Reg. No. 04-11/28 **June 4, 2026**	**APPROVED** **by the Supervisory Board of** **ANOR BANK JSC**

Minutes No. 25 dated

May 26, 2026

Chairman of the Supervisory Board

of ANOR BANK JSC

_____

(signature)

Sh. N. Nosirov

INFORMATION SECURITY POLICY

OF JOINT-STOCK COMPANY

“ANOR BANK”

Tashkent - 2026

TABLE OF CONTENTS

Appendix 10 - Internet and Corporate E-mail Usage Rules
Appendix 11 - Information Asset Management Rules
Appendix 12 - Rules for Organizing Technical Information Protection
Appendix 13 - Rules for Organizing Cryptographic Information Protection
Appendix 14 - Business Recovery and Business Continuity Procedure for Emergency Situations
Appendix 15 - Information Security Incident Response Procedure
Appendix 16 - Information Security Policy Acknowledgement Log
Appendix 17 - Information Security Risk Assessment Methodology
Appendix 18 - List of Hardware-Software and Software Solutions Used by the Bank

1. GENERAL PROVISIONS

1.1. Introduction

The Information Security Policy of ANOR BANK Joint-Stock Company (hereinafter referred to as the "Bank") (hereinafter referred to as the "Policy") defines the information security approaches and methods adopted by the Bank's management for the purpose of conducting its activities. It represents a structured set of high-level information protection objectives and tasks that shall guide the Bank in its operations and establishes the fundamental principles for the development of the Bank's Information Security Management System (hereinafter referred to as the "ISMS").

The Bank is a commercial digital bank and places priority on the provision of banking services in an interactive manner through its website and mobile applications (hereinafter referred to as "Digital Banking Services") within the territory of the Republic of Uzbekistan.

To conduct its activities, the Bank effectively implements and utilizes digital technologies on the basis of which the Bank's information and communication infrastructure is established and continuously developed.

Ensuring information security is a priority objective in the context of providing Digital Banking Services and maintaining the reliable and uninterrupted operation of the information and communication infrastructure in order to comply with the requirements of the legislation of the Republic of Uzbekistan in the field of information security.

Information security encompasses any activities aimed at protecting the Bank's information resources and information systems.

The primary objective of this Policy is to reduce information security threats across the Bank's entire information infrastructure in order to enhance the overall resilience of its operations.

Information security is considered from the perspective of ensuring the confidentiality, integrity, and availability of protected confidential information, including commercial and banking secrecy, personal data of the Bank's employees and customers, information relating to the Bank's assets, as well as ensuring the continuous and uninterrupted functioning of information processing activities. The scope of information security includes the Bank's information systems and information resources, including the Automated Banking System (hereinafter referred to as the "ABS").

Information security is achieved through the implementation and enforcement of a comprehensive set of measures, including policies, practices, procedures, and organizational structures.

The information security framework shall ensure the protection of information (data) and the Bank's information and communication infrastructure against a wide range of threats in order to maintain the continuity of Digital Banking Services, minimize damage resulting from the materialization of threats, anticipate

and prevent their impact, preserve the Bank's business reputation, and ensure compliance with applicable legal and regulatory requirements.

This Policy constitutes a set of documented principles, rules, procedures, and practical methods in the field of information security that guide the Bank in the conduct of its activities.

This Policy applies to all structural divisions of the Bank and is mandatory for all employees and officers of the Bank. The provisions of this Policy shall be applied in the development and implementation of the Bank's internal regulatory documents.

1.2. Regulatory Documents Used in the Development of the Policy

The Bank's Information Security Policy has been developed to ensure the information security of information assets in accordance with the following legislative and regulatory acts of the Republic of Uzbekistan:

1) Law of the Republic of Uzbekistan No. 560-II dated December 11, 2003, "On Informatization".

2) Law of the Republic of Uzbekistan No. 530-II dated August 30, 2003, "On Banking Secrecy".

3) Law of the Republic of Uzbekistan No. 611-II dated April 29, 2004, "On Electronic Document Management".

4) Law of the Republic of Uzbekistan No. 30 dated April 4, 2006, "On Information Protection in the Automated Banking System".

5) Law of the Republic of Uzbekistan No. 374 dated September 11, 2014, "On Commercial Secrecy".

6) Law of the Republic of Uzbekistan No. 547 dated July 2, 2019, "On Personal Data".

7) Law of the Republic of Uzbekistan No. 578 dated November 1, 2019, "On Payments and Payment Systems".

8) Law of the Republic of Uzbekistan No. 580 dated November 5, 2019, "On Amendments and Additions to the Law of the Republic of Uzbekistan 'On Banks and Banking Activities'".

9) Law of the Republic of Uzbekistan No. 764 dated April 15, 2022, "On Cybersecurity".

10) Law of the Republic of Uzbekistan No. 792 dated September 29, 2022, "On Electronic Commerce".

11) Law of the Republic of Uzbekistan No. 793 dated October 12, 2022, "On Electronic Digital Signature".

12) Decree of the President of the Republic of Uzbekistan No. UP-6007 dated June 15, 2020, "On Measures for the Introduction of the State System for the Protection of Information Systems and Resources of the Republic of Uzbekistan".

13) Resolution of the President of the Republic of Uzbekistan No. PD-614 dated April 3, 2007, "On Measures for Organizing Cryptographic Protection of Information in the Republic of Uzbekistan".

14) Resolution of the President of the Republic of Uzbekistan No. PD-1572 dated July 8, 2011, “On Measures for the Protection of National Information Resources”.

15) Resolution of the President of the Republic of Uzbekistan No. PD-4024 dated November 21, 2018, “On Measures to Improve the System of Control over the Implementation of Information Technologies and Communications and Ensuring Their Protection”.

16) Resolution of the President of the Republic of Uzbekistan No. PD-4452 dated September 14, 2019, “On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Organizing Their Protection”.

17) Resolution of the President of the Republic of Uzbekistan No. PD-4751 dated June 15, 2020, “On Measures for the Further Improvement of the Cybersecurity Assurance System in the Republic of Uzbekistan”.

18) Resolution of the President of the Republic of Uzbekistan No. PD-5170 dated July 1, 2021, “On Measures to Improve Cybersecurity in the Activities of Payment System Operators, Credit Institutions, and Payment Organizations”.

19) Resolution of the President of the Republic of Uzbekistan No. PD-167 dated May 31, 2023, “On Additional Measures to Improve the Cybersecurity Assurance System for Critical Information Infrastructure Facilities of the Republic of Uzbekistan”.

20) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 137 dated March 26, 1999, “On Approval of the Regulation on the Procedure for the Preparation and Distribution of Information Resources of the Republic of Uzbekistan through Data Transmission Networks, Including the Internet”.

21) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 256 dated November 22, 2005, “On Improving the Regulatory Framework in the Field of Informatization”.

22) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 126 dated May 4, 2011, “On Measures for the Introduction and Use of a Unified Secure Electronic Mail and Electronic Document Management System within the Executive Office of the Cabinet of Ministers, State and Economic Administration Bodies, and Local Government Authorities”.

23) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 296 dated November 7, 2011, “On Measures for the Implementation of Resolution of the President of the Republic of Uzbekistan No. PD-1572 dated July 8, 2011 ‘On Additional Measures for the Protection of National Information Resources’”.

24) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 295 dated October 16, 2015, “On Approval of the Regulation on the Procedure for Organizing and Ensuring the Security of Confidential Information at Information Assets of the Republic of Uzbekistan”.

25) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 365 dated December 17, 2015, “On Measures for the Establishment of Centralized Databases of Individuals and Legal Entities and the Introduction of the

Unified User Identification Information System of the ‘Electronic Government’ System”.

26) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 930 dated November 21, 2019, “On Approval of the List of Facilities Subject to Protection by the Units of the Main Directorate of Security of the National Guard of the Republic of Uzbekistan”.

27) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 570 dated October 5, 2022, “On Approval of Certain Regulatory Legal Acts in the Field of Personal Data Processing”.

28) Resolution of the Board of the Central Bank of the Republic of Uzbekistan “On Approval of the Regulation on Information Security in the Payment Systems of Payment System Operators and Payment Service Providers”, registered by the Ministry of Justice of the Republic of Uzbekistan on February 14, 2006, under No. 1545.

29) Resolution of the Board of the Central Bank of the Republic of Uzbekistan No. 2/4 dated January 25, 2020, “On Approval of the Regulation on Information Protection in Automated Systems of Commercial Banks of the Republic of Uzbekistan”, registered by the Ministry of Justice of the Republic of Uzbekistan on March 10, 2020, under No. 3224 (new edition - No. 3224-2 of 2023).

30) Resolution of the Board of the Central Bank of the Republic of Uzbekistan “On Approval of the Regulation on Information Security in the Payment Systems of Payment System Operators and Payment Service Providers”, registered by the Ministry of Justice of the Republic of Uzbekistan on May 21, 2024, under No. 3531.

31) Order of the Chairman of the State Security Service of the Republic of Uzbekistan No. 91 dated September 4, 2023, “On Approval of the Regulation on the Procedure for Assessing the Level of Cybersecurity Assurance in the Republic of Uzbekistan and the Cybersecurity of Critical Information Infrastructure Facilities”, registered by the Ministry of Justice of the Republic of Uzbekistan on September 22, 2023, under No. 3458.

32) Order of the Ministry of Justice of the Republic of Uzbekistan No. 19-mh dated November 14, 2023, “On Approval of the Standard Procedure for Organizing the Activities of a Structural Unit or Authorized Person Responsible for Personal Data Processing and Protection by the Owner and/or Operator of a Personal Data Database”, registered by the Ministry of Justice of the Republic of Uzbekistan on November 15, 2023, under No. 3477.

33) Order of the Ministry of Justice of the Republic of Uzbekistan No. 20-mh dated November 15, 2023, “On Approval of the Procedure for Personal Data Processing”, registered by the Ministry of Justice of the Republic of Uzbekistan on November 15, 2023, under No. 3478.

34) Instruction on the Procedure for Recording, Processing, and Storing Documents, Files, and Publications Containing Restricted-Distribution Information, approved on December 5, 2006, by the Chairman of the Interdepartmental Commission for Ensuring the Protection of State Secrets under the Deputy Prime Minister of the Republic of Uzbekistan.

35) National Standard O‘zMSt 816:2025, “Information Security, Cybersecurity and Privacy Protection — Guidance for Information Security Policy Development”.

36) Uz ST 1092:2009, “Information Technology. Cryptographic Information Protection. Electronic Digital Signature Generation and Verification Processes”.

37) Uz ST 1108:2011, “Information Technology. Open Systems Interconnection. Public Key Certificate and Attribute Certificate Framework”.

38) O‘zDSt 1047:2018, “Information Technology. Terms and Definitions”.

39) O‘zDSt 1109:2013, “Information Technology. Cryptographic Information Protection. Terms and Definitions”.

40) Uz ST 2927:2015, “Information Technology. Information Security. Terms and Definitions”.

41) Uz ST 2590:2012, “Information Technology. Requirements for the Integration and Interoperability of Information Systems Used by Government Authorities within the Framework of the National Information System”.

42) Uz ST 2814:2014, “Information Technology. Automated Systems. Classification by Levels of Protection against Unauthorized Access to Information”.

43) Uz ST 2815:2014, “Information Technology. Firewalls. Classification by Levels of Protection against Unauthorized Access to Information”.

44) Uz ST 2816:2014, “Information Technology. Classification of Information Security Software by the Level of Control over the Absence of Undeclared Capabilities”.

45) Uz ST 2817:2014, “Information Technology. Computer Hardware. Classification by Levels of Protection against Unauthorized Access to Information”.

46) Uz ST 2875:2014, “Requirements for Data Processing Centers. Ensuring the Availability and Security of Telecommunications Infrastructure Facilities in Accordance with the ‘Infrastructure and Information Security Assurance’ Standard”.

47) Uz ST 3078:2016, “Telecommunication Networks. Virtual Private Networks (VPN). General Requirements”.

48) Uz ST 3243:2017, “Information Technology. Local Area Networks and Corporate Computer Networks. General Technical Requirements”.

49) Uz ST 3386:2019 (Uz ST ISO/IEC 27035-1:2016, MOD), “Information Technology. Security Techniques. Information Security Incident Management. Part 1. Principles of Incident Management”.

50) Uz ST 3387:2019 (Uz ST ISO/IEC 27035-2:2016, MOD), “Information Technology. Security Techniques. Information Security Incident Management. Part 2. Guidelines for Incident Response Planning and Preparation”.

51) Uz ST ISO/IEC 11770-1:2017, “Information Technology. Security Techniques. Key Management. Part 1. Framework”.

52) Uz ST ISO/IEC 13335-1:2009, “Information Technology. Security Techniques. Management of Information and Communications Technology Security. Part 1. Concepts and Models for the Management of Information and Communications Technology Security”.

53) Uz ST ISO/IEC 15408-1:2016, “Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 1. Introduction and General Model”.

54) Uz ST ISO/IEC 15408-2:2016, “Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 2. Security Functional Components”.

55) Uz ST ISO/IEC 15408-3:2016, “Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 3. Security Assurance Components”.

56) Uz ST ISO/IEC 27000:2022, “Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary”.

57) Uz ST ISO/IEC 27001:2020, “Information Technology. Security Techniques. Information Security Management Systems. Requirements”.

58) Uz ST ISO/IEC 27002:2016, “Information Technology. Security Techniques. Code of Practice for Information Security Controls”.

59) Uz ST ISO/IEC 27003:2022, “Information Technology. Security Techniques. Guidance for Information Security Management System Implementation”.

60) O‘zMSt ISO/IEC 27005:2024, “Information Security, Cybersecurity and Privacy Protection. Guidance on Information Security Risk Management”.

61) Uz ST ISO/IEC 27007:2022, “Information Security, Cybersecurity and Privacy Protection. Guidelines for Auditing Information Security Management Systems”.

