*/Logo: PrivatBank/*

**Joint-Stock Company Commercial Bank PrivatBank**

**APPROVED BY**
**Decision of the Bank's Management Board**
**Minutes No. 52 dated July 19, 2023**
**Chairperson of the meeting Gerhard Boesch**
*/Siganture/*
*/Round seal: JOINT-STOCK COMPANY COMMERCIAL BANK PRIVATBANK * JOINT-STOCK COMPANY COMMERCIAL BANK PRIVATBANK * UKRAINE * Code 14360570 *JSB PRIVATBANK/*

# Information Security Policy

**Registration No.:** 2023/7161258
**Document type:** open
**Approval data:**

Decision of the Bank's Management Board, Minutes No. 58 dated August 26, 2022;
Decision of the Bank's Management Board, Minutes No. 23 dated May 18, 2021;
Decision of the Bank's Management Board, Minutes No. 34 dated August 13, 2019;
Decision of the Bank's Management Board, Minutes No. 32 dated August 7, 2018;
Order No. PR/18-2016-6601636 dated February 25, 2016;
Order No. PR/18-2016-6520391 dated January 18, 2016;
Order No. СП-2015-6638173 (6650881) dated April 14, 2015

The city of Kyiv

**TABLE OF CONTENTS**

## 1. INTRODUCTION

1.1. The Information Security Policy is developed in accordance with the Bank's internal regulations, the applicable laws of Ukraine, including regulations of the National Bank of Ukraine, namely:

- Resolution of the Management Board of the National Bank of Ukraine No. 95 dated September 28, 2017 "On Approval of the Regulation on Organization of Measures for Ensuring Information Security in the Banking System of Ukraine";
- Resolution of the Management Board of the National Bank of Ukraine No. 178 dated August 12, 2022 "On Approval of the Regulation on the Organization of Cyber Defense in the Banking System of Ukraine and Making Amendments to the Regulation on the Definition of Critical Infrastructure Objects in the Banking System of Ukraine";
- The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine";
- The Law of Ukraine "On Banks and Banking";
- The Law of Ukraine "On Personal Data Protection";
- DSTU ISO/IEC 27001:2015. Information technology. Security techniques. Information security management systems. Requirements";
- DSTU ISO/IEC 27002:2015. Information technology. Security techniques. Code of practice for information security controls;
- Charter of JSC CB PrivatBank,

and subject to internationalstandards of information security, cybersecurity, and information security in cloud environments, and generally accepted international principles of information security and cybersecurity.

1.2. The Information Security Policy is a top-tier document in the information security management system. The components of the security management process that are not specified in the Policy are described in other internal regulatory documents of the Bank (regulations, procedures, etc.).

## 2. DEFINITIONS AND ABBREVIATIONS

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

- **"Bank"** means JOINT STOCK COMPANY COMMERCIAL BANK PRIVATBANK (JSC CB PRIVATBANK).
- **"Confidentiality"** means a property of information implying that the information cannot be accessed by an unauthorized user and/or process.
- **"Integrity"** means a property of information implying that the information cannot be modified by an unauthorized user and/or process.
- **"Accessibility"** means a property implying that the information is accessible and can be used at the request of an authorized entity.
- **"Observability"** means a system property that makes it possible to record the activities of users and processes and the use of passive entities, and to uniquely identify the users and processes involved in certain events in order to prevent violations of the security policy and/or ensure responsibility for certain actions.
- **"Policy"** means this Information Security Policy.

- **"Risk"** means the probability of damages or additional losses or a shortfall in income, or failure to fulfill contractual obligations by a party as a result of adverse internal or external factors;
- **"Information Security Risk" (a component of operational risk** ) means the probability of damages or additional losses, or a shortfall in planned income as a result of a breach of confidentiality, integrity, or availability of data in the bank's information systems, defects 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"** means information security management system.
- **"Information Security"** means a multi-tier complex of organizational measures, software, and hardware intended to protect information from accidental and intentional threats that may result in a breach of accessibility, integrity, or confidentiality of information, as well as to ensure the continuity of business processes, mitigate operational risks, and optimize the bank's costs.
- **"Information Security Incident (IS Incident)"** means the occurrence of one or more undesirable or unexpected information security events that are associated with the occurrence or a substantial probability of negative consequences for information security, information, information assets, business processes, or damage to the Bank and the security system.
- **"Information Resource"** means a set of human, hardware, and software resources in the Bank's information systems and processes.
- **"Restricted Information (RI)"** means information that constitutes a banking secrecy, trade secret, personal data, and other confidential information of the Bank. Information classified as a banking secrecy, trade secret, personal data, or confidential information is defined in the Regulation on the Information Classifier.
- **"Critical (Key) Process of the Bank's Activities"** means a process, which, in the absence of effective management and control, threatens the Bank's activities and/or prevents the Bank from achieving its objectives.
- **"Minimum Level of Authority"** means the minimum authority and access rights required for the Bank's employees to perform their duties efficiently.

