

National Bank of Iraq

Information Security Policy

Introduction

The management and Board of Directors of the National Bank of Iraq, located in Baghdad, Al-Saadoun Street, shall maintain the confidentiality, integrity, and availability of all informational assets, including Personally Identifiable Information (PII) within the bank. This commitment aims to preserve the bank's competitive advantage, profitability, legal and regulatory compliance, and its reputation to ensure that information requirements, privacy, and information security are aligned with the objectives of the National Bank of Iraq. The Information Security Management System (ISMS) is designed to enable secure information exchange, electronic operations, and e-commerce while reducing information and privacy-related risks to acceptable levels.

Compliance and Obligations

The National Bank of Iraq shall ensure compliance with all applicable legislative, regulatory, and contractual requirements, including all laws related to the protection of personal information (PII).

Information Security Risk Management Framework

The bank's current strategic business plan and the approved risk management framework provide the necessary context for identifying, assessing, and monitoring risks related to information and privacy through the establishment and maintenance of the ISMS. The initial risk assessment, risk acceptance statement, and risk treatment plan outline how to control risks related to information, privacy, and physical assets. The Information Security Risk Manager shall manage and maintain the risk treatment plan. Additional risk assessments may be conducted when necessary to determine appropriate controls for identified risks.

Objectives and Controls

Business continuity plans, data backup procedures, antivirus and anti-malware protections, system access controls, and security and privacy incident reporting are essential components that support this policy. Control objectives for each of these areas are supported by specific documented policies and procedures.

Privacy Security Objectives

The National Bank of Iraq seeks to achieve specific and clear objectives in the field of information security and privacy, developed based on business goals, organizational context, risk assessment outcomes, and the risk treatment plan.

Employee Compliance

All employees of the National Bank of Iraq and external parties specified in the Information Security Management System (ISMS) are required to comply with these provisions. All employees receive appropriate training in information security and cybersecurity. External parties and service providers are required to ensure adequate training for their staff. Consequences of violating information security and privacy policies are determined in accordance with the bank's disciplinary policy and the contracts signed with third parties.

Review and Improvement of the ISMS

The ISMS is subject to continuous review and improvement. The Information Security and Cybersecurity Committee has been formed, headed by the CEO, the Information Security Manager, other executive directors, and specialists to support the ISMS framework and periodically review the security policy.

Compliance with Security Standards

The National Bank of Iraq shall comply with the highest international security standards and the security controls mandated by local regulatory authorities, including the Central Bank of Iraq, to adhere to best practices aimed at protecting data and information and ensuring their confidentiality, integrity, and availability.

Annual Review

This policy is reviewed in response to any changes in risk assessment or the risk treatment plan, on an annual basis or as needed.

Key Definitions in This Policy:

1. Information Security Management System (ISMS)

A set of policies and procedures aimed at protecting sensitive information and ensuring the confidentiality, integrity, and availability of data within the bank.

2. Confidentiality

Ensure that information is accessible only to authorized individuals, thereby preventing unauthorized access to the bank's data and systems.

3. Integrity

Ensure the accuracy and completeness of information and its processing, protecting it from unauthorized alteration or destruction.

4. Availability

Ensure that information and associated assets are accessible to authorized users when needed, requiring the bank's internal network to remain operational without interruption.

5. Physical Assets

Includes all physical assets of the bank, such as computers, cables, phone systems, file systems, and physical data.

6. Information Assets

Includes all informational assets such as electronically stored or transmitted data, and software operating systems.

7. Privacy Breach

Any incident or activity that causes or may cause the disclosure of personal or sensitive information without the consent or authorization of the concerned parties.