62) Uz ST ISO/IEC 27008:2022, “Information Technology. Security Techniques. Guidance for Auditors on Information Security Control Assessment”.

63) Uz ST ISO/IEC 27010:2015, “Information Technology. Security Techniques. Information Security Management for Inter-Sector and Inter-Organizational Communications”.

64) Uz ST ISO/IEC 27014:2018, “Information Technology. Security Techniques. Governance of Information Security”.

65) Uz ST ISO/IEC 27031:2016, “Information Technology. Security Techniques. Guidelines for Information and Communication Technology Readiness for Business Continuity”.

66) Uz ST ISO/IEC 27032:2017, “Information Technology. Security Techniques. Guidelines for Cybersecurity”.

67) Uz ST ISO/IEC 27033-1:2016, “Information Technology. Security Techniques. Network Security. Part 1”.

68) Uz ST ISO/IEC 27033-2:2016, “Information Technology. Security Techniques. Network Security. Part 2. Guidelines for the Design and Implementation of Network Security”.

69) Uz ST ISO/IEC 27033-4:2016, “Information Technology. Security Techniques. Network Security. Part 4. Securing Communications between Networks Using Security Gateways”.

70) Uz ST ISO/IEC 27033-5:2016, “Information Technology. Security Techniques. Network Security. Part 5. Securing Inter-Network Communications Using Virtual Private Networks (VPNs)”.

71) Uz ST ISO/IEC 27033-6:2018, “Information Technology. Security Techniques. Network Security. Part 6. Securing Wireless IP Network Access”.

72) Uz ST ISO/IEC 27037:2017, “Information Technology. Security Techniques. Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence”.

73) Uz ST ISO/IEC 27039:2018, “Information Technology. Security Techniques. Selection, Deployment, and Operation of Intrusion Detection Systems”.

74) Uz ST ISO/IEC 27040:2018, “Information Technology. Security Techniques. Storage Security”.

75) Payment Card Industry Data Security Standard (PCI DSS) - an international information security standard for the payment card industry establishing a comprehensive set of requirements for the protection of payment cardholder data.

76) Access Control Rules of the Bank, approved by Minutes of the Management Board No. 7 dated September 24, 2020.

77) IT Service Emergency Management Procedure, approved by Minutes of the Management Board No. 26 dated August 22, 2022.

78) Instruction on the Procedure for Recording, Maintaining, and Storing Documents and Files Containing Information for Official Use Only (FOUO), approved by Minutes of the Management Board No. 32 dated February 12, 2022.

79) Regulation on Compliance with the Commercial Secrecy (Confidentiality) Regime, approved by Minutes of the Management Board No. 32 dated December 2, 2022.

80) Regulation on the Procedure for Processing Personal Data of Employees of ANOR BANK JSC, approved by Minutes of the Management Board No. 7-1 dated May 16, 2023.

1.3. Terms and Definitions

The following terms, definitions, and abbreviations are used in this Policy:

Automated Banking System (ABS) - a system consisting of banking process automation tools and the Bank’s personnel, ensuring the application of banking information technologies to perform specific functions.

information resources - information in electronic form, data banks, and databases that form part of an information system.

information system - an organizationally structured set of information resources, information technologies, and communication facilities that ensures the collection, storage, retrieval, processing, and use of information.

information security incident - a single event or a series of unwanted or unexpected information security events that create a high probability of information compromise or the realization of information security threats.

authentication - the process of verifying the authenticity of an identifier presented by a user to obtain access rights to an information resource; confirmation of the legitimacy of access to a resource.

information asset - information systems of various levels and purposes, telecommunication networks, technical means of information processing, premises in which such means are located and operated, as well as premises intended for conducting meetings and negotiations, including confidential negotiations.

information security management system (isms) - a part of the overall management system based on business risk assessment methods and intended for the development, implementation, operation, monitoring, review, maintenance, and continual improvement of information security.

information protection - activities aimed at preventing the dissemination of protected information, as well as preventing unauthorized or unintentional impact on protected information and the software and hardware means used to access it.

information security - the state of protection of information, its media, and infrastructure against information disclosure (breach of confidentiality), compromise of the integrity of databases and information resources, loss of information, or reduction in information availability.

information infrastructure - a set of core information services and networks, computing systems, and data storage, processing, and transmission systems that ensure the operation of information services.

intellectual property - inventions, developments, trademarks, trade names, commercial designations, names, and images owned by the bank.

security information and event management (SIEM) system - a system that provides the collection, storage, monitoring, and management of information security events, identifies incidents through event stream analysis, and promptly notifies analysts of detected events.

information security event (hereinafter referred to as an **"event"**) - an identified occurrence relating to a system, service, or network indicating a possible violation of the security policy, failure of security controls, or a previously unknown situation that may be relevant to security.

cryptographic information protection tools (CIPT) - a set of software and hardware components of data processing systems capable of operating independently or as part of other systems and performing cryptographic transformation of information to ensure its security.

banking secrecy - information protected by the bank concerning:

- transactions, accounts, and deposits of its customers (correspondent banks);
- information obtained by the Bank about a customer (correspondent bank) in connection with the provision of banking services;
- the existence, nature, and value of a customer's (correspondent bank's) assets held in the Bank's safes and premises;
- interbank transactions and transactions carried out on behalf of or in the interests of a customer (correspondent bank);

– information concerning a customer (correspondent bank) of another bank that became known as a result of the exchange of information constituting banking secrecy between banks.

banking telecommunications network of the central bank of the republic of uzbekistan (BTN) - a set of technologies that provide centralized control and management of banking information collection and processing processes, resource management, and the efficient, reliable, and secure operation of the payment system.

business process - a sequence of technologically interconnected operations for the provision of products, delivery of services, and/or performance of a specific activity.

threat actor - an individual or legal entity interested in obtaining unauthorized access to an information system and its resources and undertaking deliberate actions to obtain or modify information without appropriate authorization.

virtual private network (VPN) - a technology that provides the establishment of a secure connection through the internet.

software - a set of software programs and software documentation necessary for the operation of a data processing system.

confidential information - documented information that does not contain state secrets and access to which is restricted in accordance with applicable legislation.

access control system (ACS) - a combination of software and hardware tools used to control and manage access.

intrusion detection and prevention system (IDPS) - a set of software and/or hardware tools designed to detect and prevent attempts of unauthorized access to the corporate system.

electronic document management system (EDMS) - a system for exchanging electronic documents within the bank, as well as with partner organizations and government authorities, ensuring the creation, approval, transmission, receipt, archiving, and reuse of information.

electronic digital signature (EDS) - an attribute of an electronic document that enables verification of authorship, confirmation of the time of signing, and confirmation that no changes have been made to the document after signing.

database - a collection of data (articles, calculations) presented in an objective form and organized in such a way that it can be searched and processed using computer technology.

database management system (DBMS) - software designed for the creation, management, maintenance, and analysis of databases.

data center (DC) - a physical facility intended for hosting computing equipment and related hardware.

controlled area - a location (territory, building, or part of a building) where uncontrolled presence of unauthorized persons and vehicles without permanent or temporary access authorization is prohibited.

Note. The boundary of a Controlled Area may include:

– the perimeter of the organization's controlled territory;

– the enclosing structures of a protected building or its secured section if located outside the protected territory.

risk assessment - the process of comparing an assessed risk against established risk criteria in order to determine its nature and significance.

information security risk - the possibility of exploiting a specific vulnerability of a data processing system through the realization of a particular threat.

risk analysis - the systematic performance of processes for identifying data processing system assets, threats to those assets, and system vulnerabilities related to such threats.

unauthorized access - access by a subject to an object or information in violation of the established access control rules within the system.

risk treatment - the process of selecting and implementing measures to modify (reduce) risk.

personal data - information relating to an identified or identifiable natural person and enabling that person's identity to be established.

threat - a potential possibility of compromising the security of a computer system or information resources.

commercial secret - information having commercial value due to being unknown to third parties, relating to scientific, technical, technological, production, financial, economic, or other activities, to which there is no lawful free access, and with respect to which its owner takes measures to ensure confidentiality.

vulnerability - a weakness in a data processing system, the exploitation of which may result in a breach of its integrity or improper functioning.

privileged access management (PAM) system - a system intended to ensure the security of critical assets within a client's corporate network (information systems, information resources, and equipment) when granting access to developers, administrators, and representatives of third-party organizations for maintenance and administration purposes.

intellectual property – inventions, developments, trademarks, trade names, commercial identifiers, as well as names and graphic representations owned by the Bank.

user account - a set of information about a user stored in a computer system and required for identification (authentication), as well as for granting access to personal data and settings. as a rule, a user account consists of a username and password combination.

1.4. Scope of Application

The Bank's Information Security Policy defines the Bank's objectives and tasks in the field of information security, as well as the rules, procedures, practices, and governing documents that guide the Bank in the conduct of its activities.

The Bank's Information Security Policy shall serve as the basis for establishing an integrated Information Security Management System (ISMS), including the development of the Bank's internal information security regulatory

documents and the implementation of organizational, technical, and other information security measures.

The requirements of this Policy apply to all protected information of the Bank and the means used for its creation, processing, storage, transmission, protection, and destruction, except for information containing state secrets. The protection of information containing state secrets shall be ensured in accordance with the legislation of the Republic of Uzbekistan governing the protection of state secrets.

The Bank comprises:

a) Head Office - a building intended for the accommodation of the Head Office structural units and the operation of a customer service point on the ground floor (5th Sayram Passage, Tashkent, owned premises);

b) IT Office - a building accommodating the Head Office IT divisions (59 Muqimiy Street, Tashkent, leased premises);

c) Sales Offices - customer service points of the Bank.

In addition, the Bank's infrastructure includes a primary Data Center (DC) located at the Head Office and a disaster recovery Data Center located at the ATS-233 Data Center of JSC Uzbektelecom (51 Istiqlol Street, Tashkent).

For the operation of the primary and disaster recovery Data Centers, the Bank uses its own information processing and storage facilities (servers and data storage systems).

For the operation of the disaster recovery Data Center, the Bank leases premises within the ATS-233 Data Center of JSC Uzbektelecom and utilizes the infrastructure supporting the operation of the data center, including uninterrupted power supply systems, air conditioning systems, fire suppression systems, and other engineering systems.

The connection of the above-mentioned Data Centers to the Bank's corporate network and external networks of the Central Bank of the Republic of Uzbekistan (the Internet and the Banking Telecommunications Network (BTN)) is organized independently by the Bank.

The requirements of this Policy apply to:

a) all information systems and information resources of the Bank;

b) all Bank personnel (permanent employees, temporary employees, contractors, and other personnel), regardless of their workplace location or position held;

c) third parties interacting with the Bank (Bank customers, suppliers, tenants, contractors, auditors, visitors, service personnel, external users of information systems, and other persons) who, on any lawful basis, have access to the Bank's premises and protected assets, including its information resources and information systems.

The Management Board of the Bank, heads of structural divisions, and the Information Security Department shall ensure continuous monitoring of compliance with the requirements of this Policy.

The functions and responsibilities of information security management shall be approved in accordance with the established procedure as part of the relevant Department Regulation.

2. OBJECTIVES AND TASKS OF INFORMATION SECURITY IN THE BANK

2.1. Objectives of Information Security

The objectives of the Bank's information security framework are as follows:

- to protect participants in the Bank's information relationships and users of banking services (hereinafter referred to as the "Bank's Customers") from financial, physical, moral, and other forms of damage that may result from the accidental or deliberate realization of information security threats;
- to ensure the confidentiality, integrity, and availability of information related to the Bank's activities, as well as to ensure the operation of critical information resources, information systems, and other information assets;
- to ensure compliance with the legislation of the Republic of Uzbekistan in the field of information security, as well as applicable regulations, instructions, procedures, and this Policy;
- to protect the lawful rights of participants in information relationships and the Bank's Customers regarding the non-disclosure of information constituting commercial secrets, banking secrecy, personal data, and other confidential information;
- to protect the Bank's information assets from information security threats in order to ensure their stable and reliable operation, which is necessary for the successful and uninterrupted provision of banking services;
- to ensure the resilience of the Bank's operations by guaranteeing the availability of necessary information and maintaining business continuity;
- to establish a balanced approach to protection against information security threats through the implementation of economically and technically justified, as well as necessary and sufficient, information security controls.

2.2. Information Security Objectives and Tasks of the Bank

To achieve the information security objectives, the Bank shall address the following tasks:

- establishing, implementing, and continuously developing the Information Security Management System (ISMS) in accordance with business requirements, applicable legislation, and regulatory requirements;
- implementing effective information security management methods and controls to protect the Bank's information assets and protected information against various threats, as well as to mitigate information security risks;
- ensuring continuous monitoring of the information security posture in order to timely identify and eliminate information security threats;
- establishing mechanisms and conditions for prompt response to information security threats and information security incidents;

- enhancing the awareness of users and Bank personnel, as well as improving the qualifications of information security specialists, while ensuring their active involvement in information security management processes;

- ensuring control over compliance by users and Bank personnel with information protection requirements during information processing activities;

- developing and continuously improving the regulatory and methodological framework for information security;

- organizing antivirus protection for the Bank's information assets;

- increasing the level of security and operational reliability of the Bank's critical information assets.

3. KEY INFORMATION SECURITY PROVISIONS

3.1. The Bank's Information Security Policy is Based on the Following Principles

1) Legality - compliance with the requirements of applicable laws, regulations, and regulatory documents when ensuring information security.

2) Involvement - the Bank's management and all Bank personnel participate in information security management processes.

3) Segregation of Duties - roles, authorities, and responsibilities relating to information security shall be clearly allocated among Bank personnel.

4) Personal Accountability - Bank personnel shall bear personal responsibility for complying with information security requirements established by employment agreements, job descriptions, and other agreements (contracts) concluded with the Bank.

5) Professionalism - the knowledge level and professional qualifications of personnel responsible for information security shall be continuously enhanced and effectively applied within information security management processes.

