Joint-Stock Company Commercial Bank "PrivatBank"

APPROVED
by the Management Board decision
minutes No. 72 dated 04.10.2024
Chairman of the MB, Gerhard Boesch

Information Security Policy

Registration number: 2024/7575090
Document classification: Unrestricted
Approval data:

decision of the Bank's Management Board, minutes No. 52 dated 19.07.2023;
decision of the Bank's Management Board, minutes No. 58 dated 26.08.2022;
decision of the Bank's Management Board, minutes No. 23 dated 18.05.2021;
decision of the Bank's Management Board, minutes No. 34 dated 13.08.2019;
decision of the Bank's Management Board, minutes No. 32 dated 07.08.2018;

Kyiv

Information security policy

TABLE OF CONTENTS

1. INTRODUCTION

1.1. The information security policy was developed in accordance with the internal regulatory documents of the Bank, the requirements of the current legislation of Ukraine, including the regulatory legal acts of the National Bank of Ukraine, in particular:

- The NBU Board Resolution dated 28.09.2017 No. 95 "On approval of the Regulation on the organization of measures to ensure information security in the banking system of Ukraine";
- The NBU Board Resolution dated 12.08.2022 No. 178 "On approval of the Regulation on the organization of cyber protection in the banking system of Ukraine and amendments to the Regulation on the identification of critical infrastructure objects in the banking system of Ukraine";
- The Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine";
- The Law of Ukraine "On Banks and Banking";
- The Law of Ukraine "On Protection of Personal Data";
- The Law of Ukraine "On Cloud Services";
- SSU ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) "Information security, cyber security and privacy protection. The information security management systems. Requirements";
- SSU ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) "Information security, cyber security and privacy protection. The means of information security controlling";
- The Charter of JSC CB "PrivatBank",

and taking into account international standards on issues of information security, cybersecurity and information security in cloud environments, principles of ensuring information security and cyber protection accepted in international practice.

1.2. The information security policy is the top-level document in the information security management system. The components of the information security management process that are not specified in the Policy are presented in other internal regulatory documents of the Bank (procedures, etc.).

2. TERMS AND ABBREVIATIONS

2.1. The terms and abbreviations used in this document have the following meanings:

- **Bank** - JOINT STOCK COMPANY COMMERCIAL BANK “PRIVATBANK” (JSC CB “PRIVATBANK”).
- **Confidentiality** - a property of information that cannot be obtained by an unauthorized user and/or process.
- **Integrity** - a property of information that cannot be modified by an unauthorized user and/or process.
- **Availability** - a property of accessibility and possibility of using information at the request of an authorized object.
- **Observability** - a property of a system that allows recording the activity of users and processes, the use of passive objects, and also unambiguously establishing the identifiers of users and processes involved in certain events in order to prevent violation of security policy and/or ensure responsibility for certain actions.
- **Policy** — Information security policy.

- **Risk** - a probability of losses or additional losses or loss of income, or failure of a party to fulfill contractual obligations due to the influence of negative internal and external factors;
- **Information security risk (a component of operational risk)** — a probability of losses or additional losses or failure to receive planned income due to a breach of confidentiality, integrity, or availability of data in the bank's information systems, deficiencies or errors in the organization of internal processes, or the occurrence of external events, including cyberattacks or inadequate physical security. Information security risk includes cyber risk;
- **ISMS** - information security management system.
- **Information security** - a multi-level complex of organizational measures of the Bank, software and technical means that ensure the protection of information from accidental and intentional threats, as a result of which the availability, integrity, confidentiality of information may be violated, as well as that ensure the continuity of business processes, reduction of operational risks and optimization of bank costs.
- **Information security incident (IS incident)** - an occurrence of one or more unwanted or unexpected information security events, that are associated with the occurrence or significant probability of negative consequences for information security, information, information assets, business processes or cause damage to the Bank and the protection system.
- **Cybersecurity incident (cyber incident)** - an event or a series of unfavorable events of an unintentional nature (natural, technical, technological, erroneous, including as a result of the human factor) and/or having signs of a possible (potential) cyberattack, posing a threat to the security of electronic communications systems, process control systems, creating the possibility of disruption of the normal functioning of such systems (including disruption and/or blocking of the system, and/or unauthorized management of its resources), threatening the security (protection) of electronic information resources.
- **Information resource** - a set of human, hardware and software resources in the Bank's information systems and processes.
- **Restricted access information (RAI)** - information that constitutes a banking secret, a commercial secret, an insurance secret, personal data and other confidential information of the Bank. Information classified as a banking secret, commercial secret, insurance secret, personal data, confidential information is defined in the "Regulation on the classification of information".
- **Critical (key) process of the Bank's activity** - a process, the absence of effective management and control over which poses a threat to the Bank's activities and/or will not allow the Bank to achieve its goals.
- **Cybersecurity** - protection of vital interests of individuals and citizens, society and the state when using cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace.
- **Minimum level of authority** – powers and access rights that are minimally necessary for the Bank's employees to perform their job responsibilities efficiently.

