shearwater

SHEARWATER INFORMATION SECURITY POLICY

1. PURPOSE AND SCOPE

This Information Security Policy ("Policy") sets out how Shearwater manages information security. It provides the principles and responsibilities that protect the confidentiality, integrity and availability of information, and gives the framework for setting information security objectives We commit to satisfying applicable legal, regulatory, contractual and other requirements, and to the continual improvement of our Information Security Management System (ISMS), in line with Shearwater's business strategy.

This Policy applies to all Shearwater Co-workers and Business Associates (as defined in the Code of Conduct), and to third parties authorised to access Shearwater information or systems It governs information, hardware, software, communications and services within the boundaries defined in Shearwater's ISMS Scope Statement, including relevant business processes, locations and assets

2. ROLES AND RESPONSIBILITIES

- **Board of Directors**
  Approves this Policy, reviews ISMS performance at least annually, and sets the information security risk appetite in line with business objectives
- **Executive Management**
  Demonstrates commitment, sets measurable security objectives, allocates resources, removes blockers, and drives continual improvement of the ISMS
- **Chief Information Security Officer (CISO)**
  Accountable for ISMS implementation and maintenance; policy owner, reports performance, risks and improvement needs to Executive Management and the Board
- **Information Security Committee**
  Oversees ISMS execution and risk management, ensures cross-functional coordination, and tracks progress against objectives.
- **Operational Security**
  Runs day-to-day security controls, coordinates with the outsourced Security Operations Centre (SOC), monitors threats, responds to incidents, and supports business continuity planning
- **Legal Team**
  Advises on compliance, including cross-border data transfers and intellectual property (IP) protection; manages personal data breach reporting to authorities as required
- **Information/Asset Owners**
  Classify information and approve access in line with the Information Classification and Handling Standard, ensure controls for their assets remain effective.
- **Co-Workers and Business Associates**
  Follow this Policy and related standards/procedures, complete induction and annual refresher training, and report incidents promptly.

3. INFORMATION SECURITY PRINCIPLES

- **Objectives and improvement**
  We protect the confidentiality, integrity and availability of information, meet legal/contractual obligations, and continually improve the ISMS. Objectives are documented, measurable, and reviewed at least annually and after significant change
- **Classification and handling**
  Information is classified by sensitivity and handled accordingly, following the Information Classification and Handling Standard.
- **Access control**
  Access is based on role and least privilege Information/Asset Owners approve access. Reviews take place at defined intervals and when roles change

- **Cryptography**
  Sensitive data is encrypted at rest and in transit using approved cryptographic standards.
- **Secure disposal**
  Information and assets are disposed of securely at end of life.
- **Risk management**
  Risk assessments run at least annually and when risks, technology or operations change. Risks are treated to acceptable levels in line with documented risk appetite.
- **Suppliers and third parties**
  Suppliers/third parties with access to our information or systems undergo risk assessment and must meet the Supplier Security Policy. Security requirements are built into contracts and monitored.
- **Business continuity**
  Continuity and recovery measures are established and tested at least annually.
- **Testing and drills**
  Security drills and tests run at least annually and after significant change to check performance.
- **Incident management**
  Incidents and non-compliance are reported through the incident tool. Major incidents are escalated to the CISO and the Information Security Committee within one hour of detection, with lessons learned tracked to closure.
- **Personal data breaches**
  All personal data breaches are reported to Legal for handling and notifications. This includes supplier breaches and follows the Personal Data Breach Response Procedure.
- **Awareness and training**
  All Co-workers and Business Associates complete induction and annual refresher training, supported by regular awareness activity.

4. POLICY COMMUNICATION AND DOCUMENT CONTROL

This Policy is published on the intranet, covered in onboarding and annual training, and material updates are communicated to all affected Co-workers and Business Associates; relevant parts are shared with suppliers where needed. ISMS documents are approved, versioned and reviewed at least annually per the ISMS Document Control Procedure; only current versions are in use and obsolete versions are withdrawn or clearly marked.

5. IMPLEMENTATION

This Policy has been approved by the CEO and is effective from August 21st, 2025. It is reviewed at least annually and when there are significant changes in risks, technology, the regulatory environment or the needs and expectations of interested parties.

Irene Waage Basili
CEO