6) Cooperation and Coordination - information security activities shall be carried out in cooperation with relevant stakeholders and on the basis of alignment of information security objectives, tasks, principles, and controls.

7) Enhanced Protection - information security controls shall be selected with due consideration for the need to establish effective protection against all categories of information security threats.

8) Systematic Approach - the development of the Bank's Information Security Management System (ISMS) shall take into account all elements, conditions, and factors affecting information security and their changes over time.

9) Comprehensive Protection - the integrated application of information protection methods and controls shall ensure the coordinated use of diverse security measures in the construction of a holistic protection system that eliminates vulnerabilities in individual components and provides coverage against all significant threat vectors.

10) Continuity of Protection - information security activities shall be performed on an ongoing basis and shall encompass all levels of the Bank's operations.

11) Defense in Depth - information security management processes shall be implemented at all levels and throughout all structural units of the Bank.

12) Accountability and Activity Logging - ensuring monitoring of compliance by Bank personnel with information security requirements, managing access to information assets, and maintaining records of all actions performed by personnel in connection with the use of information assets.

13) Timeliness - information security measures shall be proactive in nature, requiring the establishment of comprehensive information protection objectives and the implementation of information security controls at the earliest stages of the development and evolution of information systems and information protection systems.

14) Sufficiency - expenditures on information security shall be commensurate with the value of information assets and the potential damage that may result from their disclosure, loss, leakage, destruction, or alteration. Information security controls and measures shall not materially impair the usability and operational characteristics of the Bank's information systems.

15) Personal Responsibility - each employee shall be responsible for ensuring the security of information and information processing systems within the scope of their authority. In accordance with this principle, the allocation of rights and responsibilities among personnel shall be organized in such a manner that, in the event of a violation, the responsible individual(s) can be clearly identified or the circle of responsible persons can be reduced to the minimum possible extent.

3.2. Information Security Implementation

In the course of implementing its information security objectives, the Bank shall:

- establish and maintain a regulatory framework governing information security processes within the Bank's information and communication infrastructure;
- identify and classify the Bank's information and other protected assets;
- conduct objective and comprehensive analysis and forecasting of information security threats, as well as information security risk analysis and assessment;
- develop information security requirements and controls for the Bank's information and communication infrastructure;
- organize the activities of the necessary structural divisions to implement a set of measures aimed at preventing, detecting, countering, and mitigating information security threats;
- ensure the implementation, development, and monitoring of information security controls, as well as organize certification and licensing activities in the field of information security in accordance with applicable legal and regulatory requirements;
- perform periodic assessments of the security posture of information assets, identify and record actual, ongoing, or potential information security violations, and ensure timely response to such violations.

3.3. Specific methods and measures implemented as part of the Bank's information security program are set out in Section 7 of this Policy.

4. INFORMATION ASSETS SUBJECT TO PROTECTION

4.1. The Primary Information Security Assets Subject to Protection within the Bank Include:

1) Confidential Information, including:

- internal (business) information intended for restricted distribution;
- information constituting the commercial secret of the Bank, its customers, partners, and counterparties within the framework of contractual relationships;
- information constituting banking secrecy;
- personal data of the Bank's employees and customers;
- payment information and payment system documentation.

2) The Bank's Business Processes, including information and payment processes implemented through the Bank's information systems.

3) Information Relationship Participants, including:

- the Bank's customers and information relating to their transactions;
- Bank employees;
- developers of the Bank's information systems software.

4) The Bank's Intellectual Property Assets.

5) Hardware Assets, including:

workstations, laptops, tablets, servers, data storage systems (DSS), and other information processing and storage equipment.

6) Software Assets, including:

operating systems, application software and applications, source code, database management systems (DBMS), diagnostic software, development tools, and utility software.

The Bank shall maintain a list of software authorized for use. Requirements for maintaining such list, as well as requirements relating to the installation and use of software, shall be governed by the List of Authorized Software (Appendix 9 to this Policy).

7) Information Exchange Services and Systems, including:

- corporate e-mail services operated through the Bank's own mail server for all Bank employees. The procedure for the use of corporate e-mail and Internet access is governed by the Internet and Corporate E-mail Usage Rules (Appendix 10 to this Policy);
- the Myanor.uz Electronic Document Management System (EDMS);
- the Anor Chat corporate messenger intended for оперативный exchange of messages between Bank employees;
- the IP telephony system and Contact Center (Call Center);
- the video conferencing system.

8) Physical Security Systems, including:

- the Access Control System (ACS), which controls employee access to protected areas within the Head Office and IT Office through the use of plastic identification cards and biometric data (facial recognition);

- the video surveillance system that provides video monitoring and collection of video data through cameras installed around the perimeter and inside the premises of the Head Office, IT Office, and ATM locations.

9) The Bank's Network Infrastructure, including:

- domain controller servers used to operate the Bank's managed network environment (primary and backup servers located in the Bank's primary Data Center);

- core corporate network switches and access switches of local networks within the Head Office, IT Office, and Sales Offices;

- local area networks (LANs) deployed within the Head Office, IT Office, and Sales Offices;

- communication channels of the Bank's corporate network (connections between the primary Data Center, disaster recovery Data Center, IT Office, and Sales Offices), as well as external communication channels providing connectivity between the Bank's corporate network and the Internet and the Banking Telecommunications Network (BTN) of the Central Bank of the Republic of Uzbekistan;

- dedicated fiber-optic communication lines ("dark fiber") connecting the Bank's primary Data Center (Head Office) and the disaster recovery Data Center located at the ATS-233 Data Center of JSC Uzbektelecom.

10) Information Resources, including:

- the Bank's official website: https://anorbank.uz/, hosted primarily within the Bank's Data Center;

- the remote banking services web portal (BSS Internet Banking), hosted in the Bank's primary Data Center;

- the file repository maintained on a server located in the Bank's primary Data Center for use by the Bank's structural divisions;

- databases of information systems, including the database of the Bank's Automated Banking System (ABS), as well as their electronic archives.

11) Media Containing Protected Information.

12) Protected Premises, including:

- office premises of the Bank's Head Office where confidential information is processed;

- the server room of the Bank's primary Data Center.

13) Information Security Controls, including:

firewalls, Intrusion Detection and Prevention Systems (IDPS), VPN connectivity solutions, antivirus protection tools, and other information security solutions.

14) The Bank's Information Systems.

15) The Bank's Intangible Assets.

4.2. The Following Information Systems Operate within the Bank

1) Automated Banking System (ABS) - a system used to perform banking transactions for the Bank's customers.

The ABS includes the following hardware and software components:

- database servers (two physical database servers operating in cluster mode within the primary and disaster recovery Data Centers);

- application servers providing Head Office employees (ABS users) with access to the ABS through the Bank's corporate network, hosted on virtual servers in the primary Data Center with failover capabilities in the disaster recovery Data Center.

Users of the ABS are Bank employees.

2) BSS Remote Banking Service System (hereinafter referred to as the "BSS RBS System") - an Internet banking system for providing Digital Banking Services to legal entities, as well as the Anor Business mobile banking application for legal entities and the Anorbank mobile application for individuals.

The BSS RBS System consists of two virtual database servers and three virtual application servers.

Users of the BSS RBS System are the Bank's customers and employees.

3) ELMA Business Process Management System (hereinafter referred to as the "ELMA System"), designed to automate the Bank's customer service processes.

The system is hosted on virtual servers in the primary Data Center with redundancy provided through dedicated physical servers located in the primary and disaster recovery Data Centers.

Users of the system are Bank employees.

4) Wings System - a system for collecting and processing information on the creditworthiness of the Bank's customers (borrower credit scoring).

The system consists of two virtual database servers and two virtual application servers with redundancy within the Data Center environment.

Users of the Wings System are Bank employees.

5) BillMaster System - a settlement processing system hosted on virtual servers within the primary Data Center with redundancy provided through dedicated physical servers located in the primary and disaster recovery Data Centers.

Users of the BillMaster System are Bank employees.

6) BillMaster Settlement System (hereinafter referred to as the "BillMaster System") - a system consisting primarily of virtual central database servers with redundancy provided through dedicated physical servers of the primary and backup databases.

Users of the system are Bank employees.

7) AGC (previously ADPMS) - a platform that consolidates all Bank databases into a unified system for convenient management, administration, and use by Bank employees.

Users of the system are Bank employees.

8) AnorHub - a centralized access management platform designed to facilitate authorized interaction with the Bank's information systems and

information resources through a single access gateway and to ensure registration (logging) of all access requests.

Users of the system are Bank employees.

9) Qlik Sense - a real-time data analytics and visualization platform utilizing a centralized data warehouse and a specialized query language.

Users of the system are Bank employees.

10) Confluence - an internal system intended for maintaining the Bank's centralized knowledge base, including technical documentation, project documentation, privilege matrices, and guidelines for the use of the Bank's information resources.

Users of the system are Bank employees.

11) GitLab - a Git-based source code repository management system that includes an integrated Wiki, issue tracking system, CI/CD pipeline, and other software development functions.

Users of the system are Bank employees.

12) Jira - a platform for planning, allocation, and management of IT projects and tasks, facilitating effective collaboration among teams.

Users of the system are Bank employees.

13) Keycloak - a software solution providing centralized identity and access management for information systems.

14) MerchantCabinet - a platform for interaction with partners of ANOR BANK JSC, intended for event monitoring, reporting analysis, and generation of settlement reports relating to partner transactions.

15) ServiceDesk - a platform for organizing and managing IT service support processes.

16) Verifix - a system for recording employee attendance within the Bank's sales divisions.

17) WEBIM - a platform that consolidates requests received through the mobile application, Instagram, and Telegram bots into a single customer request processing system, enabling Contact Center personnel to provide 24/7 response and support.

18) Superset - a real-time data analytics and visualization platform based on a centralized data warehouse and a specialized query language.

Users of the system are Bank employees.

19) IC - an accounting and tax management system supporting all financial and business operations of the Bank.

4.3. The Bank's Automated Banking System (ABS) is integrated with all internal information systems of the Bank, including the BSS Remote Banking Service (RBS) System, ELMA, Wings, BillMaster, and other information systems.

4.4. The Bank’s ABS interacts with (exchanges data with) external information systems, including the information systems of the Central Bank of the Republic of Uzbekistan, the HUMO and UzCard processing systems, the Credit Bureau system of the Banking Association, and the information systems of other organizations.

4.5. The interaction between the ABS and external information systems is carried out through the Banking Telecommunications Network (BTN) of the Central Bank of the Republic of Uzbekistan using secure IPSec VPN communication channels.

4.6. In accordance with the state standard Uz ST 2814:2014 “Information Technology. Automated Systems. Classification by Levels of Protection against Unauthorized Access to Information”, the Bank’s Automated Banking System (ABS) is classified as Security Class 3B.

4.7. The classification of the Bank’s information resources by security level is set out in the Register of the Bank’s Information Resources, which forms an appendix to this Policy (Appendix 11).

4.8. The databases of the Bank’s information systems specified in Table 1 contain personal data of the Bank’s employees and customers.

In accordance with the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 570 dated October 5, 2022, “On Approval of Certain Regulatory Legal Acts in the Field of Personal Data Processing”, the relevant protection levels have been established for these databases.

The requirements for the protection of personal data processed within the Bank’s information systems are defined by the Regulation on the Procedure for Processing Personal Data of Employees of ANOR BANK JSC, approved by Minutes of the Management Board No. 7-1 dated May 16, 2023.

Table 1. List of the Bank’s Databases Intended for the Processing of Personal Data, Including the Assigned Protection Level**.**

Database Name	**Type of Personal Data**	**Protection Level**
ABS Database	Personal data of the Bank’s customers	Level 2
BSS Remote Banking Service (RBS) System Database	Personal data of the Bank’s customers	Level 2
Wings System Database	Personal data of the Bank’s customers	Level 2
BillMaster System Database	Personal data of the Bank’s customers	Level 2
Keycloak System Database	Personal data of the Bank’s customers	Level 2

Database Name	Type of Personal Data	Protection Level
Oktell System Database	Personal data of the Bank's customers	Level 2
Access Control System (ACS) Database	Personal data of the Bank's employees	Level 1

4.9. The Bank's protected assets are created and operated using hardware-software and software solutions, the list of which is provided in Appendix 18 to this Policy.

5. INFORMATION SECURITY RISK AND THREAT MODEL

5.1. The Bank's information security threat model shall be defined for each critical protected asset specified in Section 4 of this Policy and shall include:

- a description of the protected asset;
- a list and description of potential information security threats affecting the protected asset;
- an information security threat actor model;
- potential vulnerabilities;
- methods of threat realization;
- consequences of threat realization.

5.2. Based on their nature of occurrence, information security threats to the Bank may be natural (objective) and man-made (subjective).

5.3. Sources of information security threats may be - internal - where the source of the threat is located within the Bank and external - where the source of the threat is located outside the Bank.

5.4. Information security threats may be intentional - deliberately carried out to achieve a specific objective and accidental - arising as a result of failures of hardware, software, or human error.

5.5. The Bank's primary information security threat model is set out in Table 2.

5.6. For the purpose of determining the level of information security, the Bank shall perform information security risk analysis and assessment.

An information security risk is determined by the likelihood of damage and losses occurring as a result of the realization of information security threats.

Information security risks arise due to the existence of a real possibility that threats may affect protected assets.

