INFORMATION SECURITY POLICY

PIRAEUS BANK ICB JSC

2021

Contents

1. Information Security Policy

1.1. Introduction

The Information Security Policy ("Policy") is the internal regulation that sets out and reflects the position of PIRAEUS BANK ICB JSC (the "Bank") with respect to information security. It describes the information security development strategy and the basic principles formulated by the Bank Management that define the structure of the Bank's information security.

Banking information is an important asset of the Bank. All banking information is subject to protection based on its value and in a way that would enhance customers' trust, ensure compliance with regulatory requirements, and maintain the competitiveness of the Bank.

This document sets forth the strategic vector of information security development and the principles established by the Bank Management that are applied to manage information security of the Bank with a view to achieving the objective of the Bank's business strategy. Other, more specific, policies, procedures, standards, instructions, regulations, and guidelines are drafted subject to the requirements of this Policy.

1.2. Scope

The requirements of the Information Security Policy apply to all units of the Bank and are binding on all employees of the Bank; it is also applicable to suppliers, providers, partners, and companies whose services are related to using, processing, or accessing information or information assets of the Bank or who process or use banking information in their operations.

All personnel of the Bank, including external partners of the Bank, must adhere to the Information Security Policy. Any failures to comply with the Information Security Policy must be investigated. Should any violations be revealed, the guilty parties will be held liable in accordance with the applicable laws of Ukraine.

1.3. Terms and definitions

"**Bank**" means PIRAEUS BANK ICB JSC.

"**Banking information**" means information (whether in electronic, written, or verbal form) processed in the Bank and used to maintain the business processes of the Bank. Information created by third parties on behalf of the Bank and information in and to which the Bank holds copyrights also falls under the banking information.

"**Information system**" means any hardware and software tools and data that support the business processes of the Bank.

"**Information owner**" means a unit of the Bank (or any part of its unit) responsible for the functioning of business processes, depending on information processed. An information owner is responsible for protecting information and determining what information is to be used and who may have access to such information.

"Information security" means a set of processes and measures to ensure availability, confidentiality, integrity and tracebility of information.

"**Availability**" means accessibility of information or of an information asset that characterizes the possibility of using information or an information system upon request of an authorized object in the minimum required amount.

"**Confidentiality**" means a characteristic of information (or of an information asset) that may not be accessed by an unauthorized person, object, and/or process as a result of legal restrictions imposed by its owner.

"**Integrity**" means a characteristic of information (or of an information asset) that may not be modified without the authorization of its owner.

"**Traceability**" means a system characteristic that allows to record user activities and processes and determine accurately identifiers of users and processes associated with certain events to prevent security policy violations and/or ensure liability actions.

"Information security management system (ISMS)" means a part of the overall management Bank's system, that is based on risk assessment and is intended for create, implement, exploitation, control, analysis, support and improvement of information security of the Bank.

"Critical information assets (critical information)" means a set of information in written or electronic format that is valuable to Bank or Bank's customers and unauthorized or uncontrolled disclosure may harm the Bank and/or its client. Criticality of information is based on classification level to availability, confidentiality and integrity.

"**Bank Management**" means Chairman and members of the Supervisory Board of the Bank, Chairman and members of the Management Board of the Bank.

1.4. Regulatory framework

This Policy is drafted subject to the following requirements:

- National standards of Ukraine in information security:
  - DSTU ISO/IEC 27000:2015 "Information technology. Methods of protection. Information security management system. Overview and glossary";
  - DSTU ISO/IEC 27001:2015 "Information technology. Methods of protection. Information security management systems. Requirements";
  - DSTU ISO/IEC 27002:2015 "Information technology. Methods of protection. Corpus of information security practices";
- Resolution No. 95 of the Management Board of the NBU "On approving the Regulation on Implementing Measures to Ensure Information Security in the Ukrainian Banking System" of Sept. 28, 2017;
- Resolution No. 4 of the Management Board of the NBU "On approval of the Regulation on control over the observance by banks of the requirements of the legislation on information security, cybersecurity and electronic trust services" of Jan. 16, 2021;
- Guidelines and rules adopted within the Piraeus Bank Group.