Other terms used in the Policy shall have the meanings defined by the laws of Ukraine, the regulations of the National Bank of Ukraine and DSTU ISO/IEC 27000:2015.

## 3. PURPOSE OF THE DOCUMENT

3.1. The purpose of this Policy is to implement and effectively operate an 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 the Bank's employees;
- continuous operation of the Bank;

- mitigation of the risks of the Bank's operating activities;
- maintaining the Bank's good business reputation and corporate culture.

## 4. SCOPE OF APPLICATION

4.1. This Policy applies to the entire Bank.

## 5. ORGANIZATIONAL STRUCTURE OF THE INFORMATION SECURITY MANAGEMENT PROCESS

5.1 The Bank uses a risk-oriented approach to information security and a process-based approach to its operations. The Bank has implemented a three-tiered risk management model with responsibilities divided between its departments as follows:

- First line – business and support units, which own all operational risks arising within their area of responsibility;
- Second line – the Operational Risk Management Department, which coordinates the overall operational risk management system, and the Compliance Division, which ensures compliance with the laws and the Bank's internal regulations;
- Third line of protection – internal audit, which assesses the effectiveness of the operational risk management system by the units of the first and second security levels, including the effectiveness of the internal control system.

According to the organizational structure of the Risk Management System, the information security unit is the first line of protection. As part of the risk management system, the information security unit is responsible for IS risks and reports to the Governing Body on the current state of management of such risks and the overall Information Security Management System.

5.2 During the annual review of the ISMS, the Bank identifies the ISMS stakeholders, their roles and responsibilities, and takes into account their requirements.

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

**Supervisory Board:**

1. Approves internal regulations governing the activities of the information security unit;
2. Reviews the reports of the Technology, Data and Innovation Committee on information security issues.
3. Approves the Bank's Business Continuity Plan and the Business Continuity Management Policy.

**Technology, Data and Innovation Committee of the Supervisory Board:**

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

2. Provides support for technical aspects of information security (cybersecurity, fraud, etc.) and data protection (including personal data).
3. Provides advice and recommendations to the Risk Committee of the Supervisory Board on process risks, including information security (cybersecurity, fraud, etc.), IT risk management, and data protection (including personal data).
4. Evaluates on an ongoing basis and reports to the Supervisory Board at least once a year on its performance results.

**Management Board:**

1. Ensures the implementation and operation 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 customer assets.
3. Determines the list of information constituting a trade secret and confidential information about the Bank's activities, and the procedure for their use and protection.

**Operational Risk and Information Security Committee (ORISC):**

The Bank has a collective governing body established to ensure the complexity and efficiency of operational and information risk management processes, the implementation and operation of internal control and information security management systems, and management of risks arising from relations with non-banking institutions.

**ORISC**:

1) Approves and reviews information security policies, regulations on the applicability and strategies for the development of the Bank's information security;

2) Coordinates the implementation of new projects, areas, and strategic tasks related to the Bank's information security, as well as information security measures;

3) Reviews, approves, and controls the implementation of projects for the development, implementation, operation, monitoring, review, maintenance, and improvement of the Bank's ISMS;

4) Determines the optimal resources required to implement information security measures;

5) Organizes practical activities to raise awareness / train the Bank's personnel on information security issues;

6) Ensures timely monitoring of the implementation status and efficiency of the Bank's ISMS functioning with a subsequent assessment of improvement possibilities and the need for corrective actions.

