

INFORMATION SECURITY POLICY

The **objective** of information security policy is to ensure the preservation of information security of CIF and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

The **policy's goal** is to ensure the preservation of information security of CIF (information, information systems and information processing facilities) against all internal, external, deliberate or accidental threats.

The Managing Director has approved the information security policy and supports active acknowledgment and implementation of its principles and values among all employees and other interested parties.

Objectives and principles that CIF applies regarding information security:

- Information shall be protected against any **unauthorized access**
- **Confidentiality** of information shall be assured
- **Integrity** of information is assured
- **Availability** of information for business processes is maintained
- **Legislative and regulatory** requirements shall be met
- **Business continuity and disaster recovery plans** are developed, maintained and tested
- **Information security training** is available for all employees
- **All actual or suspected information security breaches** shall be reported and thoroughly investigated
- **Processes for handling deviations and exceptions** are established
- Commitment to **continual improvement** of the information security management system.

Policies, procedures and other documentation exist to support this policy.

Business requirements for information security and systems are met by implementation of the ISO/IEC 27000 series of standards, BaFin Supervisory Requirements for IT in Financial Institutions (BAIT) and Technical and Organizational Measures to ensure the Security of the Data (TOMs) and other applicable requirements.

The Management Representative is responsible for maintaining the policy and providing support and advice during its implementation.

All managers and process owners are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.

Compliance with the Information Security Policy is mandatory for all employees and other relevant parties.

Date: 19.09.2022.