Policy Statement

At the Alternative Bank, we recognize that information and information systems are critical assets, essential to maintaining trust, ensuring compliance, and achieving our business objectives. Protecting the confidentiality, integrity, and availability of these assets is central to our operations and long-term success.

In line with ISO/IEC 27001, the Alternative Bank is committed to:

- Establishing and maintaining an information security management system (ISMS) that is appropriate to the Bank's purpose and aligned with its strategic objectives.
- Meeting all applicable legal, regulatory, contractual, and stakeholder requirements related to information security.
- Continually improving the ISMS to adapt to changing risks, business needs, and the evolving threat landscape.

To achieve these commitments, the Alternative Bank shall pursue the following information security objectives:

1. Ensure confidentiality, integrity, and availability of systems and customer data through implementation of baseline security controls, continuous monitoring, and incident detection capabilities
2. Establish robust data protection and fraud prevention controls aligned with applicable regulatory and legal requirements
3. Implement real-time monitoring, alerting, and incident response processes to ensure timely detection, reporting, and remediation of security events
4. Enforce strong identity, authentication, and access management controls based on least privilege and segregation of duties principles
5. Integrate security requirements into business processes, system workflows, and operational procedures
6. Implement governance structures, risk assessment processes, and reporting mechanisms to ensure ongoing compliance with applicable regulatory obligations
7. Ensure all new systems, applications, and technologies undergo risk assessment, security review, and testing prior to deployment

To support these objectives, The Alternative Bank shall implement suitable policies, processes, procedures, organizational structures, and technical and physical controls.

We will also provide regular awareness and training to employees and stakeholders to promote a culture of information security and resilience.

This policy shall be maintained as documented information, communicated to all employees, contractors, and third parties, and made available to interested parties as appropriate. It will be reviewed annually—or sooner if required—to ensure continued suitability, adequacy, and effectiveness.