Table 2. Primary Information Security Threat Model of the Bank

Category	Code	Threat Name	Type, Nature and Source of Threat*	Affected Assets and Consequences
Physical Threats	TP01	Fire	A, D, E, F, B, C	All protected assets. Failure or loss
	TP02	Flooding	A, D, E, F, B, C	
	TP03	Contamination, Harmful Radiation	A, D, E, F, B, C	
	TP04	Major Accident	A, D, E, F, B, C	
	TP05	Explosion, Disaster	A, D, E, F, B, C	
	TP06	Dust, Corrosion, Icing	A, D, E, F, B, C	
Natural Threats	TN01	Climatic Events	A, E, C	All protected assets. Failure or loss
	TN02	Seismic Events	A, E, C	
	TN03	Volcanic Events	A, E, C	
	TN04	Meteorological Events	A, E, C	
	TN05	Flood	A, E, C	
	TN06	Pandemic / Epidemic	A, E, C	
Infrastructure Failures	TI01	Failure of Supporting Systems	A, D, F, C	Hardware and software, workstations and servers, local network, corporate e-mail, information systems and information resources. Failure or service disruption
	TI02	Cooling or Ventilation System Failure	A, D, F, B, C	
	TI03	Power Supply Disruption	A, D, E, F, C	
	TI04	Telecommunications Network Failure	A, D, E, F, C	

Category	Code	Threat Name	Type, Nature and Source of Threat*	Affected Assets and Consequences
	TI05	Telecommunications Equipment Failure	A, D, F, B	
	TI06	Electromagnetic Radiation	A, D, E, F, C	
	TI07	Thermal Radiation	A, D, E, F, B, C	
	TI08	Electromagnetic Pulse (EMP)	A, D, E, F, C	
Technical Failures	TT01	Device or System Failure	A, F, B	Hardware and software, workstations, servers, local networks, information systems and information resources. Failure, service disruption, loss of equipment or data
	TT02	Information System Overload	A, D, F, B	
	TT03	Impaired Maintainability of an Information System	A, D, F, B	
Human-Related Threats	TH01	Terrorism, Attack, Sabotage	D, F, B, C	All protected assets. Failure or loss
	TH02	Social Engineering	D, F, B, C	Hardware and software of networks and information systems. Compromise of confidentiality, integrity, and availability
	TH03	Interception of Equipment Emissions	D, F, B, C	Information. Breach of confidentiality
	TH04	Remote Monitoring	D, F, B, C	

Category	Code	Threat Name	Type, Nature and Source of Threat*	Affected Assets and Consequences
	TH05	Eavesdropping	D, F, B, C	
	TH06	Theft of Information Media or Documents	D, F, B, C	Information media, repositories, and documents. Breach of integrity and confidentiality
	TH07	Theft of Equipment	D, F, B, C	Equipment. Loss and disruption of operations
	TH08	Theft of Digital Identifiers or Credentials	D, F, B, C	Workstations, servers, networks, and information systems. Unauthorized access
	TH09	Recovery of Data from Discarded or Reused Media	D, F, B, C	Information. Breach of confidentiality
	TH10	Disclosure of Information	A, D, F, B, C	Information. Breach of confidentiality
	TH11	Input of Data from Untrusted Sources	A, D, F, B, C	Information. Loss of integrity and reliability
	TH12	Damage to Equipment	D, F, B, C	Equipment and data. Compromise of functionality, integrity, confidentiality, and availability
	TH13	Damage to Software	A, D, F, B, C	Software and data. Compromise of functionality, integrity, confidentiality, and availability
	TH14	Exploitation of Vulnerabilities through	D, F, B, C	Information resources and information

Category	Code	Threat Name	Type, Nature and Source of Threat*	Affected Assets and Consequences
		Web Connections (Drive-by Exploitation)		systems. Unauthorized access
	TH15	Replay Attack, Man-in-the-Middle Attack	D, F, B, C	Data. Unauthorized access
	TH16	Unauthorized Processing of Personal Data	A, D, F, B, C	Personal data. Breach of confidentiality
	TH17	Unauthorized Access to Assets	D, F, B, C	All protected assets. Unauthorized access
	TH18	Unauthorized Use of Equipment	D, F, B, C	Equipment. Failure or service disruption
	TH19	Improper Operation of Equipment	A, D, F, B, C	Equipment. Failure or service disruption
	TH20	Damage to Equipment or Information Media	A, D, F, B, C	Equipment and information media. Failure or service disruption
	TH21	Copying of Unlicensed Software	D, F, B, C	Software. Functional impairment and copyright infringement
	TH22	Use of Counterfeit or Unlicensed Software	A, D, F, B, C	
	TH23	Data Corruption	D, F, B, C	Data. Breach of integrity
	TH24	Unlawful Data Processing	D, F, B, C	Data. Illegal use of information and copyright infringement
	TH25	Transmission or Distribution of Malware	A, D, E, F, B, C	Workstations, networks, information systems, and information resources. Failure, loss, or unauthorized access

Category	Code	Threat Name	Type, Nature and Source of Threat*	Affected Assets and Consequences
	TH26	Location Tracking / Geolocation Determination	D, F, B, C	Information. Breach of confidentiality
Service or Functional Disruptions	TC01	Usage Errors	A, F, B, C	Hardware and software, networks, information systems, information resources, and information. Failure, loss, or unauthorized access
	TC02	Abuse of Rights or Privileges	A, D, F, B, C	
	TC03	Forgery of Rights or Privileges	D, F, B, C	
	TC04	Repudiation of Performed Actions	D, F, B, C	
Organizational Threats	TO01	Insufficient Personnel	A, E, F, B	Hardware and software, networks, information systems, information resources, and information. Disruption of operations
	TO02	Insufficient Resources	A, E, F, B	
	TO03	Insolvency of a Service Provider	A, E, F, C	
	TO04	Violation of Legal and Regulatory Requirements	A, D, F, B, C	
Threats to Data Storage Systems and Infrastructure	TD01	Unauthorized Use	D, F, B, C	Data storage systems and storage infrastructure, stored data, and information media. Compromise of integrity, availability, and confidentiality

Category	Code	Threat Name	Type, Nature and Source of Threat*	Affected Assets and Consequences
	TD02	Unauthorized Access	D, F, B, C	
	TD03	Legal Liability for Non-Compliance with Legal and Regulatory Requirements	A, D, F, B, C	
	TD04	DoS and DDoS Attacks on Data Storage Systems	D, F, C	
	TD05	Damage, Alteration, or Destruction of Data	A, D, F, B, C	
	TD06	Data Leakage	D, F, B	
	TD07	Theft or Accidental Loss of Information Media	A, D, F, B, C	
	TD08	Malware Attack or Malicious Code Injection	D, F, B, C	
	TD09	Improper Processing or Disposal after End of Use	A, D, F, B	

*Note: Threats may be classified according to the following criteria:
- by source of origin: B - internal; C - external;
- by cause of occurrence: A - accidental; D - intentional;
- by nature of occurrence: E - natural (objective); F - man-made (subjective).

5.7. Within the Bank, risk identification is carried out through the identification, analysis, and assessment of information security risks in accordance with the requirements of the national standard O‘zMSt ISO/IEC 27005:2024 “Information Security, Cybersecurity and Privacy Protection — Guidance on Information Security Risk Management.”

5.8. The results of risk identification shall serve as the basis for determining appropriate management decisions and priority areas of information security management and shall be aimed at implementing selected controls, methods, and protective measures to address identified information security risks.

5.9. Risk identification includes a systematic approach to risk assessment (risk analysis), as well as the comparison of assessed risks against risk acceptance criteria in order to determine their level of significance.

In addition to risk identification, the risk management process shall include: risk treatment; risk acceptance; risk communication and consultation; risk monitoring and review.

5.10. Information security risk identification shall be performed by the Information Security Department.

5.11. The information security risk assessment methodology, as well as the procedure for calculating information security risks relating to the Bank’s primary protected assets, is set out in Appendix 17 to this Policy.

5.12. The results of information security risk assessments shall be compared against the established risk acceptance criteria. Risks whose values exceed the established risk acceptance threshold shall be deemed unacceptable risks.

Table 3. Information Security Risk Acceptance Criteria of the Bank.

Risk Level	**Risk Rating**	**Quantitative Value**	**Description**
Low (Green)	Accepted without additional measures	0–1	The risk may be accepted without implementing additional measures.
Medium (Yellow)	Accepted subject to the existence of controls	1–2	Risk treatment measures shall be identified and implemented within the framework of continual improvement processes over the medium and long term.
High (Red)	Unacceptable	Greater than 2	Risk mitigation measures shall be implemented in the short term to reduce the risk level.

5.13. The results of information security risk assessments relating to the Bank's primary protected assets, after comparison against the risk acceptance criteria, shall be presented in the form of a risk heat map (risk matrix) and are provided in Table 4.

5.14. An information security risk classified as "High" (Red Level) indicates that its value exceeds the established risk acceptance criteria and requires the implementation of risk mitigation measures. Such measures may be aimed at: reducing the likelihood of a threat occurring or eliminating the threat altogether; eliminating or reducing the level of the corresponding vulnerability.

5.15. Following the implementation of risk treatment measures, a reassessment of risks shall be performed taking into account the updated threat parameters and the current level of existing vulnerabilities. The resulting revised risk value shall be considered the residual information security risk.

Measures implemented to reduce high-level information security risks, as well as the corresponding residual information security risk values after implementation of such measures, are provided in Table 5.

5.16. To mitigate high-level information security risks, appropriate information security controls and protection tools possessing the required security characteristics shall also be selected and implemented. The requirements applicable to information security controls used by the Bank are set out in Section 7 of this Policy.

Table 4. Results of Information Security Risk Assessment for the Bank's Protected Assets

№	Threat Description	Automated Banking System (ABS)	BSS Remote Banking Service System (BSS RBS)	ELMA, CRM, AGC (ADPMS), and AnorHub (MerchantCabinet) Systems	BillMaster, MyAnor EDMS, Superset, and 1C Systems	Wings, Qlik Sense, WEBIM, and Keycloak Systems	Jira, ServiceDesk, Verifix, and Oktell Systems	Confluence and GitLab Systems	Corporate E-mail System	IP Telephony System and Contact Center (Call Center)	Domain Controller Server	File Server	Official Website	End-User Devices	Access Control System (ACS)	Video Surveillance System (VSS)
TP01	Fire	0,59	0,59	0,52	0,46	0,39	0,33	0,26	0,46	0,39	0,46	0,46	0,28	0,54	0,30	0,26
TP02	Flooding	0,47	0,47	0,42	0,37	0,32	0,26	0,21	0,37	0,32	0,37	0,37	0,23	0,44	0,26	0,23
TP03	Contamination, Harmful	0,18	0,18	0.16	0,14	0,12	0,10	0,08	0,14	0,12	0,14	0,14	0,10	0,18	0,14	0,12
TP04	Major Accident	0,66	0,66	0,58	0,51	0,44	0,36	0,29	0,51	0,44	0,51	0,51	0,33	0,59	0,48	0,41
TP05	Explosion, Disaster	0,23	0,23	0,21	0,18	0,15	0,13	0,10	0,18	0,15	0,18	0,18	0,11	0,23	0,24	0,21
TP06	Dust, Corrosion, Icing	0,23	0.23	0,21	0,18	0,15	0,13	0,10	0,18	0,15	0,18	0,18	0,11	0,21	0,17	0,15
TN01	Climatic Events	0,90	0,90	0,80	0,70	0,60	0,50	0,40	0,70	0,60	0,70	0,70	0,48	0,96	0,35	0,30
TN02	Seismic Events	0,68	0,68	0,60	0,53	0,45	0,38	0,30	0,53	0,45	0,53	0.53	0,50	1,05	0,53	0,45
TN03	Volcanic Events	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0.00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
TN04	Meteorological Events	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,32	0,64	0,28	0,24
TN05	Flood	0.84	0,84	0,75	0,65	0,56	0,47	0,37	0,65	0,56	0,65	0,65	0,37	0,80	0,65	0,56
TN06	Pandemic / Epidemic	0,54	0,54	0,48	0,42	0.36	0,30	0.24	0,42	0.36	0,42	0,42	0.40	0,84	0,42	0,36
TI01	Failure of Supporting Systems	1,26	1,26	1,12	0,98	0,84	0,70	0,56	0,98	0,72	1,12	1,12	0,64	1,32	1,12	0,96
TI02	Cooling or Ventilation System	1,58	1,58	1,40	1,23	1,12	0,93	0,75	1,39	1,12	1,47	1,55	0,84	1,75	1,47	1,26
TIO3	Power Supply Disruption	1,80	1,80	1,60	1,40	1,28	1,07	0,85	1,59	1,36	1,59	1,68	0,91	1,88	1,47	1,26
TI04	Telecommunications Network Failure	1,89	1,89	1,68	1,47	1,32	1,10	0,88	1,61	1,44	1,68	1,61	0,72	1,68	1,61	1,38

