data in all its forms and covers usage and storage. It is an essential component of Asteron's overall corporate governance and supports Asteron's Enterprise Risk Management Framework and Privacy Management Policy. The Framework defines: – Asteron's implementation principles for Data Governance. – The key data capabilities and processes for governing Critical Data at Asteron. – The key elements of 'How Data Governance works' at Asteron. – Aligns to the Security Management Framework.
Data Governance Standard	This Standard outlines the mandatory processes and controls against each of the components of the Data Governance Framework to make the overarching principles of the Data Governance Framework more meaningful and effective - Standards & Guidelines - Organisation - Processes - Tools & Technology - Governance Controls This Standard applies whenever Asteron information is used or stored.

Data Quality Standard	This Standard provides an overview of the Data Quality Model including the discrete steps that are undertaken as part of the data quality management process at Asteron as follows: - Assess and Discovery - Profiling - Data Quality Monitoring - Issue Management & Remediation This Standard aligns to regulatory guidance.
Data Retention Standard	This Standard specifies the data retention process, criteria and timings that support and conform to Asteron's data retention obligations. It covers all electronic and physical personally identifiable data & records that Asteron owns. This Standard aligns to the New Zealand Privacy Act 2020.
Data Sharing Standard	This Standard defines three types of data as part of a data sharing relationship: - First Party Data - Second Party Data - Third Party Data Business Owners of the data sharing arrangements are responsible for assessing the data type classification and adhering to data governance requirements based on the data type classification. This Standard includes an overview matrix of data governance requirements with links to more information.
Enterprise Portfolio Governance (EPG) Framework	This Framework is a collection of practices, tools, templates, supporting frameworks and forums that support Asteron's project and portfolio management community.
Enterprise Risk Management Framework (ERMF)	This Framework describes how risk is managed at Asteron and applies to all of Asteron (unless precluded by specific legal or regulatory requirements). The Framework operates in conjunction with the Risk Appetite Statement (RAS) and Risk Strategy.
EU General Data Protection Regulation Guidance	This Guidance is designed to improve awareness and understanding of the requirements in the European Union (EU) General Data Protection Regulation (GDPR) and how and when the GDPR requirements apply to Asteron.
Incident Management Standard	This Standard provides clear, minimum requirements for recording and managing incidents across all material risk types.
Incident and Breach Response Guideline	This Guideline provides practical advice about the identification, remediation, assessment and notification of suspected and notifiable data breaches.
Privacy Impact Assessment (PIA) documentation	This Process consists of a PIA Threshold Assessment followed by a full PIA, if required. The Process supports a 'privacy by design' approach whereby privacy compliance is built into business processes right from the start. The process will help to identify privacy risks in the design of a new or changed business initiative, third-party engagement or BAU change.
Privacy Statement for Employees	This Standard outlines how Asteron manages the personal information of employees. This Standard does not apply to contingent workforce participants or candidates for employment (unless the candidate is successful.)

ROCSA Standard	This Standard provides clear, minimum requirements for establishing non-financial and insurance risk events, obligations and controls that could materially impact Asteron's objectives during the business plan period. The key requirements of the Standard are to: – establish context and maintain risk-based value chains and sub-processes, – identify and assess risk events, obligations and controls, – consolidate risk events into risk profiles and obligations into compliance plans, and – monitor and manage risk events, obligations and controls.
Risk Appetite Statements	Risk appetite is the expression of the risk that Asteron is willing to accept in the pursuit of our strategic objectives. Risk appetite as a key component in setting the strategic direction of Asteron.

Policy Administration

Document Title	Privacy Management Policy
Version No.	1.0
Policy Owner	Chief Risk Officer, Asteron Life Limited
Policy Administrator	Chief Risk Officer, Asteron Life Limited
Primary Relationship Policies *(These must be read in conjunction with the Policy)*	Compliance Management and Regulator Engagement Policy Security Management Policy
Supporting frameworks, procedures or guidelines *(These must be read and implemented in conjunction with the Policy as required)*	See under *"Policies and Procedures"* above
Date of publication/effective date	1 February 2025
Date of last review	-
Next scheduled review	October 2025
Regulator (if applicable)	Privacy Commissioner
Compliance Assurance	Privacy Compliance Plan Due Diligence Process
Approval Body	Board

Policy History

Date	Comment	Version	Approval
01/02/2025	Approval of the policy	1	Board