Other terms used in the Policy are used in the meanings defined by the laws of Ukraine, regulations of the National Bank and SSU EN ISO/IEC 27000:2022.

3. DOCUMENT PURPOSE

3.1. The purpose of the Policy is the implementation and effective functioning of the

information security management system, that ensures:

- protection of the Bank's information resources (including those located in the cloud environment) from real and potential external and internal threats, including those related to intentional and unintentional actions of bank employees;
- continuous operation of the Bank;
- reduction of the risks of the Bank's operational activities;
- maintenance of good business reputation and business corporate culture of the Bank.

4. SCOPE OF APPLICABILITY

4.1. The Policy is applicable to all areas of the Bank.

5. ORGANIZATIONAL STRUCTURE OF THE INFORMATION SECURITY MANAGEMENT PROCESS

5.1 The Bank uses a risk-oriented approach to ensure information security/cybersecurity and a process-based approach to its activities. The Bank has implemented a three-level model of risk management with the division of responsibilities between units in accordance with the following:

- **the first line** - the business units and support units, that are the owners of all operational risks arising in the area of their responsibility;
- **the second line** - the Operational Risk Management Department, that coordinates the operational risk management system as a whole, the Compliance Division, that ensures compliance with legislation and the Bank's internal regulations;
- **the third line of defense** - the internal audit, that evaluates the effectiveness of the operational risk management system by units of the first and second levels of defense, including an evaluation of the effectiveness of the internal control system.

According to the organizational structure of the Risk Management System, the information security unit belongs to the first line of defense. As part of the risk management system, the information security unit is responsible for information security risks/cyber risks (hereinafter referred to as “IS risks”) and reports to the ISMS Governing Body on the current state of managing such risks and the Information Security Management System as a whole.

5.2 During the annual revision of the Information Security Policy, the Bank determines the stakeholders of the ISMS, their roles, responsibilities and takes into account their requirements.

5.2.1 The organizational structure of the information security management system consists of (internal stakeholders):

Supervisory Board:

1. Approves the internal regulation that regulates the activities of the information security unit;
2. Considers the reports of the Technologies, Data and Innovations Committee on information security issues.
3. Approves the Bank's Business Continuity Plan, as well as the Business Continuity Management Policy

Technologies, Data and Innovations Committee of the Supervisory Board:

1. Assists the Supervisory Board in the implementation of its powers to determine the Bank's approaches to information security and data protection.

2. Provides support for technical aspects of information security (cyber security, fraud, etc.), data protection (including personal data).

3. Provides advice and recommendations to the Risk Committee of the Supervisory Board on technological risks, including information security (cyber security, fraud, etc.), IT risk management, data protection (including personal data).

4. Evaluates on an ongoing basis and reports on performance to the Supervisory Board at least once a year.

Management Board:

1. Ensures the implementation and functioning of the ISMS in accordance with the regulations of the National Bank of Ukraine.
2. Ensures the security of the Bank's information systems and systems used to store customers' assets.
3. Defines the list of information that constitutes a commercial secret and confidential information about the Bank's activities, and the procedure for their use and protection.