TI05	Telecommunications Equipment Failure	1,62	1,68	1,49	1,31	1,16	0,97	0,77	1,40	1,20	1,49	1,49	0,88	1,80	1,45	1,24
TI06	Electromagnetic Radiation	0,54	0,54	0,48	0,42	0,36	0,30	0,24	0,42	0,36	0,42	0,42	0,24	0,48	0,2	0,18
TI07	Thermal Radiation	0,72	0,72	0,64	0,56	0,48	0,40	0,32	0,56	0,48	0,56	0,56	0,32	0,48	0,5	0,48
TI08	Electromagnetic Pulse (EMP)	0,54	0,54	0,48	0,42	0,36	0,30	0,24	0,42	0,36	0,42	0,42	0,24	0,48	0,1	0,12
TT01	Device or System Failure	3,40	3,35	2,98	2,61	1,81	1,84	1,47	2,58	2,22	1,96	2,53	1,42	1,90	1,9	1,80
TT02	Information System Overload	1,35	1,35	1,20	1,05	0,90	0,75	0,60	1,05	0.90	1,05	1,05	0,72	1,38	0,8	0,72
TTO3	Impaired Maintainability of an Information System	0,92	0,92	0.81	0,71	0,63	0,53	0,42	0,76	0,63	0,79	0,81	0,48	0,89	0,76	0,65
TH01	Terrorism, Attack, Sabotage	0,37	0,38	0,34	0,30	0,26	0,22	0,18	0,35	0,27	0,33	0,31	0,21	0,38	0,2	0,25
TH02	Social Engineering	1,26	1,32	1,17	1,02	0,92	0,76	0.61	1,25	0,95	1,16	1,07	0,79	1,34	0.9	0,84
THO3	Interception of Compromising Electromagnetic Emanations from Equipment	0,81	0.81	0,72	0,63	0,54	0,45	0,36	0,63	0,54	0,63	0.63	0,36	0,72	0,63	0,54
TH04	Remote Monitoring	0,70	0,70	0,62	0,55	0,50	0,42	0,34	0,59	0,50	0,63	0,59	0,38	0,68	0,5	0,50
TH05	Eavesdropping	0,86	0,86	0,77	0,67	0,65	0,54	0,43	0,76	0,65	0,84	0,76	0,53	1,08	0,7	0,65
TH06	Theft of Information Media or Documents	1,37	1,37	1,22	1,06	0,94	0,78	0,62	1,09	0,94	1,12	1,09	0,72	1,42	1,06	0,91
TH07	Theft of Equipment	0,83	0,83	0,74	0,64	0,58	0.48	0,38	0,67	0,58	0,70	0,67	0,46	0,84	0,6	0,58
TH08	Theft of Digital Identifiers or Credentials	1,27	1,27	1,13	0,99	0,87	0,73	0,58	1,02	0,87	1,05	1,02	0,69	1,21	1,02	0,87
TH09	Recovery of Information from Discarded or Reused Media	1,44	1,44	1,28	1,12	1,02	0.85	0,68	1,19	1,02	1,26	1,19	0,84	1,44	1,12	0,96
THIO	Disclosure of Information	2,15	2,09	2,07	1,31	1,17	0,98	0,78	1,37	1,17	1,42	1,37	0,81	1,35	1,3	1,17
TH11	Input of Data from Untrusted Sources	1,65	1,73	1,53	1,34	1,20	1,00	0,80	1,40	1,20	1,46	1,40	0,83	1,35	1,28	1,10

TH12	Damage to Equipment	0,86	0,86	0,77	0,67	0,58	0,48	0,38	0,67	0,58	0,67	0,67	0,40	0,72	0,6	0,55
TH13	Damage to Software	1,14	1,16	1,04	0,91	0,79	0,66	0.53	0,91	0,78	0,91	0,93	0,59	1,01	0,7	0,65
TH14	Exploitation of Vulnerabilities through Web Connections (Drive-by Exploitation)	1,03	1,13	1,00	0,88	0,79	0.65	0,52	1,07	0,82	0,99	0,92	0,63	1,18	0,57	0.49
TH15	Replay Attack, Man-in-the-Middle Attack	1,08	1,14	1,01	0,89	0,80	0,67	0,53	1,12	0,80	0,98	0,93	0,67	1,04	0,79	0,68
TH16	Unauthorized Processing of Personal Data	1,64	1,67	1,48	1,30	1,11	0,93	0,74	1,30	1,13	1,32	1,30	0,86	1,53	1,22	1,05
TH 17	Unauthorized Access to Assets	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,27	0,64	0,3	0.32
TH18	Unauthorized Use of Equipment	0,82	0,82	0,73	0,64	0,55	0,46	0,37	0,64	0,55	0,64	0,64	0,41	0,75	0,6	0,55
TH19	Improper Operation of Equipment	1,08	1,08	0,96	0,84	0,72	0,60	0,48	0,84	0,72	0,84	0.84	0,48	0,72	0.8	0,72
TH20	Damage to Equipment or Information Media	0,99	0,99	0,88	0,77	0,72	0,60	0,48	0,77	0,66	0,77	0,84	0,60	1,20	0,63	0.54
TH21	Copying of Unlicensed Software	1,50	1,50	1,33	1,16	1,00	0,83	0,67	1,16	1.00	1,16	1,16	0,74	1,42	1,0	0.89
TH22	Use of Counterfeit or Unlicensed Software	0,96	0,96	0,85	0,75	0,68	0,57	0,45	0,79	0.68	0,84	0,79	0,51	0,88	0,70	0,60
TH23	Data Corruption	1,13	1,13	1,00	0,88	0,75	0,63	0,50	0,88	0,75	0,88	0,88	0,54	1,32	0,8	0,75
TH24	Unlawful Data Processing	1,49	1,53	1,36	1,19	1,02	0,85	0,68	1,19	1,02	1,19	1,19	0,72	1,20	1,1	0,96
TH25	Transmission or Distribution of Malicious Software	1,14	1,20	1,07	0,93	0,84	0,70	0,56	1,17	0,84	1,03	0,98	0.64	1,04	0,70	0,60
TH26	Location Tracking / Geolocation	0,45	0,45	0,40	0,35	0,30	0,25	0.20	0,35	0,36	0,42	0,35	0,24	0.42	0,3	0,30
TC01	Usage Errors	1,18	1,18	1,05	0,92	0,83	0,69	0,55	0,94	0,81	0,96	0,96	0,60	1,11	0,7	0,68
TC02	Abuse of Rights or Privileges	1,49	1,49	1,32	1,16	0,99	0,83	0.66	1,16	0.99	1,16	1,16	0,66	1,08	1,1	0.99
TC03	Forgery of Rights or Privileges	1,20	1,20	1,07	0,93	0,84	0,70	0,56	0,98	0,84	1,03	0,98	0,67	1,04	0,9	0,84
TC04	Repudiation of Performed	1,41	1,41	1,26	1,10	0,94	0,79	0,63	1,10	0,94	1,10	1,10	0,63	1,11	1,5	1,32

TO01	Insufficient Personnel	1,26	1,26	1,12	0,98	0,84	0,70	0,56	0,98	0,84	0,98	0,98	0,56	0,84	0,9	0,84
TO02	Insufficient Resources	1,44	1,44	1,28	1,12	1,08	0,90	0,72	1,40	1,20	1,40	1,40	0,64	1,44	1,4	1,20
TO03	Insolvency of a Service Provider	1,26	1,26	1,12	0.98	0,84	0,70	0.56	0,98	0,72	1,12	1,12	0.64	1,32	1,1	0,96
TO04	Violation of Legal and Regulatory Requirements	1,54	1,54	1,37	1,20	1,08	0,94	0,75	1,32	1,08	1,38	1,26	0,79	1,44	1,26	1,08
TD01	Unauthorized Use	1,23	1,25	1,11	0,97	0,83	0,70	0,56	0,97	0,85	0,99	0,97	0,64	1,15	0,9	0,79
TD02	Unauthorized Access	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,27	0,64	0,3	0,32
TD03	Legal Liability for Non-Compliance with Legal and Regulatory Requirements	1,54	1,54	1,37	1,20	1,08	0,94	0,75	1,32	1,08	1,38	1,26	0,79	1,44	1,26	1,08
TD04	DoS and DDoS Attacks on Data Storage Systems	1,89	1,89	1,68	1,47	1,26	1,05	0,84	1,47	1,26	1,47	1,47	0,84	1,26	1,26	1,08
TD05	Damage, Alteration, or Destruction of Data	1,40	1,40	1,25	1,09	0,96	0.80	0,64	1,12	0,96	1,15	1,12	0,75	1,37	1,09	0.94
TD06	Data Leakage	2,09	2,09	1,50	1,31	1,17	0,98	0,78	1,37	1,17	1,42	1,37	0,81	1,35	1,3	1,17
TD07	Theft or Accidental Loss of Information Media or Data Storage Devices	0,79	0,79	0,70	0,62	0,58	0,48	0,38	0.62	0,53	0,62	0,67	0,48	0,96	0,50	0,43
TD08	Malware Attack or Malicious Code Injection	1,14	1,20	1,07	0,93	0,84	0,70	0,56	1,17	0,84	1,03	0,98	0,64	1,08	0,70	0,60
TD09	Improper Processing or Disposal after End of Use	2,13	2,13	2,04	1,84	1,22	1,02	0,82	1,43	1,22	1,51	1,43	1,01	1,73	1,34	1,15

Table 5. Information Security Risk Mitigation Measures and Residual Information Security Risk Following the Implementation of Such Measures

Threat Name	Risk Rating	Protected Assets	Planned Measures	Residual Risk
Device or System Failure	3.40	Automated Banking System (ABS)	1. Control and maintain records of changes to configurations, settings, and software. 2. Establish and enforce procedures for software verification prior to commissioning, including testing (pilot operation) before deployment.	1.5
	3.35	BSS Remote Banking Service System (BSS RBS)		1.44
	2.98	ELMA, CRM, AGC (ADPMS), and AnorHub (MerchantCabinet) Systems		1.35
	2.61	BillMaster, MyAnor EDMS, Superset, and 1C Systems	3. Establish and implement a software change management procedure. 4. Maintain records of software installation tools and media. 5. Maintain records of software updates and implemented changes. 6. Maintain disaster recovery plans and conduct relevant training. 7. Perform scheduled maintenance activities.	1.20
	2.58	Corporate E-mail System		1.18
	2.22	IP Telephony System and Contact Center (Call Center)		0.95
	2.53	File Server		1.13
Disclosure of Information	2.15	Automated Banking System (ABS)	1. Document the responsibilities of users and administrators. 2. Conduct user awareness training regarding accountability and responsibilities. 3. Strengthen accountability for	1.70

Threat Name	Risk Rating	Protected Assets	Planned Measures	Residual Risk
			violations and establish enforcement measures for offenders. 4. Deploy DLP agents on all employee workstations.	
	2.09	BSS Remote Banking Service System (BSS RBS)		1.56
	2.07	ELMA, CRM, AGC (ADPMS), and AnorHub (MerchantCabinet) Systems		1.02
Data Leakage	2.09	Automated Banking System (ABS)	1. Deploy DLP agents on all employee workstations. 2. Establish procedures for granting and managing privileged user access to data repositories. 3. Classify information resources according to information protection levels. 4. Maintain records of media containing protected information.	0.98
	2.09	BSS Remote Banking Service System (BSS RBS)		0.98
Improper Processing or Disposal after End of Use	2.13	Automated Banking System (ABS)	1. Establish and comply with procedures for decommissioning, destruction, and disposal of equipment and information media. 2. Appoint responsible personnel. 3. Apply effective methods for sanitization and destruction of residual information on storage media. 4. Ensure proper storage of information media pending further processing. 5. Monitor compliance with disposal procedures.	1.25
	2.13	Internet Banking and Mobile Banking Systems		1.25

Threat Name	Risk Rating	Protected Assets	Planned Measures	Residual Risk
	2.04	BPM Systems, CRM Systems, Karaf Data Bus, and Artemis		0.98

6. INFORMATION SECURITY THREAT ACTOR MODEL

6.1. The information security threat actor model is developed for the purpose of systematizing information regarding the capabilities and types of actors, the objectives of unauthorized actions, and the development of adequate and sufficient countermeasures against such actions.

When developing the threat actor model, the following shall be taken into account:

- categories of threat actors;
- approaches to assessing the threat level and significance of threat actors, as well as analysis of their technical capabilities;
- restrictive and counteracting measures.

6.2. With respect to the Bank's protected assets, threat actors may include both Bank employees who have direct (physical and/or logical) access to protected assets and employees who do not have such access. In addition, threat actors may include persons who are not employees of the Bank.

6.3. The Bank shall develop an information security threat actor model for the purpose of identifying potential threat actors and assessing their practical and theoretical capabilities to realize information security threats against the Bank's protected assets.

6.4. Internal information security threat actors of the Bank may include:

1) Bank employees who are registered (authorized) users of information systems and networks (direct users);
2) Bank employees who are not users of information systems and networks (facility maintenance personnel, building maintenance personnel, etc.);
3) Personnel responsible for servicing the Bank's technical equipment and having physical access to such equipment;
4) Administrators responsible for maintaining information systems, networks, and information security controls, possessing privileged physical and logical access to protected assets;
5) Bank employees involved in the development of information systems (system designers and software developers);
6) Security personnel (guards) who have physical access to premises and other protected assets, as well as other persons.

6.5. External information security threat actors of the Bank may include:

1) Former employees of the Bank;
2) Visitors who are customers or representatives of third-party organizations (partners, regulatory authorities, etc.);
3) Representatives of third-party organizations performing work under contractual arrangements (contractors, suppliers, developers, etc.), as well as outsourcing service providers;
4) External users having access to the Bank's information systems through external networks or communication channels (customers, partners, shareholders, etc.);

5) Threat actors conducting activities through external networks, as well as other individuals.

6.6. Potential threat actors may be classified according to the following criteria:

1) Experience - the level of expertise in information technology;

2) Capability Level - the level of functional capabilities, rights, and authorities with respect to a protected asset.

6.7. Based on their level of expertise in information technology, potential threat actors are divided into the following categories:

1) Inexperienced User (Category A) - possesses no specialized knowledge regarding the use of standard organizational tools and primarily represents a threat as a source of errors, negligence, or improper actions. Such actions may result in operational disruptions, system failures, and damage to the organization.

2) Knowledgeable User (Category B) - possesses skills in the use of standard tools and may become a source of disruptions affecting protected assets. Attempts to install personal software or use external resources, including the Internet, shall be prevented through access control mechanisms and information security controls.

3) Qualified User (Category C) - possesses an advanced level of knowledge and practical experience in operating technical equipment, programming, designing, and operating information systems, as well as knowledge of the structure, functions, and operational mechanisms of information security controls, including their strengths and weaknesses.

6.8. Based on potential capabilities, a threat actor may be assigned to one of four capability levels:

1) Level One (Low Capability) - characterized by the ability to execute tasks from a predefined set of information processing functions.

2) Level Two (Medium Capability) - includes the capabilities of Level One and the ability to independently develop and execute custom programs with additional information processing functions.

3) Level Three (High Capability) - includes the ability to manage the operation of a protected asset, including influencing system software, its composition, configuration, and operation.

4) Level Four (Very High Capability) - includes all capabilities of personnel responsible for the design, implementation, and maintenance of technical components of protected assets, including the ability to introduce software and hardware tools with new information processing functions into the hardware-software environment and security architecture.