**Responsible for information security across the Bank (Chief Information Security Officer):**

1. Provides strategic guidance on the Bank's information security.

2. Determines the areas of the Bank's information security development and their compliance with the Bank's development strategy.
3. Decides on changes to the IS development strategy as part of its scheduled or unscheduled review due to significant changes affecting the government activities or the Bank's operations.
4. Ensures that information security measures meet the needs of business processes / banking products.
5. Supervises the implementation of information security measures across the Bank.
6. Raises issue of applying enforcement measures to violators of information security requirements.
7. Ensures the implementation of measures for reviewing and updating the list of critical IT infrastructure objects and the submission of the updated list of critical IT infrastructure objects to the National Bank of Ukraine.
8. Ensures the implementation of measures for reviewing and updating information on critical IT infrastructure objects and the submission of the updated information to the National Bank of Ukraine.
9. Ensures the Bank's participation in the information exchange with the National Bank of Ukraine and other banks of Ukraine.
10. Ensures priority implementation of cybersecurity measures for the Bank's critical IT infrastructure in accordance with the developed Response Plan in case of a cyberattack (attempted cyberthreat) on the Bank's cybersecurity objects.
11. Ensures provision of information on the outsourcing of the Bank's cybersecurity function at the request of the National Bank of Ukraine in the scope and within the timeframe specified in such request.
12. Ensures the conditions for advanced training of employees of the Cyber Defense Unit (Information Security Division), training of the Bank's employees in digital skills, cyber awareness and counteraction of modern cyber threats.

**Information Security Division:**

1. Ensures the functioning of the information security management system in compliance with the requirements of the applicable laws, the National Bank of Ukraine, international payment systems, other counterparties of the Bank, regulatory authorities, PCI DSS, 3D Security standards, etc.
2. Manages the Bank's information security risks / cyber risks.
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. Controls the implementation of information security measures at all stages of the life cycle of the Bank's information systems.
6. Ensures organizational and technical protection of information.
7. Manages vulnerabilities and information security risks / cyber incidents.

8. Controls the leakage of restricted information.
9. Develops, or participates in the development of, the Bank's information security and cybersecurity documents.
10. Maintains a stable operation of software and hardware systems of the Bank's key certification center.
11. Ensures that data on internal information security events (incidents) / cyber incidents are provided to the Operational Risk Management Department.

**Other units involved in the information security management process**

**IT units:**

1. Collaborate with the Information Security Division on the assessment of security risks that may arise upon the implementation of new projects.
2. Ensure elimination of vulnerabilities in information systems identified by the Information Security Division
3. Ensure compliance with security requirements during the development, modernization, and acquisition of information resources.
4. Ensure secure configuration of server operating systems, databases, and network equipment.
5. Ensure proper use of cloud technologies to maintain confidentiality, integrity, and accessibility of information circulating in the cloud environment.

**HR and Corporate Governance Directorate:**

1. Ensures a high level of HR security and reliability of employees to optimize overall performance.
2. Identifies HR risks of the Bank's applicants and employees based on checks of past events or actions and abuses.

**Security Service Division:**

1. Ensures that internal investigations are conducted to confirm the facts of violation of information security requirements;
2. Considers the implementation of measures for protecting the Bank's information resources against external and internal threats;
3. Counteracts cybercrime and telephone fraud, ensuring 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 and controls compliance with the applicable laws of Ukraine on personal data protection across the Bank;
2. Provides training and consultations to the Bank's employees on compliance with personal data protection laws;
3. Develops the Bank's internal regulatory documents (standards, policies, administrative documents) on personal data protection;

4. Analyzes threats to personal data security.

**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. Controls the development of the Bank's Business Continuity Plan;
4. Develops, together with the first line of defense units, a list of specifications for key indicators of operational and information risks;
5. Ensures timely identification and prevention of operational and information risk events.

**Compliance Division:**

1. Ensures control of personal data protection in accordance with the laws of Ukraine;
2. Ensures and controls the Bank's compliance with the laws, internal banking documents, including procedures, and relevant standards of professional associations whose market standards apply to the Bank;
3. Monitors changes in legislation and relevant standards of professional associations applicable to the Bank, assesses the impact of such changes on the processes and procedures implemented within the Bank, and ensures that the relevant changes are communicated and monitored in the internal banking documents;

**Legal Support Division:**

1. Provides legal support for the Bank's activities to ensure correct interpretation of legislation in order to comply with information security requirements;
2. Provides legal support and adjusts the level of enforcement measures against violators of information security requirements.
3. In accordance with the procedure established by the Bank, approves draft internal regulations of the Bank on information security and verifies their compliance with the Bank's charter documents and applicable laws.