Operational Risk and Information Security Committee

The Bank has a collective management body created to ensure the comprehensiveness and effectiveness of operational and information risk management processes, the implementation and operation of internal control systems and information security management, and the management of risks arising in the process of relationships with non-banking institutions.

Operational Risk and Information Security Committee:

1. Approves and revises information security policies, regulations on applicability and strategies for the development of the Bank's information security;
2. Coordinates the implementation of new projects, directions, strategic tasks on the Bank's information security issues and information security measures;
3. Considers, approves and monitors the implementation of projects related to the development, implementation, operation, monitoring, revision, maintenance and improvement of the Bank's ISMS;
4. Determines the necessary optimal resources for the implementation of information security measures;
5. Organizes practical measures to raise awareness/train the Bank's staff on information security issues;
6. Ensures timely monitoring of the state of implementation and effectiveness of the Bank's ISMS with further assessment of improvement opportunities and the need for corrective actions.

Technological and Architectural Committee

1. Ensures implementation of the Bank's information technology development strategy.

2. Approves the Bank's internal documents relating to the technical, technological and operational aspects of information technologies determines their functioning and interaction.

3. Approves technical tasks for the purchase/development of information services and technologies.

Information Security Officer:

1. Provides strategic management of the Bank's information security.

2. Determines directions for the development of the Bank's information security, their compliance with the Bank's development strategy.

3. Makes decisions on making changes to the IS development strategy as part of its planned review, or unplanned, due to significant changes that affect the state activity or the Bank's activities.

4. Ensures compliance of information security measures with the needs of business processes/banking products.

5. Monitors the implementation of information security measures in the Bank.

6. Raises issues regarding the application of corrective actions to violators of information security requirements.

7. Ensures the implementation of measures to review and maintain the list of critical information infrastructure objects in an up-to-date state, providing an up-to-date list of critical information infrastructure objects to the National Bank of Ukraine.

8. Ensures implementation of measures to review and update information on objects of critical information infrastructure, providing up-to-date information to the National Bank of Ukraine.

9. Ensures the Bank's participation in information exchange with the National Bank of Ukraine and other banks of Ukraine.

10. Ensures priority implementation of cyber protection measures for the Bank's critical information infrastructure in accordance with the developed Response Plan in the event of a cyber attack (attempt to implement a cyber threat) on the Bank's cyber protection facilities.

11. Ensures the provision of information on the outsourcing of the Bank's cyber protection function at the request of the National Bank of Ukraine in the amount and within the time limit set in such request.

12. Ensures the creation of conditions for improving the skills of employees of the cyber security unit (Information Security Division), training Bank employees in digital skills, cyber awareness of modern cyber threats and counteraction to them.

Information Security Division:

1. Ensures the functioning of the information security management system in accordance with the requirements of current legislation, the National Bank of Ukraine, international payment systems, other counterparties of the Bank, regulatory bodies, PCI DSS standards, 3D Security, etc.

2. Manages information security risks/cyber risks of the Bank.

3. Develops, updates and tests business continuity plans for the Bank's business processes and information systems.

4. Manages the role model and access to the Bank's information resources.

5. Monitors the implementation of measures to ensure information security at all stages of the life cycle of the Bank's information systems.

6. Provides organizational and technical protection of information.

7. Manages information security vulnerabilities and incidents/cyber incidents.

8. Controls the leakage of RAI.

9. Develops or participates in the development of the Bank's documents on information security and cyber protection.

10. Supports the stable operation of software and technical complexes of the Bank's key certification center.

11. Ensures the provision of data on internal information security events (incidents)/cyber incidents to the Operational Risk Management Department.

Other units involved in the information security management process

IT units:

1. Cooperate with the Information Security Department on issues of IS risk assessment when implementing new projects.

2. Ensure the elimination of vulnerabilities in information systems that have been identified by the Information Security Division.

3. Ensure compliance with IS requirements during the development, modernization and acquisition of information resources.

4. Provide secure configuration of server operating systems, databases and network equipment.

5. Ensure the proper use of cloud technologies in order to maintain the confidentiality, integrity and availability of information that circulates in the cloud environment.