6.9. For each potential threat actor, the Bank’s information security threat actor model shall include:

1) experience category;

2) capability level for performing actions;

3) characteristics of the threat actor, including capabilities and anticipated actions;

4) methods, techniques, and tools that may be used to compromise information security;

5) motives of the threat actor (error, negligence, self-affirmation, or personal gain);

6) protected assets that may be targeted;

7) principal restrictive measures (countermeasures) applicable to the threat actor.

6.10. A threat actor may employ the following methods and tools:

1) collection of information and data;

2) passive information interception tools;

3) use of legitimate information system or information security system tools, including exploitation of their weaknesses;

4) use of active attack tools, including modification and connection of additional devices, connection to data transmission channels, insertion of malicious code, and use of specialized software, technological, and service tools.

The Bank’s model of potential threat actors is provided in Table 6.

Table 6. Model of Potential Information Security Threat Actors of the Bank

Model Attribute	Description
1. Employees who are registered (authorized) users of information systems and networks (direct users)	
Experience Category	**Category B (Knowledgeable User)**
Capability Level	**First (Low) Capability Level**
Characteristics	Capable of realizing threats primarily associated with attempts to escalate their own privileges and bypass information security controls. May also be a source of negligent or erroneous actions affecting protected assets. Additionally, they may cause information leakage and disclosure of protected information.
Methods, Capabilities, and Means of Attack	Use of legitimate software and hardware resources of protected assets, means of interaction with such assets, as well as exploitation of their weaknesses or weaknesses in the information security system.
Motives	Error, negligence, or personal gain.
Target Assets	Information systems, networks, workstations, software, and information (electronic data).
Restrictive and Counteracting Measures	Segregation and control of access rights to protected assets; logging and monitoring of employee activities within information systems; reduction and control of information leakage channels; compliance by employees with confidentiality and non-disclosure requirements relating to protected information.

Model Attribute	Description
2. Employees Who Are Not Users of Information Systems and Networks (Building and Facility Maintenance Personnel, etc.)	
Experience Category	**Category A (Inexperienced User)**

Model Attribute	Description
Capability Level	**First (Low) Capability Level**
Characteristics	Their ability to realize threats is limited to obtaining unauthorized physical access to protected assets or committing negligent and erroneous actions that may result in system malfunction or failure.
Methods, Capabilities, and Means of Attack	Information gathering or the use of passive information interception tools.
Motives	Error or negligence.
Target Assets	Any tangible assets of the organization, as well as information in tangible or intangible form (knowledge).
Restrictive and Counteracting Measures	Compliance with requirements governing the placement and protection of assets; implementation of administrative, organizational, and technical measures to prevent unauthorized access; proper personnel selection and assignment; establishment of access control and access management procedures for premises housing protected assets.

Model Attribute	Description
3. Personnel Responsible for Maintaining the Organization's Technical Equipment	
Experience Category	**Category C (Qualified User)**
Capability Level	**Second (Medium) or Third (High) Capability Level**
Characteristics	Have physical access to the technical and software components of protected assets but are not registered users of such assets.
Methods, Capabilities, and Means of Attack	Information gathering, passive interception tools, use of legitimate system tools, or active attack methods and tools.
Motives	Error or self-affirmation.

Model Attribute	Description
Target Assets	Maintained technical assets (information processing and storage systems, network equipment, information security controls), software installed on such equipment, and stored data.
Restrictive and Counteracting Measures	Restriction of physical access to premises housing protected assets; control and supervision of maintenance activities; granting access exclusively to the equipment being serviced; verification of the integrity of equipment configurations and data following completion of maintenance work.

Model Attribute	Description
4. Administrators Responsible for Maintaining Networks, Information Systems, and Information Security Controls	
Experience Category	**Category C (Qualified User)**
Capability Level	**Third (High) or Fourth (Very High) Capability Level**
Characteristics	Possess authorized physical and logical access to protected assets, belong to the group of privileged users, and are considered trusted personnel with extensive capabilities to influence the internal state and operation of protected assets.
Methods, Capabilities, and Means of Attack	Use of legitimate system tools, exploitation of their weaknesses, or application of active attack methods and tools.
Motives	Error, self-affirmation, or personal gain.
Target Assets	The organization’s information systems, technical infrastructure, software, and information processed and stored within such systems.
Restrictive and Counteracting Measures	Logging and monitoring of administrator activities; implementation of a Privileged Access Management (PAM) system; detection, logging, and blocking of attempts to circumvent security controls; enhanced accountability measures applicable to this category of personnel.

Model Attribute	Description
5. Information System Developers (System Designers and Software Developers)	
Experience Category	**Category C (Qualified User)**
Capability Level	**Third (High) or Fourth (Very High) Capability Level**
Characteristics	Have the capability to realize threats associated with errors in application software development or the introduction of undeclared functionalities (“backdoors”) that may disrupt normal system operation, enable unauthorized access, or result in information leakage.
Methods, Capabilities, and Means of Attack	Use of legitimate system tools or active attack methods and tools.
Motives	Error or self-affirmation.
Target Assets	Information system software and the organization’s information systems themselves.
Restrictive and Counteracting Measures	Logging and monitoring of developer activities; source code analysis using static code analysis tools; testing of software functionality, input data, and output data; certification of software products for compliance with information security requirements.

Model Attribute	Description
6. Security Personnel (Security Guards)	
Experience Category	**Category A (Inexperienced User)**
Capability Level	**Fourth (Very High) Capability Level**
Characteristics	Possess authorized physical access to premises and other protected assets.
Methods, Capabilities, and Means of Attack	Use of passive interception tools or legitimate system tools.
Motives	Negligence or personal gain.

Model Attribute	Description
Target Assets	Premises and physical assets of the organization that are subject to physical protection.
Restrictive and Counteracting Measures	Recording and monitoring access to premises (video surveillance, entry and exit logs); enhanced accountability measures; implementation of appropriate personnel screening and selection procedures.

External Threat Actors

Model Attribute	Description
1. Former Employees of the Organization	
Experience Category	Depending on the position previously held
Capability Level	Depending on the position previously held
Characteristics	May use knowledge acquired during their employment regarding protected information, technologies, and technical assets to obtain personal benefit, cause damage to the organization, or commit other unlawful acts.
Methods, Capabilities, and Means of Attack	Information and data gathering, use of active attack methods and tools.
Motives	Personal gain.
Target Assets	Knowledge and confidential information acquired during employment with the organization.
Restrictive and Counteracting Measures	Compliance with post-employment confidentiality and non-disclosure obligations; disabling the use of former user accounts and credentials; mandatory return of information media, access credentials, and other organizational assets and information upon termination of employment.

Model Attribute	Description
2. Visitors Who Are Customers or Representatives of Third-Party Organizations	
Experience Category	**Category A (Inexperienced User) or Category B (Knowledgeable User)**
Capability Level	**First (Low) Capability Level**
Characteristics	Their ability to realize threats is primarily associated with obtaining unauthorized physical access to protected assets.
Methods, Capabilities, and Means of Attack	Passive interception tools or legitimate system tools.
Motives	Personal gain.
Target Assets	Physical assets and information processing facilities that are not adequately protected by physical security measures.
Restrictive and Counteracting Measures	Compliance with requirements governing the placement of protected assets; segregation of premises into security zones; restriction of visitor access to restricted premises and controlled areas; visitor registration and monitoring; mandatory visitor escort procedures; receiving visitors only in areas with a low security classification.

Model Attribute	Description
3. Representatives of Third-Party Organizations Performing Work under Contract (Contractors, Suppliers, Developers, etc.), as well as Outsourcing Service Providers	
Experience Category	**Category B (Knowledgeable User) or Category C (Qualified User)**
Capability Level	**Second (Medium) or Third (High) Capability Level**
Characteristics	Have logical and physical access to protected assets while performing implementation, configuration, maintenance, and support activities for hardware and software. Potentially capable of executing various attack scenarios using specialized tools and techniques.

Model Attribute	Description
Methods, Capabilities, and Means of Attack	Use of active attack methods and tools.
Motives	Personal gain.
Target Assets	Hardware and software components used and maintained by this category of personnel.
Restrictive and Counteracting Measures	Control and supervision of work performance procedures; presence of an authorized representative of the organization during the execution of work; granting access only to assets required for the performance of assigned tasks; compliance with technical requirements during product development; vulnerability testing based on the white-hat hacking approach; verification of the integrity of system configurations and data following completion of work.

Model Attribute	Description
4. External Users Having Access to the Organization's Information Systems through External Networks	
Experience Category	**Category B (Knowledgeable User)**
Capability Level	**First (Low) Capability Level**
Characteristics	Are registered users of the organization's information systems. Potential threats are primarily associated with attempts to escalate privileges and bypass information security controls using legitimate software and technical means.
Methods, Capabilities, and Means of Attack	Use of legitimate software and hardware resources of the protected asset and the means of interaction with it.
Motives	Personal gain.
Target Assets	Information systems to which access has been granted.
Restrictive and Counteracting Measures	Segregation of access rights; access control to protected assets; logging and monitoring of user activities within information systems.

Model Attribute	Description
5. Threat Actors Who Have Obtained Unauthorized Logical Access to Protected Assets through External Networks by Circumventing Security Controls	
Experience Category	**Category C (Qualified User)**
Capability Level	**Second (Medium), Third (High), or Fourth (Very High) Capability Level**
Characteristics	Conduct targeted actions using specialized software and hardware tools or by exploiting system vulnerabilities.
Methods, Capabilities, and Means of Attack	Use of active attack methods and tools.
Motives	Personal gain or self-affirmation.
Target Assets	The organization's local and corporate networks, connected information resources and information systems, as well as information processing, storage, and transmission facilities.
Restrictive and Counteracting Measures	Use of a comprehensive set of hardware and software information security controls designed to prevent and suppress unauthorized activities; identification and remediation of vulnerabilities within the network infrastructure and software.

7. INFORMATION SECURITY CONTROLS

7.1. To establish the Bank's Information Security Management System (ISMS), a comprehensive set of information security measures shall be implemented, including:

- legal measures;
- behavioral and ethical (psychological) measures;
- organizational measures;
- technological measures;
- engineering and technical measures;
- software and technical measures;
- security measures for interaction with external users.

7.2. Legal Measures (Regulatory and Documentation Support Measures)

Regulatory and documentation support measures within the Bank are aimed at establishing a framework of regulatory documents that guide the Bank in managing information security.

The Bank's regulatory framework in the field of information security includes the state standards of the Republic of Uzbekistan specified in Section 1.2 of this Policy, as well as regulatory and internal normative documents of the Bank governing information security matters.

The Bank's regulatory framework in the field of information security shall be developed and maintained by the Information Security Department.

Internal regulatory documents of the Bank in the field of information security shall be developed (updated) by the Information Security Department in cooperation with other relevant structural units of the Bank (the General Security Department, the Information Technology Department, etc.).

Regulatory documents shall be reviewed, approved, and adopted in accordance with the procedures established by the Bank's internal normative documents.

The Bank's information security documentation shall include the following levels of documents:

a) the principal document - the Bank's Information Security Policy;

b) documents defining and classifying protected assets (registers, inventories, classifiers);

c) documents allocating functions and responsibilities (structural unit regulations, job descriptions);

d) documents governing information security management processes and procedures (policies, procedures, rules, regulations, instructions, methodologies);

e) administrative and organizational documents aimed at implementing information security measures (orders, directives, plans);

f) documents establishing requirements for protected assets and security controls (requirements, technical specifications, designs);

g) operational documentation (manuals, operating instructions);

h) documents used to record and confirm the execution of information security procedures and activities (forms, logs, reports, requests, protocols, certificates of completion).

Internal information security documents and the requirements contained therein shall be communicated by the Information Security Department to the relevant Bank employees and shall be mandatory for compliance.

Certain types of internal regulatory documents on information security are provided in the appendices to this Policy.

7.3. Behavioral and Ethical (Psychological) Information Protection Measures

7.3.1. Behavioral and ethical (psychological) information protection measures shall be aimed at:

- creating a healthy moral and psychological climate within the workforce;
- reducing the likelihood of negative behavior and information security violations associated with the human factor;
- eliminating the influence of personal and psychological factors in cases of breaches of information protection requirements;
- ensuring compliance by Bank employees with standards of ethical conduct.

Behavioral and ethical protection measures are preventive in nature and include:

- conducting awareness and educational activities among Bank employees;
- applying disciplinary measures to violators;
- encouraging and incentivizing employees.

7.3.2. Awareness and educational activities shall be conducted by the Information Security Department in the form of specialized training sessions or individual consultations.

Employees of the General Security Department and the Human Resources Department of the Bank may be involved in conducting such activities.

Awareness and educational activities shall be conducted for the purposes of:

- informing employees about existing threats to the Bank’s operations, the potential consequences of their realization, and the liability measures applicable to violators;
- increasing employees’ awareness of the need to comply with the requirements and provisions of the Information Security Policy;
- enhancing employees’ knowledge and sense of responsibility regarding information security;
- fostering the required standards of conduct and ethics among employees that contribute to compliance with information security rules and requirements;
- strengthening cooperation among employees in addressing information security objectives.

Awareness and educational activities shall be conducted both upon hiring employees and throughout the course of their employment.

Such activities shall be carried out separately for the following categories of Bank employees:

- employees who are users of information systems;

- employees responsible for servicing the Bank’s clients;

- employees responsible for the support and maintenance of information systems and resources, as well as the technical and technological components of the Bank’s information infrastructure;

- technical personnel.

7.3.3. Newly hired Bank employees shall undergo information security induction training.

The set of implemented measures shall be aimed at creating conditions under which Bank employees are required to comply with information security rules and requirements, including liability measures for their violation.

By decision of the Bank’s management and authorized committees, disciplinary actions may be imposed on violators within the framework of employment relations in accordance with labor legislation, including a warning, reprimand, or financial penalties stipulated by the employment agreement.

7.3.4. Incentive measures shall be aimed at creating conditions that encourage Bank employees to demonstrate proper and responsible conduct in matters relating to information security.