5.2.2 External stakeholders:

**Verkhovna Rada of Ukraine:**

1. Adopts new legislative acts regulating further operation of the banking system and the need to make changes to the ISMS.

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

1. Determines the main (strategic) areas of the Bank's activities;
2. Approves the Bank's development strategy;
3. Amends the Bank's Charter;
4. Appoints and terminates the powers of the Supervisory Board members.

**Government agencies (the Ministry of Finance, the State Special Communications Service, the Security Service of Ukraine, and other government agencies):**

1. Determine the conditions for the Bank's functioning as a critical infrastructure facility of Ukraine;

2. Contribute to better protection of information resources and participation in IT/IS coordination centers.

**National Bank of Ukraine:**

1. Determines the conditions for the operation of banking systems;
2. Sets requirements for IT and IS architecture;
3. Implements new or makes changes to existing information systems of the National Bank of Ukraine;
4. Checks the state of implementation of the Bank's ISMS and the completeness of information security measures.

**Cloud service providers:**

1. Provide cloud services in accordance with a certain level of information security / cybersecurity;

**Criminal organizations, computer criminals, hackers, fraudsters:**

1. Seek to disclose/steal restricted information using technical or software tools, human factors, and attempts to negatively affect the Bank's reputation;
2. Incite/engage the Bank's employees for their own benefit and facilitate the commission of illegal acts.

**Competitors of the organization:**

1. Promote/stimulate the search for and creation of new competitive solutions/products, improvement of existing processes, and improvement of market attractiveness.

**Customers**:

1. The customers' experience of using the products helps determine the ISMS further development and the implementation of information security measures.

**Aggressor states and state sponsor of terrorism (hostile countries):**

1. Such countries as the Russian Federation, the Republic of Belarus and other countries supporting them in their armed aggression against Ukraine impact the ISMS development by deploying information warfare in cyberspace, as well as military operations and acts of terrorism in the territory of Ukraine;
2. They sponsor criminal organizations, computer criminals and hackers.

## 6. APPROACHES TO INFORMATION SECURITY MANAGEMENT

### 6.1. Approaches to defining ISMS objectives

Information security objectives are defined to maintain proper protection of information (primarily restricted information), ensuring its integrity, confidentiality, accessibility, and observability. Information security objectives are expressed in the form of characteristics and parameters, the achievement of which is ensured by implementing information security measures and requires qualitative and quantitative indicators to be set in the internal control system of ISMS processes.

The sources for setting information security objectives are external and internal factors that determine the Bank's activities, namely:

- laws of Ukraine;
- information security standards;
- regulations of the National Bank of Ukraine;
- rules of payment systems and money transfer systems in which the Bank is a member;
- agreements with third parties;
- risk assessment results that take into account the Bank's overall business strategy and performance goals;
- the Bank's internal regulatory documents governing the principles of information exchange and processing in accordance with business needs.

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

### 6.2. Information security risk management

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

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

### 6.3. Information security incident management

1. Detecting and recording IS events in a most efficient way, confirming their classification as IS incidents / cyber incidents;
2. Consistent assessment and continuous response to detected IS incidents / cyber incidents in a most favorable and effective manner;
3. Implementation of an effective incident management system to minimize adverse consequences for the Bank;
4. Notification of information security officers in a timely manner about IS incidents / cyber incidents through an escalation process;
5. Implementation of monitoring, assessment, and elimination of IS vulnerabilities to reduce the number of incidents;
6. Rapid learning from the results of IS incident management.

### 6.4. Approaches to IS management and monitoring

To manage information security, the Bank uses an effective combination of technical and organizational solutions enabling the Bank to ensure high quality monitoring of the ISMS.

1. Technical solutions are a set of tools for collecting information about the state of information system elements, as well as means of influencing their behavior. They include malware monitoring tools, as well as security information and event management systems (SIEM).
2. Organizational solutions are used in the form of establishing processes of interaction between people (employees) aimed at ensuring the required level of monitoring of IT systems and IS subsystems. This makes it possible to create incident response teams consisting of experts of different levels and leads to the establishment of a Security Operation Center.

## 7. PRINCIPLES AND REQUIREMENTS OF INFORMATION SECURITY

7.1. The basic principle of information security is to maintain proper protection of information (primarily restricted information), while ensuring its integrity, confidentiality, accessibility, and observability.