HR and Corporate Governance Directorate

1. Ensuring a high level of personnel security and reliability of employees with the aim of general optimization of activities.

2. Identification of personnel risks of candidates and bank employees based on verification of past events or actions and abuses.

Security Service Division

1. Ensures the conduct of internal official investigations, with the aim of confirming facts of violation of information security requirements;

2. Considers the implementation of measures to protect the Bank's information resources from external and internal threats;

3. Counteracts cybercrime and telephone fraud, provides a high level of protection for electronic payments and services;

4. Ensures the protection of electronic payment instruments in international payment systems;

Personal Data Protection Sub-department

1. Ensures the organization and control over compliance with the norms of the current legislation of Ukraine on the protection of personal data in the Bank;

2. Conducts training and consulting of Bank employees on compliance with legislation

on the protection of personal data;

3. Develops internal regulatory documents of the Bank (standards, policies, administrative documents) on the protection of personal data;

4. Analyzes security threats to personal data.

Operational Risk Management Department:

1. Develops, implements and ensures continuous development of the operational risk management system;

2. Assesses the Bank's operational risk.

3. Monitors the development of the Business Continuity Plan

4. Develops in cooperation with units of the first line of defense, a list of specifications of key indicators of operational and information security/cyber risk.

5. Ensures timely identification and prevention of operational and information security/cyber risk events.

Compliance Division:

1. Ensures the organization of control over the protection of personal data in accordance with the legislation of Ukraine;

2. Ensures the organization of control over the Bank's compliance with legislation, internal bank documents, including procedures, and relevant standards of professional associations, market standards, the effect of which extends to the Bank;

3. Ensures monitoring of changes in legislation and relevant standards of professional associations that apply to the Bank, and assessment of the impact of such changes on the processes and procedures introduced in the Bank, and ensures communication and control over the implementation of relevant changes in internal banking documents;

Business Legal Support Division:

1. Provides legal support and adjusts the level of measures taken against violators of information security requirements.

2. In accordance with the procedure established by the Bank, approves the drafts of the Bank's internal regulations on information security and checks their compliance with the Bank's statutory documents and current legislation.

Judicial Defense and General Support Division:

1. Provides legal support for the Bank’s activities for the correct interpretation of legislation in order to comply with information security requirements;

5.2.2 External stakeholders:

Verkhovna Rada of Ukraine:

1. Adopts new legislative acts that affect the further work of the banking system and the need to make changes to the ISMS.

Cabinet of Ministers of Ukraine (as the supreme body of the Bank):

1. Determines the main (strategic) directions of the Bank's activity;

2. Approves the Bank's development strategy;

3. Amends the Charter of the Bank;
4. Appoints and terminates the powers of members of the Supervisory Board.

Government agencies (Ministry of Finance, SSSCP, SSU and other government bodies):

1. Determine the conditions of the Bank's functioning as an object of critical infrastructure of Ukraine;
2. Promotes improved protection of information resources and participation in IT/IS coordination centers.

National Bank of Ukraine:

1. Determines the working conditions of banking systems;
2. Sets forth requirements for IT and IS architecture;
3. Introduces new or makes changes to current NBU information systems;
4. Checks the status of implementation of the bank's ISMS and the completeness of information security measures.

Cloud service providers:

1. Provide cloud services in accordance with the defined level of information security/cyber security;

Criminal structures, computer criminals, hackers, fraudsters:

1. Seek to disclose/steal RAI using technical or software means, human factor, and making attempts to have a negative impact on the Bank's reputation;
2. Incite/involve Bank employees for the purpose of obtaining their own benefit and facilitate the commission of illegal actions.

Competitors:

1. Contribute/stimulate the search and creation of new competitive solutions/products, improvement of existing processes and increase of attractiveness on the market.

Customers:

1. The experience of using products by customers helps to determine the further development of the ISMS, the implementation of information security measures.

States-aggressors, states-sponsors of terrorism (hostile countries):

1. Countries such as the Russian Federation, the Republic of Belarus and other countries that support them in armed aggression against Ukraine influence the development of ISMS through the deployment of information warfare in cyberspace, as well as military actions and acts of terrorism on the territory of Ukraine;
2. Act as sponsors of criminal structures, computer criminals and hackers.

