SHEARWATER INFORMATION SECURITY POLICY

1. PURPOSE AND SCOPE
This Information Security Policy (“Policy”) outlines Shearwater’s approach to information security management and provides the guiding principles and responsibilities necessary to safeguard the security of the information systems and is aligned with the business goals and strategy. Shearwater is committed to the confidentiality, integrity and availability of information, because failure to adequately secure information, risks significant reputational and financial losses.

This Policy governs all aspects of hardware, software, communications, and information. This Policy applies to all Shearwater Co-workers and Business Associates (as defined in Shearwater’s Code of Conduct). It also applies to other entities who may be given permission to log in, view or access Shearwater information.

2. ROLES AND RESPONSIBILITIES

• Information Security Officer
  o Overall responsibility for all aspects of Information Security.

• Information Security Committee
  o Cross-functional group responsible for the implementation and monitoring of Information Security.

• IT Security Team
  o IT systems on site and cloud based, Information security technical solutions, monitoring and response to incidents, testing and specialist advice.

• Legal Team
  o Advising upon and reporting of breaches of personal data to appropriate authorities.

• Co-Workers and Business Associates
  o Adherence this policy and all associated standards, procedures and guidelines.

3. INFORMATION SECURITY PRINCIPLES

• The risk appetite for Shearwater, each business area and type of information will be defined.
• Information will be classified according to confidentiality and availability requirements and in accordance with relevant legislative, regulatory and contractual requirements.
• All Co-workers and Business Associates must ensure the information is handled in accordance with the classification.
• Information will be protected and secured against unauthorised access and processing.
• Shearwater will provide industry leading technical solutions and mandatory training to aid with the protection of information.
• Drills and tests will be carried out on a regular basis to monitor performance.
• Incidents and non-compliance will be reported in the incident reporting tool, all major and catastrophic incidents should be brought to the attention of the Information Security Officer and committee immediately.
• Breaches of personal data will be reported to the Legal team for appropriate handling and notification to authorities.

Violations of this policy may result in disciplinary action, up to and including, termination of employment.

4. IMPLEMENTATION
This Policy has been approved by the CEO and shall be effective as of 12th January 2024 and may be revised from time to time.