

Information Security Management System Policy

In today's digital era, the banking sector is especially vulnerable to information security threats due to the sensitive and high-value nature of the transactions it processes. The increasing use of interconnected systems, shared infrastructure, and digital platforms has significantly broadened the risk landscape. In this context, ONE Bank PLC recognizes the critical importance of safeguarding its information assets to ensure secure, resilient, and trustworthy banking operations. This policy statement supports the Bank's strategic direction by reinforcing customer trust, enabling business continuity, complying with regulatory requirements, and protecting shareholder value through strong information security governance.

ONE Bank PLC is committed to establishing, implementing, and maintaining an Information Security Management System (ISMS) that is appropriate to the purpose, context, and strategic direction of the Bank. The ISMS is designed to protect the Confidentiality, Integrity, and Availability (CIA) of all information assets against unauthorized access, disclosure, modification, or destruction. The Bank adopts a risk-based approach to information security by proactively identifying threats and vulnerabilities, assessing their potential impacts, and applying appropriate risk treatment measures in line with international best practices.

This policy statement provides a framework for establishing and reviewing measurable information security objectives that align with the Bank's business goals. These objectives aim to support secure digital banking operations, compliance excellence, customer satisfaction, and a competitive position in the market. Objectives are set across relevant functions and levels of the organization and are monitored and reviewed periodically to ensure their ongoing effectiveness.

ONE Bank PLC is fully committed to complying with all applicable legal, regulatory, contractual, and other requirements related to information security. This includes adherence to both national laws and globally accepted standards where applicable. The Bank ensures these requirements are integrated into its ISMS and continually monitored to maintain legal compliance and mitigate reputational and financial risks.

The Bank also maintains a strong commitment to the continual improvement of its ISMS. This is achieved through regular risk assessments, internal audits, incident investigations, management reviews, and the implementation of corrective and preventive actions. By fostering a culture of continual learning and adaptation, ONE Bank PLC strives to enhance the resilience and maturity of its information security program.

To promote transparency and shared understanding, this policy statement is communicated internally to all relevant personnel and made available to external interested parties as appropriate. Regular awareness and training programs are being conducted to ensure that all employees are informed of their roles and responsibilities in protecting the Bank's information assets and supporting the Information Security Management System (ISMS).

This policy statement is formally approved and supported by top management, demonstrating leadership commitment to its principles and implementation. It is reviewed at planned intervals or when significant changes occur, to ensure its continued relevance, adequacy, and effectiveness in addressing evolving threats, regulatory changes, and business needs.

Date: 01 June, 2025


Managing Director (CC)
ONE Bank PLC