6. APPROACHES TO INFORMATION SECURITY MANAGEMENT

6.1. Approaches to determining the ISMS objectives

The objectives of information security are defined in order to maintain proper protection of information (first of all, RAI) and ensure its integrity, confidentiality, availability and observability.

The objectives of information security are expressed in the form of characteristics and parameters, for the achievement of which information security measures are implemented and qualitative and quantitative indicators are established in the internal control system of the ISMS processes.

Sources for the formation of information security objectives are external and internal factors that determine the Bank's activities, namely:

- laws of Ukraine;
- information security standards;
- regulatory legal acts of the National Bank of Ukraine;
- rules of payment systems and money transfer systems where the Bank is a participant
- agreements with third parties;
- results of risk assessment, that take into account the general business strategy and goals of the Bank's activity;
- internal regulatory documents of the Bank, that regulate the principles of information exchange and processing in accordance with business needs.

Information security objectives are approved by a separate section in the Bank's internal regulatory document on ISMS management.

6.2. Information security risk management

When managing information security risks, the Bank is guided by the main principles of the Bank's risk management system:

1. Adherence to the three-level model of risk management.
2. Creation and implementation of an information security risk management procedure in order to effectively manage information security risk/cyber risk.
3. Ensuring timely detection of information security threats and elimination of information security risks.
4. Identification and consideration of risk factors that threaten the availability, integrity, and confidentiality of information in the Bank.
5. Ensuring the Bank's employees are aware of information security risks.

6.3. Information security incidents management

1. Detection and recording of IS events in the most effective way, confirmation of their classification as IS incidents/cyber incidents;
2. Consistent assessment and continuous response to identified IS incidents/cyber incidents in the most favorable and effective manner;
3. Application of an effective incident management system to minimize adverse consequences for the Bank;
4. Use of timely notification of persons responsible for information security about information security incidents/cyber incidents through the escalation process;
5. Implementation of monitoring, assessment and elimination of IS vulnerabilities to reduce the number of incidents;
6. Rapid extraction of experience based on the results of IS incident management.

6.4. Approaches to IS management and monitoring

An effective combination of technical and organizational solutions is used to manage

information security in the Bank, which allows for high-quality monitoring of the ISMS status.

1. Technical solutions are a set of means for collecting information about the state of elements of information systems, as well as means of influencing their behavior. In particular, malware monitoring tools, as well as security event and incident management systems (SIEM).

2. Organizational solutions are used in the form of establishing human (employee) interaction processes aimed at ensuring the necessary level of monitoring of IT systems and IS subsystems. This enables the formation of incident response teams consisting of experts of different levels and necessitates the creation of a Security Operation Center.

7. PRINCIPLES AND REQUIREMENTS OF INFORMATION SECURITY

7.1. The main principle of information security is to maintain adequate protection of information (primarily RAI) while ensuring its integrity, confidentiality, availability and observability.

7.2. The principles of ensuring information security are:

- a systemic (complex) approach to ensuring the Bank's information security;
- continuity of the process of improvement and development of information security and its implementation through the substantiation and implementation of rational means, methods, and measures using international experience;
- timeliness and adequacy of protection measures against real and potential threats to the Bank's information security;
- control and support of the appropriate level of information security by bank managers;
- provision of sufficient resources, including financial ones, for the sustainable development of information security systems.

7.3. The Bank's information security department reports directly to the person responsible for the Bank's information security (ISO).

7.4. The management of the Bank fully supports the implementation of information security and ensures its financing at a sufficient level.

7.5. Information security/cyber protection documents are developed by the information security unit and other units in the relevant areas of activity. Permanent control of the implementation, execution, improvement and maintenance of the Policy in an up-to-date state is entrusted to the information security unit.