1.5. Purpose, goals, and objectives

The purpose of the Policy is to implement and maintain the effective operation of the ISMS, which is designed to ensure the necessary level of information security under routine operating conditions and upon occurrence of potential threats, and to protect information and resources of the Bank against external and internal threats and threats related to intentional and unintentional actions of the Bank's employees.

The goals and objectives of the Bank's Information Security Policy are:

- Supporting the business objectives of the Bank by ensuring confidentiality, integrity, and availability of banking information and information systems;
- Reducing the risk of disturbing confidentiality, integrity, and availability of banking information by establishing the rules of appropriate use of banking information and information systems;
- Introducing common rules of information security among the Bank's personnel, thereby defining duties, responsibility, and role of each employee;
- Ensuring compliance with all regulatory requirements and contractual obligations;
- Ensuring protection of the business reputation and image of the Bank;
- Ensuring growth of the Bank and enhancing customers' trust in products and services of the Bank, thus creating competitive advantages;
- Managing information security, including defining information security roles and responsibilities;
- Establishing and maintaining the information security management system ("ISMS") of the Bank;
- Classifying information assets;
- Assessing information security risks;
- Ensuring security of information assets considering their classification category and risk assessment;
- Monitoring information security events and managing information security incidents;
- Ensuring continuity of the Bank's business to the extent of information security;
- Coordinating and controlling ensuring secure management of the Bank's information system life cycle.

1.6. Key information security requirements, rules, principles, roles, and responsibilities

Principles and rules:

- The Bank's public services and internal networks comply with information security standards;
- With a view to reducing the information security incident risk, the management of the Bank ensures that all employees of the Bank can be regularly trained in information security regulations and measures;
- Business continuity plans are drawn up, in effect, and regularly tested and updated at the Bank;
- Employees of the Bank participate in maintaining the proper information security level to the extent of their duties and responsibilities and are liable for a failure to maintain it under the applicable laws of Ukraine and internal regulations of the Bank.

The Bank applies the following requirements for ensuring information security:

- The list of critical processes, information resources (assets) that ensure their functioning and measures for their protection are identified;
- The list of information regarded as bank secrecy is drawn up and approved;
- The criticality of information assets is assessed;
- The rules of accessing information resources and software and hardware suites are established;
- The control of physical and logical access to all available resources is ensured;
- The anti-virus protection of information resources is ensured;
- The network protection and protection of remote access to (local, internet, and third-party) network resources is ensured;
- The identification and authentication of all designated resources is ensured;

- The cryptographic protection of information is ensured;
- The Bank must develop information security requirements for third parties who provide IT outsourcing and information system and resource development and implementation services to the Bank and receive restricted information from the Bank. Such requirements and responsibility for, and control of, their performance by the above third parties are set out in agreements with those parties.

Roles and responsibility:

- Effective information security of the Bank is ensured by continuous involvement of employees of all units at all operating levels;
- Each employee of the Bank ensures that the proper level of the Bank's information security is maintained;
- Within the purview of their functional duties and powers, the employees must comply and be responsible for complying with the Policy requirements and legal, regulatory, and intrabank rules and are liable for any violations thereof under the applicable laws of Ukraine and internal regulations of the Bank;
- A specific management body for information security is established and permanently functions in the Bank (the "ISMS management body"); its decisions are binding on all employees of the Bank;
- The ISMS management body ensures developing, implementing, functioning, monitoring, reviewing, maintaining, and improving the ISMS;
- The ISMS management body is responsible for defining information security objectives and ensuring their compliance with the applicable laws of Ukraine, including regulations of the National Bank of Ukraine and regulations of the Bank, as well as their integration with the business processes and banking products;
- The ISMS management body approves and reviews the Policy, analyzes its implementation effectiveness, and supervises any Head Office unit and Bank units to the extent of their compliance with information security regulations of the NBU and of the Bank by initiating audits of Head Office units and Bank units before the Head of the Management Board of the Bank with respect to the implementation and operation of the ISMS and performance of the ISMS management body's decisions. The ISMS management body exercises ongoing control of implementing, improving, and updating the Policy;
- With a view to reducing the information security incident risk, the management of the Bank ensures that the employees can be regularly trained in information security regulations and measures.