7.2. The principles of information security are:

- a systematic (comprehensive) approach to ensuring the Bank's information security;
- continuity of the IS improvement and development process and its implementation through substantiation and implementation of rational means, methods, and measures using the best international experience;
- timeliness and adequacy of protection measures against real and potential threats to the Bank's information security;
- control and maintenance of an appropriate level of information security by the Bank's management;
- ensuring adequate resources, including financial resources, for a sustainable development of information security systems.

7.3. The Bank's information security unit is directly subordinated to the Bank's Chief Information Security Officer (CISO).

7.4. The Bank's management strongly supports the implementation of information security and ensures that it is sufficiently funded.

7.5. Documents on information security / cybersecurity are developed by the information security unit and other units in the relevant areas of activity. The information security unit is responsible for continuous monitoring of the implementation, fulfillment, improvement, and maintenance of the Policy.

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

- the requirements for the use, provision, cancellation, and control of access to the Bank's information systems;
- the requirements for information security when using removable storage media;
- the requirements for ensuring and organizing protection against malicious code;
- the use of cryptographic tools to protect information;

- the key management process;
- the updates management process;
- the requirements for information security, maintenance, and operation of fax machines, multifunction devices, telephones and/or telephone systems;
- the requirements for the use of corporate e-mail;
- the requirements for the selection, use, modernization, or acquisition of information processing software and hardware, as well as the procedure for decommissioning the equipment of the Bank's information systems;
- the requirements for the information security incident management process.

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

7.8. In the Bank's information systems that directly ensure automation of banking activities, it is prohibited to combine the following powers within the same function (role): development and maintenance (administration), development and operation, maintenance (administration) and operation, execution of operations in such systems and further control of 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. The development, implementation, and operation of software and hardware systems must be subject to information security requirements.

7.11. The Bank's public services and internal networks must meet the requirements of information security standards.

7.12. The Bank ensures compliance with the information security requirements set forth in agreements with third parties concerning the participation in international payment and money transfer systems.

7.13. The Bank maintains a high security of information processed, stored, and transmitted using cloud storage technologies.

7.13. The Bank has developed and approved a business continuity plan, which takes into account the continuity of information security measures as part of the Bank's business continuity management process.

7.14. The IT development strategy and IT-related projects are consistent with the Policy.

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

7.16. In the course of performing their job duties and powers, each employee of the Bank must ensure compliance with the Bank's information security requirements. Bank employees will be held liable for failure to comply with information security requirements established by the Bank's internal documents and applicable laws.

7.17. The Bank maintains a program of awareness raising / training of its employees on information security / cybersecurity, taking into account the experience gained through resolution of information security incidents.

7.18. The contents of this Policy will be notified to all bank personnel and, if necessary , to representatives of third parties. The Bank is obliged to familiarize its employees with this Policy upon their employment. Each employee of the Bank is to familiarize themselves with this Policy against signature and undertake to maintain confidentiality.

7.19. The Bank implements measures to ensure compliance with personal data protection laws and contractual terms agreed upon with its partners, contractors, and relevant third parties. The Bank recognizes its responsibility to protect the privacy and confidentiality of personal data, and to ensure a secure processing and storage of such data.

## 8. REPORTING

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

8.2. Reports on monitoring the achievement of information security objectives and the ISMS effectiveness are submitted to the ISMS governing body for consideration on a quarterly basis.

8.3. Reports on the status of the implementation of the information security management system, monitoring of the achievement of information security goals, the analysis of changes in external and internal environment factors that are important for the ISMS functioning, the consideration of opportunities for continuous improvement and the need to amend the information security management system, and reports on the status of the processes of ensuring the continuity of the Bank's operations and information security risk management are submitted to the Operational Risk and Information Security Management Committee once a year.

8.4. The Information Security Division submits a final monthly report to the Bank's Chief Information Security Officer (CISO) on the measures taken to ensure the Bank's information security.

## 9. DOCUMENT REVISION

9.1. The Policy is approved by the Management Board.

9.2. The Policy will be updated and reviewed at least once a year. If the review of the Policy does not result in any amendments, no re-approval will be required.

9.3. The grounds for amending the Policy include changes in the information infrastructure and/or implementation of new information technologies, changes in legislation, information security standards or other norms, or any significant changes.

9.4. Any amendments or additions to this Policy will be agreed upon with the ISMS governing body and approved by the Management Board.