7.6. The Bank develops internal documents that define, in particular:

- requirements regarding the use, provision, cancellation and control of access to the Bank's information systems;
- requirements for information security when using removable media;
- requirements for ensuring protection against malicious code and organization of protection against malicious code;
- use of cryptographic means to protect information;
- key management process;
- update management process;
- requirements for information security, technical maintenance, operation of fax machines, multifunctional devices, telephones and/or telephone systems;

- requirements for the use of corporate e-mail;
- requirements for the selection, application or modernization of software and hardware information processing tools or in the case of acquisition, as well as the procedure for decommissioning the Bank's information systems equipment;
- requirements for the information security incident management process.

7.7. The Bank applies the principle of providing a minimum level of authority when providing access to the Bank's information systems (including access of privileged users).

7.8. In the Bank’s information systems that directly ensure the automation of banking activities, it is prohibited to combine within one function (role) the following powers: development and maintenance (administration), development and operation, maintenance (administration) and operation, execution of operations in such systems and further control over their execution.

7.9. The Bank uses the standards, documents and guidelines of the Open web application security project (OWASP) to develop secure applications.

7.10 When implementing and developing software, the Bank is guided by security principles and approaches in compliance with S-SDLC methods.

7.11. Information security requirements must be taken into account during the development, implementation and operation of software and technical complexes.

7.12. Public services of the bank and internal networks of the bank must meet the requirements of information security standards.

7.13. The Bank ensures compliance with information security requirements contained in agreements with third parties regarding participation in international payment systems and money transfer systems.

7.14. The Bank maintains a high level of information security, which is processed, stored and transmitted using cloud data storage technologies.

7.15. The Bank has developed and approved a plan for ensuring the continuity of the Bank's activities, which takes into account the continuity of the operation of information security measures as part of the process of managing the continuity of the Bank's activities.

7.16. The strategy for the development of information technologies, projects related to information technologies are consistent with the Policy.

7.17. The responsibility of the Bank's structural units in terms of information security is determined by the Bank's internal documents.

7.18. Each employee of the bank during the performance of his/her official duties and powers must ensure compliance with the Bank's information security requirements. Bank employees are responsible for non-compliance with information security requirements established by the Bank's internal documents and current legislation.

7.19. The Bank supports a program to raise awareness/train bank employees on information security/cyber protection, taking into account the experience gained from resolving information security incidents.

7.20. The content of the Policy is brought to the attention of all bank personnel and, if necessary, representatives of third parties. The Bank is obliged to familiarize employees with the Policy upon hiring. Each employee of the Bank is obliged to familiarize themselves with the Policy by signature and provide an obligation to maintain confidentiality.

7.21. The Bank implements measures to comply with the legislation on the protection of personal data, as well as the contractual conditions agreed with partners, contractors and relevant third parties. The Bank acknowledges its responsibility for the protection of privacy and

confidentiality of personal data, as well as for ensuring the safe processing and storage of such data.

8. REPORTING

8.1. The Information Security Division submits a report on the assessment of the impact of information systems on the Bank's activities to the management body of the ISMS, once a year.

8.2. Reports on monitoring the effectiveness of ISMS implementation are submitted to the ISMS governing body for review once a quarter.

8.3. Reports on the state of implementation of the information security management system, monitoring of the achievement of information security goals, analysis of changes in external and internal environmental factors that are important for the operation of ISMS, consideration of opportunities for continuous improvement and the need for changes to the information security management system, reports on the state of processes ensuring the continuity of the Bank's activities and managing information security risks are submitted to the Operational Risk and Information Security Committee once every six months.

8.4. The Information Security Division provides a final monthly report to the person responsible for information security in the Bank (ISO) regarding the implemented measures to ensure information security in the Bank.

9. DOCUMENT REVIEW

9.1. The Policy shall be approved by the Bank's Management Board.

9.2 The Policy shall be kept up to date and reviewed at least once a year. If, as a result of the review, no changes are made to the Policy, then its re-approval is not required.

9.3. The grounds for making changes to the Policy are changes in the information infrastructure and/or the introduction of new information technologies, changes in legislation, information security standards and other regulations, or when significant changes occur.

9.4. Changes and additions to the Policy shall be concurred by the ISMS management body and approved by the Bank's Management Board.