2. General provisions on information security

The Bank Management's commitment to information security management is evident and clear to all employees of the Bank. The information security development strategy reflects the Bank Management's goal to establish a reliable information security system. For this purpose, the Bank Management approves security policies, procedures, standards, and rules and ensures compliance therewith.

This document sets out the role of the Bank Management in relation to information security. The general principles of information security determine basic necessary actions and measures required to be taken to establish a protected working process. Those principles represent a summary of provisions of the Information

Security Policy that are binding on all employees of the Bank and other persons who have access to banking information or information systems.

The general provisions are based on the Banks' information security needs determined by assessing the risks in information systems and examining international information security standards and national regulations.

The general provisions establish the minimum security level as determined by the Bank Management, which is applicable to all employees of the Bank and third parties. The general provisions demonstrate the importance and necessity of protecting banking information.

All decisions on information security and information system security are made with due regard to the provisions hereof as the minimum requirements for information security.

The general provisions on information security applicable in each entity are divided into basic and functional provisions.

2.1. Basic provisions

Basic provisions are general directions used to establish and maintain on the whole an acceptable level of the Bank's information security. Basic provisions provide the grounds for defining the functional principles.

2.1.1. The Bank's chief information security officer (CISO) is the head of the Management Board of the Bank (or a person replacing him) and ensures:

- the strategic management of the Bank's information security;
- defining development areas of the Bank's information security and their compliance with the development strategy of the Bank;
- that information security measures are consistent with the requirements dictated by business processes/banking products;
- controlling implementing information security measures at the Bank.

2.1.2. Subordinacy and/or accountability make it possible to review actions of parties involved in information processing and ensure that actions of a user (being an employee or a third-party employee) may identify that user unambiguously. Roles and responsibility are determined subject to the criticality of information.

2.1.3. The responsibility for controlling that the Policy requirements are complied with and that subordinate employees are informed in a timely manner of information security issues is borne by their respective supervisors. Each employee must ensure that the proper information security level is maintained. Within the purview of their functional duties and powers, the employees must comply and be responsible for complying with the Policy requirements and regulations approved within the Bank.

2.1.4. All rules and methods used to assure an acceptable level of information security at the Bank are consistent with the established social and ethical standards.

2.1.5. An acceptable information security level is achieved as a result of joint actions of information owners, information system users, information system administrators, and information security experts. Decisions are made after an in-depth analysis and discussion and after assessment of all involved units of the Bank to achieve the highest level of reasonable information security.

2.1.6. The security and control mechanisms applicable to each information asset are proportionate to the value of that asset, threats that may affect that asset, and losses that may be incurred in the case of an information security breach of that asset.

2.1.7. The integrity principle – implementing mechanisms, policies, procedures, and standards as an integral information security system helps achieve more effective security and reduce the system cost and complexity.

2.1.8. Create an order of response to incidents. Where an information security incident occurs, the personnel of the Bank responds in a timely and coordinated manner, in accordance with the approved information security incident processing procedures. The timely use of appropriate administrative and technical security tools helps reduce and prevent future threats.

2.1.9. Due to the development of information technology and business requirements, the Bank's information and information systems are exposed to more threats and vulnerabilities so that the current situation must be reassessed regularly. A reassessment helps reveal the deviations with respect to implemented security and control mechanisms and tools as well as the excessive risk. Risk management is quite an important objective of the Bank, in the same way as making decisions to accept risk or mitigate risk to an acceptable level.

2.1.10. The Information Security Policy and security controls used in the Bank respect and do not violate the rights of parties involved in information processing.

2.2. Functional principles

Functional principles are derived from basic provisions. They cover specific subject areas (information security policies, procedures, standards, instructions, regulations, and guidelines) and determine the scope of the information security management system of the Bank.

2.2.1. Compliance with the Information Security Policy

All employees of the Bank understand the necessity of protecting banking information and comply with all requirements set forth in information security policies, procedures, technical standards, and guidelines. The Information Security Policy must be brought to notice of the Bank's personnel and third party representatives who have access to the Bank's information and information systems.

2.2.2. Designation of an information owner

To be designated for all types of banking information is an information owner, who is responsible for its business functions. An information owner is also responsible for protecting information, even if another, more specialized, party was made responsible for information processing or if the information owner authorized a third party to have access to information.