7.3.5. For the purpose of preventing offenses and eliminating the causes and conditions conducive to their commission, Bank employees shall comply with:

- the Model Rules of Professional Ethics for Civil Servants approved by Resolution No. 595 of the Cabinet of Ministers of the Republic of Uzbekistan dated October 14, 2022, “On Additional Measures to Ensure Compliance by Civil Servants with the Rules of Professional Ethics”;

- the Bank’s Corporate Code of Ethics approved by Protocol No. 7 of the Bank’s Supervisory Board dated February 25, 2021.

7.4. Organizational Measures

7.4.1. Organizational measures shall be aimed at:

- information asset management;

- personnel security, employee awareness raising, and training;

- restriction of physical access to protected assets (physical security);

- protection of confidential information;

- establishment, operation, and development of the information security system and security controls;

- information security incident response;

- security monitoring and assessment.

For the purpose of identifying information assets and determining the corresponding responsibility for their protection, organizational measures for information asset management shall be implemented.

7.4.2. Organizational measures for information asset management shall include:

a) regular inventory of information assets to identify information resources and the associated information processing facilities;

b) accounting of information assets, including the creation and maintenance of an inventory register of such assets;

c) determination of information asset owners, including the designation of information asset owners and the establishment of their duties and responsibilities with respect to the relevant information assets;

d) classification of information assets in accordance with legislative requirements based on their significance, importance, and sensitivity to the Bank, as well as ensuring an appropriate level of protection for such assets;

e) labeling of information assets, including the development and implementation of a set of procedures for labeling information assets in accordance with the classification system adopted by the Bank;

f) acceptable use and management of information assets, including the documentation and implementation of rules governing the acceptable use and management of information assets and related information processing facilities.

7.4.3. Within the Bank, the inventory, accounting, ownership assignment, classification, and labeling of information assets, the maintenance of the information asset register, as well as other information asset management procedures, shall be carried out in accordance with the Information Asset Management Procedure set forth in Appendix 11 to this Policy.

The inventory process for the purpose of identifying protected assets and information assets shall be organized and conducted by the Information Security Department jointly with the General Security Department and the Information Technology Department.

Based on the results of the inventory, amendments and additions shall be made, where necessary, to the list of protected assets, the register of information assets (information resources), and the Bank's list of confidential information. In addition, the inventory results shall be used to determine the list of premises and the composition of technical and software assets located therein.

Categorization and classification of protected assets shall be performed in accordance with the requirements of Uz SS 2814:2014 "Information Technology. Automated Systems. Classification by Level of Protection Against Unauthorized Access to Information" and other applicable regulatory documents.

The classification of protected assets shall be carried out by the Information Security Department.

7.4.4. Organizational measures aimed at ensuring personnel security, enhancing awareness, and providing training within the Bank shall include:

a) upon recruitment:

- establishing qualification requirements for specialists responsible for information security, as well as qualification requirements for employees whose activities are related to information processing and information security processes;

- verifying that candidates' knowledge and competencies meet the qualification requirements and professional skills requirements established by the Bank during the recruitment process;

b) upon employment:

- defining information security responsibilities in employment agreements;

- familiarization with this Policy;

- informing employees of the powers, duties, and responsibilities in the field of information security established by their job descriptions, as well as the incentive measures and disciplinary actions applied by the Bank for non-compliance with information security requirements;

c) during employment:

- awareness raising, education, and training activities;

- retraining and professional development of employees responsible for information security (acquisition of the required competencies);

- verification and assessment of employees' awareness and qualification levels;

- informing employees of the provisions and requirements of this Policy and other information security regulatory documents;

- monitoring employees' compliance with information security procedures and requirements;

- establishing and applying disciplinary measures;

d) upon termination of employment or change of position:

- establishing an obligation not to disclose confidential information for a period of 5 (five) years following the termination of employment of an employee who leaves the Bank or changes position;

- retrieval from departing employees or employees transferred to another position of confidential information, as well as information processing, transmission, and storage facilities used by them during their employment;

- revocation of all logical and physical access rights to the Bank's protected assets for employees who are leaving the Bank or being transferred to another position.

Qualification requirements for specialists responsible for information security, qualification requirements for employees whose activities involve information processing processes, and their functional responsibilities shall be determined by the Information Security Department.

The definition of information security duties and responsibilities in employment agreements, as well as communication of the relevant information to Bank employees, shall fall within the competence of the Human Resources Department.

The Bank shall implement, on a regular basis, awareness-raising, education, and personnel training activities, as well as assessments of awareness and qualification levels in the field of information security.

The Information Security Department shall conduct information security training sessions and seminars for Bank employees in order to enhance their awareness and understanding of their duties and responsibilities.

Verification and assessment of employees' awareness levels shall be carried out through certification, testing, and surveys of Bank employees and individual specialists based on the results of training sessions, educational activities, and seminars conducted by the Information Security Department.

7.4.5. The Bank shall apply disciplinary measures to Bank employees for the following purposes:

- establishing disciplinary liability for persons who violate the Bank's Information Security Policy or established procedures;

- preventing violations of information security requirements by Bank employees;

- holding accountable persons responsible for intentional violations of information security requirements;

- fostering a responsible attitude among employees toward information security matters and encouraging compliance with information security requirements.

7.4.6. Organizational measures aimed at restricting physical access to protected assets (physical security) shall be intended to prevent unauthorized physical access to the Bank's protected facilities, their damage, and other adverse impacts.

Within the Bank's premises, buildings, and structural subdivisions, the physical security perimeters of the Bank's premises shall be clearly defined.

The physical security perimeters of the Bank's buildings and premises shall be divided into the following security zones:

1) *Low-Security Zones (Level 1 Service Areas)* - premises and areas designated for receiving visitors, as well as customer service areas within the Head Office and branch offices;

2) *Medium-Security Zones (Level 2 Service Areas)* - premises and areas accessible only to Bank employees, including office premises of structural subdivisions and the adjacent corridors of the Head Office, IT Office, and branch offices;

3) *High-Security Zones (Level 3 Protected Areas)* - premises and areas accessible only to a limited number of authorized Bank employees, including the data center server room and the Head Office cash vault.

7.4.7. Organizational measures for ensuring physical security within the Bank shall include:

1) With respect to buildings and premises:

- ensuring perimeter security of the Head Office building and principal service points;

- organizing access control procedures (security checkpoints for employee entry/exit, as well as vehicle entry/exit within the Head Office premises);

- locating critical information infrastructure assets as far as reasonably practicable from the boundaries of controlled areas within the Head Office, IT Office, and branch offices;

- issuing material passes for the import and export of assets and property to and from the Head Office and branch office buildings;

- escorting visitors within the Head Office and IT Office buildings (Zone 2) and/or within the service premises of branch offices;

- determining the list of persons authorized to access protected Zone 3 premises.

2) With respect to information processing, storage, transmission, and protection facilities:

- placing such facilities within protected premises;

- installing equipment in locked communication cabinets;

- using locks on equipment enclosures, tamper-evident seals, official seals, security adhesive tapes, security and holographic labels, or other means for detecting unauthorized physical access.

3) With respect to confidential information in paper form:

- using safes, lockable metal cabinets, and other secure storage facilities;

- registering such media in the relevant accounting logs.

4) With respect to power and network cabling:

- implementing organizational measures to protect against damage and unauthorized interference in order to prevent information interception and other harm, as specified in Section 9 of this Policy.

Security of the Head Office building and territorial branch offices shall be provided by the National Guard under contractual arrangements.

Access to the Bank shall be governed by the Bank Access Control Rules approved by Minutes No. 7 of the Bank Management Board dated September 24, 2020.

7.4.8. Organizational measures for the protection of confidential information shall include:

1) defining the list of information constituting the Bank's confidential information and making amendments and additions thereto as necessary;

2) determining the list of Bank employees granted access to the Bank's confidential information;

3) obtaining confidentiality undertakings from Bank employees regarding the non-disclosure of the Bank's confidential information;

4) defining in agreements concluded with the Bank's counterparties the conditions, requirements, obligations, and liabilities related to the disclosure or non-disclosure of confidential information, as well as entering into Non-Disclosure Agreements (NDAs);

5) applying confidentiality markings to confidential information and its physical media;

6) registering and maintaining records of media containing confidential information;

7) establishing restrictions and/or protection requirements for the transmission of confidential information through local, corporate, and external networks, electronic mail, electronic document management systems, and establishing restrictions on the dissemination of confidential information through Internet resources, social media platforms, mass media, and other sources;

8) establishing restrictions and/or protection requirements for the storage of confidential information in paper and electronic form on information processing facilities, electronic media, mobile devices, and other storage media;

9) defining procedures for access to and use of confidential information;

10) determining the list of premises in which confidential information is processed and stored and establishing requirements for their protection against unauthorized physical access;

11) identifying information systems used for processing and storing confidential information in electronic form and establishing requirements for their protection against unauthorized logical access;

12) establishing requirements for the return of physical media containing confidential information upon the termination of employment or transfer of Bank employees to another position;

13) ensuring monitoring of compliance with confidential information protection requirements.

Activities involving information subject to protection shall be carried out in accordance with the Instruction on the Procedure for Registration, Handling, and Storage of Documents, Files, and Publications Containing Restricted-Distribution Information That Is Not Classified as Confidential, approved by the decision of the Deputy Prime Minister of the Republic of Uzbekistan dated December 5, 2006, as well as the Instruction on the Procedure for Registration, Maintenance, and Storage of Documents and Files Containing Restricted-Distribution Information (For Official Use Only), approved by Minutes No. 32 of the Bank Management Board dated December 2, 2022.

When processing confidential information, Bank employees shall be guided by the Regulation on Compliance with the Commercial Secret (Confidentiality) Regime, approved by Minutes No. 32 of the Bank Management Board dated December 2, 2022, as well as the Regulation on the Procedure for Processing Personal Data of Employees of JSC "Anor Bank", approved by Minutes No. 7-1 of the Bank Management Board dated May 16, 2023.

7.4.9. For the purpose of establishing, operating, and developing the information protection system and security controls, the following organizational measures shall be implemented:

a) procurement of information security controls as part of the implementation of the Bank's information security measures;

b) determination of technical requirements for the information security controls to be acquired;

c) implementation of organizational measures to prepare for the deployment and maintenance of the information protection system and security controls, including the allocation of premises, development of operating procedures, designation of responsible employees, and training of such employees in the operation of the relevant systems and controls;

d) conducting pilot operation and acceptance testing during the implementation of information security controls;

e) management of the information protection system, including configuration and settings control, restoration of operability, installation of software updates, maintenance of operational documentation, monitoring of information security incidents, performance of control procedures, and documentation of control results;

f) preparation and submission of proposals for improving the information protection system where deficiencies in its operation are identified or where an enhanced level of protection is required.

The organizational measures specified in this clause relating to the establishment, operation, and development of the information protection system and security controls within the Bank shall be implemented by the Information Security Department in cooperation with the Information Technology Department.

7.4.10. The Bank shall implement organizational measures for responding to information security incidents as provided for in Section 8 of this Policy.

Organizational measures for security monitoring and assessment shall be applied for the following purposes:

- identifying vulnerabilities and deficiencies in the Information Security Management System (ISMS);
- objectively assessing the level of protection of protected assets against information security threats;
- determining the compliance of the Information Security Management System and the information protection methods and controls implemented within its framework with the requirements of this Policy and applicable regulatory documents;
- assessing the effectiveness of implemented information security measures and controls;
- evaluating the Bank's achievement of information security objectives and other related purposes.

For the purpose of security monitoring and assessment, the following organizational measures shall be carried out:

1) conducting internal and external audits to assess the level of protection of protected assets and to evaluate the relevance and effectiveness of this Policy;
2) assessing the effectiveness of implemented organizational, technical, and other security measures, as well as eliminating deficiencies identified as a result of audits.

Internal audits shall be conducted at least once a year, and external audits shall be conducted at least once every three years.

Internal audits shall be conducted by the Information Security Department, with the involvement, where necessary, of specialists from the General Security Department and the Information Technology Department.

External information security audits shall be conducted by external organizations authorized to perform such audits.

The results of inspections and audits shall be documented. The relevant documentation shall include:

- identified vulnerabilities, deficiencies, and non-conformities;
- causes of the identified non-conformities;
- the need for corrective measures to achieve compliance and a list of such measures;
- assessment of the effectiveness of information security measures and controls, as well as other audit and inspection results.

Based on the results of audits and other inspections, the Information Security Department shall develop and implement measures to remediate identified

vulnerabilities, deficiencies, and non-conformities, and to improve the effectiveness of information protection.

7.5. Technological (Technical) Measures

7.5.1. Technological (technical) information security measures of the Bank shall be aimed at:

- ensuring secure data storage and protecting data against leakage, loss, theft or loss of storage media and data storage devices, as well as data corruption;
- ensuring the reliable, resilient, and secure operation of protected assets;
- protecting protected assets against disruptions to the continuity of their operation;
- ensuring the protection of protected assets against environmental impacts, natural disasters, and emergency situations;
- ensuring the prompt restoration of the functioning of protected assets in emergency situations.

7.5.2. The Bank shall implement measures to ensure secure data storage and protect data against leakage, loss, theft or loss of storage media and storage devices, as well as against data corruption, in accordance with the requirements of DSt ISO/IEC 27040:2018 “Information Technology — Security Techniques — Storage Security.”

The information security measures shall include:

- protection of storage facilities and information media against unauthorized access;
- proper and controlled destruction of information media and data storage devices;
- ensuring the physical protection of data storage devices;
- use of authentication and access monitoring mechanisms for data storage devices;
- regular backup of data stored on storage devices.

To ensure reliable data protection, the Bank shall implement the following technical (technological) measures:

- distribution of critical data storage resources;
- data backup;
- remote fault-tolerant online mirroring of data from critical information systems;
- clustering of fault-tolerant applications and related systems around a single copy of data;
- long-term storage of corporate confidential information;
- distribution of databases and file systems;
- provision of data storage for operational recovery (from backups) and archiving purposes.

