Information Management Policy

TurnMill Group recognizes the importance of responsibly managing information to protect the confidentiality, integrity, and availability of data assets. This Responsible Information Management Policy outlines our principles and expectations for the secure and ethical handling of information across the organization.

Data Classification

TurnMill Group classifies information based on its sensitivity and criticality to the organization. Common classifications include:

- Confidential: Information requiring the highest level of protection due to its sensitive nature (e.g., trade secrets, financial data, personal information).
- Internal Use Only: Information intended for internal use only and not to be shared externally without authorization.
- Public: Information intended for public consumption and does not require special protection.

Access Control

- Access to information is granted on a need-to-know basis, with appropriate access controls implemented to prevent unauthorized access, modification, or disclosure.
- Employees are provided with unique user accounts and are required to use strong passwords and multi-factor authentication where applicable.

Data Protection

- TurnMill Group employs technical and organizational measures to protect data against unauthorized access, loss, or destruction. This includes encryption, firewalls, antivirus software, and regular data backups.
- Personal data is processed in accordance with applicable data protection laws and regulations, and individuals' privacy rights are respected at all times.

Data Retention and Disposal

- TurnMill Group establishes data retention periods based on legal requirements, operational needs, and business considerations. Data that is no longer required is securely disposed of using approved methods.
- Employees are responsible for identifying and securely disposing of obsolete or unnecessary data in accordance with established procedures.

Information Security Awareness

- TurnMill Group provides regular training and awareness programs to educate employees about information security risks, policies, and best practices.
- Employees are encouraged to report any suspected security incidents or breaches promptly to the IT department or designated security contact.

Compliance Monitoring and Enforcement

- TurnMill Group regularly monitors compliance with this policy through audits, assessments, and reviews. Non-compliance may result in disciplinary action, up to and including termination of employment.
- Employees are required to cooperate with compliance efforts and report any violations or concerns to their supervisor or the appropriate authority.
- TurnMill Group conducts regular Risk Assessments according to the document “Framework for Information Security Risk Assessment”.

Third-Party Information Handling

- Third-party vendors and partners are contractually obligated to adhere to similar information management standards and practices as TurnMill Group.
- Due diligence is conducted on third parties to ensure they meet our security and privacy requirements before engaging in business relationships.

Continuous Improvement

- TurnMill Group is committed to continuously improving its information management practices through regular review, assessment, and adaptation to evolving threats and regulations.
- Feedback from employees and stakeholders is welcomed and considered in the ongoing enhancement of our information management processes.

Governance and Reporting

Adherence to this Responsible Information Management Policy is essential to safeguarding TurnMill Group's information assets and maintaining trust with our customers, partners, and stakeholders. Every employee is responsible for upholding these principles and contributing to a culture of information security and integrity. This policy, targets and achievements are reviewed annually by the Board of Directors and quarterly by the Executive Team to ensure target progress and resource allocation.

Jesper Blomquist, MD TurnMill Group AB

Targets

Target	When
All staff trained in Information Management Policy	2024-09-30
Information Security Risk Assessment performed and documented	2025-01-01
Regular monitoring and enforcement established	2025-01-01
Review and improve business continuity and disaster recovery plans	2025-06-30