2.2.3. Classification and protection of information

All banking information must be classified in accordance with the established classification rules. An information owner classifies information into a particular category based on its confidentiality, integrity, and availability. Furthermore, information is protected accordingly while stored, processed, and transferred. Classification of information ensures that information is used and protected properly.

2.2.4. Organizational structure of the information security system

Information security is an overall objective of the Bank. Close cooperation on the side of all units of the Bank is necessary to achieve an acceptable security level. For this purpose, security tasks (roles, objectives, and responsibilities), in the same way as critical procedures, must be clearly defined throughout the Bank to achieve certainty and common ground in selecting and using administrative and technical security mechanisms.

To resolve information security system management issues, an information security management body is established in the Bank; it comprises representatives of units that own and participate in critical business processes, information security experts, and where applicable, representatives of other units of the Bank.

The Bank has an information security division, that directly subordinated to the Bank’s Chief information security officer. The information security division controls and coordinates designated persons with respect to the application of the Information Security Policy of the Bank (Piraeus Group) in different areas, implementation of appropriate protection and control mechanisms, and effective accomplishment of information security objectives. The information security division is prohibited from developing, implementing, supporting, or operating the Bank’s information systems not used for ensuring information security.

2.2.5. Effectiveness of administrative and technical information security controls

In order to maintain an acceptable level of information security at the Bank, administrative and technical controls must be implemented. Administrative and technical controls are crucial as they are interrelated and form the single information security management system.

Administrative and technical controls used in the Bank are audited to verify their compliance with the existing policies, procedures, and standards, reassessed in terms of their effectiveness in preventing existing targets, and updated subject to information security requirements.

2.2.6. Liability for compliance with information security requirements by employees

Department directors and managers of standalone units of the Bank must take all necessary measures to ensure compliance with information security policies, procedures, standards, instructions, regulations, and guidelines within their units. The Bank Management and all employees at all levels of the Bank’s organizational structure are liable for the overall information security level and compliance with the Information Security Policy in the Bank (top-down approach).

2.2.7. Information Security Policy audit

Regular and direct audits are conducted to verify compliance by the Bank’s employees with information security policies, procedures, standards, instructions, regulations, and guidelines.

2.2.8. Regulatory compliance

Controls and tools implemented to protect banking information, which are determined and selected based on existing regulations and contractual obligations of the Bank and ensure a free exchange of ideas, free information flow, confidentiality of information and communications, personal data protection, and process transparency.

In accordance with the requirements of the current legislation, the Chairman of the Management Board of the Bank (or a person replacing him) organizes an external audit (in order to obtain the Bank's information security assessment) in accordance with the legislation in the field of information protection and cybersecurity. This assessment is used by the Bank to ensure timely monitoring of the implementation and effectiveness of the ISMS, to identify opportunities for improvement and the need for remedial actions.

Also, the Bank is obliged to conduct an annual self-assessment of information security / cybersecurity by compiling an annual report on information security / cyber risk assessment, taking into account the results of:

1) information security / cyber security risk assessment;

2) evaluation of the effectiveness of information security and the effectiveness of ISMS;

3) external audit of information security;

4) internal audit of information security / cybersecurity.

Responsible for compiling the Report is the Bank’s division responsible for information security.

2.2.9. Information security awareness and training

To increase third party representatives’ and employees’ information security awareness and responsibility, a relevant training program is in place at the Bank. The program is aimed at ensuring that all employees who have access to banking information and information systems understand the need to protect such information and accept the responsibility they bear. Moreover, the program is intended to clarify the general information security principles to be observed by all employees and develop information security awareness.

2.2.10. Proper use of information

The Bank’s employees are responsible for the proper use of banking information and information systems, in accordance with the existing information security policies, procedures, standards, instructions, regulations, and guidelines, to ensure that business objects and requirements are met.

2.2.11. Business continuity

With a view to ensuring business continuity and mitigating potential losses resulting from emergencies (such as natural disasters, system failures, etc.), the Bank develops and applies business continuity plans and disaster recovery plans. The Bank Management is responsible for taking appropriate action to guarantee business continuity in line with business requirements.

2.2.12. Human resource management

Information security objectives can be achieved by incorporating specific provisions into human resource agreements, implementing appropriate measures in the new employee hiring process, allocating responsibilities, and maintaining a permanent information security training process for staff. Information security trainings for staff must be conducted at least once per year and upon any revision of the Information Security Policy and when important amendments are made to this Policy or other policies and/or procedures accompanying the Bank's information security system.

The Information Security Policy of the Bank applies to all Bank units and companies that access, process, or use banking information in their operations. Any failures to comply with the Information Security Policy are investigated, and disciplinary action may be taken where any violations are revealed.

2.2.13. Access control

Owners of information and information systems are responsible for designating persons to be granted access to information and information systems, considering business requirements and user roles. Access rights are updated and reviewed subject to business requirements. The granting, modification, cancellation, blocking, and temporary transfer of the rights of access to information and information systems are governed by regulations drafted by the Bank.

2.2.14. System security monitoring

The level of security of critical information assets is regularly monitored using available technical tools, in accordance with the system audit schedule, to maintain the system security. The findings of critical system audits are provided to the Bank Management.

2.2.15. Risk assessment

Risks must be assessed regularly to identify threats and vulnerabilities, determine a risk level acceptable for the Bank, and select appropriate protection tools and administrative and technical controls to manage risks.

2.2.16. Information security requirements

The Bank's information security requirements are developed and implemented based on the information security objectives and the results of the regular risk assessment process. Compliance with information security requirements is mandatory in implementing a new information system, service, function, or project within the Bank.

2.2.17. Information security incident processing

Administrative and technical security controls relating to information security incidents of the Bank must effectively identify and process such incidents, if any. Information system users must be informed of existing information security requirements and notify respective units without delay if they become aware of such incidents. With regard to receiving information about a potential information security incident, an incident may be prevented or identified, analyzed, and processed.

2.2.18. Information security in acquiring, developing, and supporting information systems and applications

Information security must be given priority in acquiring and/or developing and supporting information systems. Information systems designed and/or developed and interacting with other information systems must comply with information security policies, procedures, standards, instructions, regulations, and guidelines approved by the Bank.

2.2.19. Physical security

The Bank's buildings where important hardware is kept (data processing centers, network equipment, server rooms, etc.) and critical premises are subject to proper physical protection, in accordance with the physical security requirements applicable in the Bank. Physical access to such premises is granted only to authorized staff.

2.2.20. External relations management

External relations management at the Bank meets established security standards and is implemented in line with the approved information security policies, procedures, standards, instructions, regulations, and guidelines.

2.2.21. Business partner relations management

Information systems of the Bank may be connected to third-party information systems and/or networks to enable quick troubleshooting or satisfy other business requirements. Where applicable, proper information security measures are implemented for such connections to protect banking information and control third-party actions.

2.2.22. Third-party access to the Bank's information systems

Third parties are granted access to the Bank's information systems and/or banking information and electronic services subject to the following conditions:

- Agreements that serve as a legal basis for the cooperation and a non-disclosure agreement are concluded;
- Necessary and sufficient information security requirements and controls are clearly stated;
- It is technically feasible to grant access;

Only authorized users may be granted access to banking information if all necessary controls are available.

2.2.23. Least privilege

Privileges and access rights for any activity in the information system of the Bank are granted in accordance with the principle of least privilege; in particular, users' privileges and access rights in the information system of the Bank are limited to the minimum scope necessary to perform their tasks in a quality manner.

3. Information Security Policy review

The Information Security Policy is reviewed as needed and at least once a year. An unscheduled review of the Information Security Policy is possible if the information infrastructure is modified and/or new information technology is implemented, as well as upon any changes of legal, regulatory, and other rules.

This Policy must be reviewed and adopted in the case of any changes in the laws of Ukraine, regulations of the National Bank of Ukraine, and international requirements.

4. Acquaintance with the requirements of the Policy

Requirments of the Policy are posted on the corporate portal to ensure acquaintance of the Bank"s staff and third party representatives who have access to the Bank's information and information systems/ structure with the Policy.

When updating the content of the Policy, the document must be updated on the Bank's corporate portal.

The ISMS management body is responsible for determining the scope of rules and Policy requirments that is published on the Bank's corporate portal.

The Information Security Policy must be brought to notice of the Bank's personnel and third party representatives who have access to the Bank's information and information systems during employment (before receiving access to information or information systems for third party representatives) and sign a non-disclosure agreement.