As part of the data resilience strategy, the following measures shall be implemented:

- inclusion of data recovery measures in disaster recovery plans;
- storage of backup copies of data in facilities geographically remote from the locations where primary data are stored.

Technological (technical) information protection measures related to operation, administration, maintenance, configuration, and destruction of data shall include:

- performing activities aimed at ensuring the continuous operation of data storage facilities;
- activities of administrators related to monitoring and allocation of storage infrastructure resources, as well as performing all actions necessary for the management of data storage systems;
- carrying out maintenance activities related to the repair and modernization of equipment and systems;
- installation of specialized software profiles and preparation of systems for operation;
- implementation of data destruction measures intended to preserve the confidentiality of information when information media are decommissioned or modified in such a manner that access to the information stored thereon becomes impossible.

7.5.3. The following data shall be subject to protection:

- the Core Banking System (CBS) database;
- databases of the information systems RBS BSS, ELMA, Wings, BillMaster, AGC (ADPMS), AnorHub, Qlik Sense, Confluence, GitLab, Jira, Keycloak, MerchantCabinet, ServiceDesk, Verifix, WEBIM, Superset, IC, and other information systems;
- databases of information exchange systems, including the corporate e-mail system, corporate messenger, and electronic document management system;
- the database of the Bank’s official website;
- configurations and databases of the domain controller server;
- configurations and databases of information security tools, including firewalls, intrusion prevention systems (IPS), data loss prevention (DLP) systems, real-time monitoring tools, antivirus solutions, and other information security controls;
- network equipment configurations.

The above-mentioned data shall be stored in server-based storage systems, while backup copies thereof shall be maintained in data storage systems, backup database servers, and magnetic tape media (electronic archive).

7.5.4. For the storage of backup copies of data and information system resources specified in Clause 7.5.3 of this Policy, the Bank shall use a data storage system connected to a Storage Area Network (SAN).

To ensure the reliability and integrity of information system data stored on servers and within the data storage system, RAID technology shall be utilized.

7.5.5. To ensure the physical protection of data, all servers, data storage systems, and tape drives shall be located in physically secured server rooms within the Bank’s primary and backup data centers, access to which shall be restricted to unauthorized persons.

The Core Banking System (CBS) shall provide remote fault-tolerant online mirroring of application servers and database servers.

The primary CBS servers shall be located in the primary data center (the Bank's Head Office), while the backup CBS servers shall be located in a geographically remote backup data center (JSC "Uzbektelecom" Data Center, ATS-233, Tashkent).

The database of the primary CBS server shall be continuously replicated to the backup CBS database server located in the backup data center.

The databases of the primary and backup CBS data centers shall be interconnected via a dedicated fiber-optic communication link (FOCL) established directly between the respective data centers.

7.5.6. The SAN storage network shall be built on Fibre Channel (FC) technology, to which all primary database servers and other information system servers, data storage systems, tape drives, and backup and recovery systems may be connected.

The SAN network shall be deployed within the server room of the primary data center using two SAN switches.

In addition, a Demilitarized Zone (DMZ) shall be established within the primary data center as a separate VLAN segment hosting servers of information systems, information resources, and information exchange systems connected to the external Internet network, including:

- corporate e-mail services;
- the Bank's official website;
- Internet banking resources;
- the mobile banking system.

7.5.7. For the long-term storage of backup copies of critical information systems, the Bank shall use tape-based data storage media (a tape library).

An electronic archive of servers and databases of critical information systems shall be maintained using tape media. The retention period for the electronic archive shall be not less than 1 (one) year.

7.5.8. Bank employees shall connect to information systems through the Head Office local area network (LAN).

Employees of the remote IT Office and branch offices shall connect to the Bank's information systems through the corporate network using secure IPSec VPN channels established between the IT Office, branch offices, and the Head Office.

When accessing information systems, users shall be authenticated through the domain controller server and the respective information systems using a username and password.

User access to the Bank's information systems shall be established through secure HTTPS connections.

7.5.9. Each information system of the Bank shall have designated information system administrators and a database administrator, who shall be employees of the Information Technology Department.

The designated administrators shall be responsible for:

- configuring and administering information system servers, server storage systems, and data storage systems, including viewing and modifying all related parameters;

- modifying account creation and management rules, creating roles and assigning privileges and permissions to information system users;

- verifying parameters and configurations of server storage systems and data storage systems, as well as reviewing operational and failure logs;

- performing backup and restoration of information system server data;

- verifying the integrity of data stored in storage systems using database integrity control mechanisms.

The Information Security Department shall perform the functions of a security auditor for information system data repositories, including conducting security analyses that enable:

- analysis of user access rights and privileges;

- verification of security parameters and configurations;

- review of audit logs.

7.5.10. The administrators specified in Clause 7.5.9 of this Policy shall access information systems remotely through the local area network or corporate network using secure SSL VPN connections established through a VPN gateway. Administrator connections shall be performed through secure connections established using the SSH protocol.

When accessing information systems, administrators shall be authenticated through the SSH protocol and by using a username and password directly within the information system, server operating system, or database management system.

In addition, when accessing information systems, administrators shall be authenticated through the Privileged Access Management (PAM) system. The PAM system shall be used to control administrator access to information system servers and databases and to monitor their activities.

7.5.11. Security auditing, logging, and monitoring shall be performed with respect to information system data repositories, including:

- logging of all significant events occurring within the data storage system;

- retention of event log data;

- archiving and retention of event log data in accordance with the data retention policy;

- synchronization of system time on devices with a reliable external time source.

The standard Syslog protocol (a standard mechanism for transmitting and recording system event messages) shall be used for event logging and recording within data repositories.

Security auditing, logging, and monitoring of data repositories shall be performed by the Information Security Department, including through the use of server operation monitoring systems and the SIEM (Security Information and Event Management) system.

Identified violations of the secure data storage policy shall be recorded in the Information Security Incident Register.

7.5.12. Data destruction on information media and data storage devices shall be carried out in accordance with the Information Security Rules for Handling

Information Media, Mobile Devices, and Data Storage Devices set forth in Appendix 7 to this Policy.

7.5.13. To strengthen the protection of information system data stored on servers and data storage systems, information system administrators shall additionally be required to implement the following measures:

- removal of unnecessary and unused software;
- removal of unused user accounts;
- renaming, deleting, or changing passwords of built-in and default accounts;
- opening only those network ports required for operational purposes;
- installation of current security updates (patches) obtained from trusted sources;
- updating firmware obtained from trusted sources;
- implementation and maintenance of anti-malware protection mechanisms.

7.5.14. To ensure the stable and uninterrupted operation of protected assets, the following measures shall be implemented:

1) carrying out appropriate maintenance activities (functional monitoring, preventive maintenance, and repairs) to ensure the continuous availability and integrity of equipment;

2) documenting operational processes related to equipment opening, repair, commissioning, backup procedures, configuration changes, and other similar activities;

3) maintaining and analyzing equipment and information system logs;

4) proper change management for information processing facilities and systems, the failure of which may result in malfunctions, disruptions, or security incidents;

5) performance and capacity management, including planning and forecasting future requirements, monitoring resource utilization, and provisioning reserve resources and additional capacity;

6) segregation of development, testing, and production environments, whereby development and testing activities shall be conducted on equipment isolated from production systems;

7) provision of redundancy for information processing, storage, transmission, and protection facilities;

8) backup of data and software;

9) software management, including installation, modification, configuration, and updating;

10) establishment of rules prohibiting eating, drinking, and smoking in the immediate vicinity of information processing assets.

7.5.15. The following technical assets shall be subject to redundancy:

- servers of the Core Banking System (CBS) and other information systems (database servers and application servers);
- the core switches used to support the corporate network infrastructure;
- firewalls and security gateways deployed at the connection points of the primary and backup data centers to the corporate network, the external Internet network, and the Central Bank’s Banking Telecommunication Network (BTN).

Requirements for the redundancy of information processing, storage, transmission, and protection facilities, as well as communication channels, shall be established by the Business Continuity and Emergency Recovery Procedure set forth in Appendix 14 to this Policy.

The following shall be subject to backup:

- databases and audit logs (log files);
- software of the Bank's information systems;
- configuration parameters (settings) of network equipment and information security controls.

Within the Bank, data backup and recovery, as well as updating of system and application software, shall be carried out in accordance with the Data Backup and Recovery Regulation set forth in Appendix 4 to this Policy.

The backup and recovery systems specified in Appendix 18 to this Policy shall be used to ensure data backup.

7.5.16. To ensure uninterrupted power supply, the following measures shall be implemented:

1) diesel generators and uninterruptible power supply (UPS) systems shall be used in the Head Office building (primary data center) and service points;

2) measures shall be implemented to ensure the continuous operation of key information systems, information exchange systems, network equipment, and information security controls located in the backup data center (JSC "Uzbektelecom" Data Center, ATS-233) through the use of diesel generators and uninterruptible power supply systems.

Communication channels used to connect the Bank's corporate network to the external Internet network and the Central Bank's Banking Telecommunication Network (BTN) shall be redundant.

Primary telecommunications equipment, databases, information system servers, and information security controls shall be deployed in both the primary and backup data centers.

The JSC "Uzbektelecom" Data Center (ATS-233) used as the backup data center, as well as the primary data center server room located in the Head Office building, shall comply with the requirements of O'zDSt 2875:2014 "Requirements for Data Processing Centers", including:

- ensuring uninterrupted power supply;
- maintaining required environmental conditions (air-conditioning systems);
- ensuring fire safety.

7.5.17. Recovery activities shall include:

1) development, training, and testing of recovery plans;

2) commissioning of backup equipment, communication channels, communication lines, or power supply sources in the event of an emergency situation;

3) restoration of software and data from backup copies;

4) repair or replacement of equipment;

5) restarting or reinstalling software and performing other similar recovery activities.

The procedure for implementing recovery activities shall be governed by the Business Continuity and Emergency Recovery Plan set forth in Appendix 14 to this Policy.

7.6. Engineering and Technical Measures

7.6.1. Engineering and technical measures are aimed at preventing unauthorized persons from gaining physical access to protected assets or creating physical barriers to such access and include the following measures:

1) defining access boundaries to zones and service premises of the Head Office by means of doors and other engineering and technical controls;

2) using employee identification cards or biometric identification mechanisms (Face ID), as well as keypad locks, for access to the Head Office building and premises equipped with an Access Control and Management System (ACMS), including individual service rooms and corridors leading to such premises;

3) using metal doors at entrances to Zone 3 premises;

4) using electronic locks at entrances to Zone 2 service premises;

5) using monitoring and technical alarm system sensors on doors and windows of the Head Office;

6) equipping windows of the Head Office, IT Office, and service points with visual protection measures (curtains, blinds) to prevent visual observation;

7) using video surveillance systems to monitor the premises of the Head Office, the IT Office, and the corridors and premises of service points;

8) installing security alarm systems and sensors in protected premises to detect unauthorized physical access;

9) using lockable fire-resistant metal cabinets for the storage of documented confidential information.

7.7. Hardware and Software Measures

7.7.1. Hardware and software information security measures shall be aimed at:

- implementing technical protection of information;
- implementing cryptographic protection of information.

7.7.2. Hardware and software measures shall be based on the use of hardware, software, and technical information security controls designed to ensure:

- information security at the network infrastructure level (network security);
- segregation and management of logical access to protected assets;
- anti-malware protection;
- protection of confidential information against leakage;
- security monitoring and analysis;
- monitoring and management of information security incidents; and
- other information security functions.

7.7.3. Network security measures shall include:

1) defining a secure architecture for the Bank’s network infrastructure;

2) physical and virtual segmentation of the Bank’s network;

3) use of network security controls (firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), VPN solutions, and Web Application Firewalls (WAF));

4) establishment of secure communication channels and network connections.

7.7.4. The secure architecture of the corporate network, the principles of its design, and the procedures for establishing secure communication channels and network connections shall be defined by the Regulation on the Organization of the Corporate Network and Secure Network Connections set forth in Appendix 1 to this Policy.

7.7.5. Security of the network infrastructure and the use of firewalls shall be ensured in accordance with the Regulation on Information Security at the Network Infrastructure and Firewall Level set forth in Appendix 2 to this Policy.

7.7.6. Taking into account information security risks associated with network attacks and threats, the Bank shall use hardware and software IDPS (Intrusion Detection and Prevention System) solutions meeting the following requirements and functional capabilities:

- support for SD-WAN and VPN technologies for distributed networks and remote users;
- deep packet inspection (DPI) of network traffic across all protocols, including application-layer protocols;
- sufficient performance to process and transmit all external network traffic while applying deep packet inspection;
- support for signature-based detection of network intrusions within network traffic;
- capability to update signature databases from the manufacturer;
- support for behavioral detection of network intrusions based on network traffic anomalies and deviations in protocol behavior;
- blocking and filtering of suspicious traffic;
- protection against web-based threats, including DNS-based threats and malicious URLs;
- application control functionality;
- detection and prevention of DoS and DDoS attacks;
- detection and filtering of network traffic containing malicious code;
- integrity monitoring functions for protected network objects within the IDPS environment;
- support for the Simple Network Management Protocol (SNMP);
- generation of alerts regarding detected and prevented attacks.

The IDPS solution shall provide protection of local networks against threats originating from external and corporate networks.

The Bank shall use IDPS capabilities integrated into firewalls, namely hardware and software firewalls with embedded IDPS functionality.

Firewalls with IDPS functionality shall be used for:

- external protection of the Head Office local area network when connected to external networks, as well as protection of the local networks of the backup data center and IT Office when connected to external networks;

- external protection of the Head Office local area network when connected to the corporate network, as well as protection of the local networks of the backup data center and IT Office when connected to the corporate network;

- internal protection of the primary data center DMZ, the server segments of the primary and backup data centers, and the processing center of the primary data center when connected to local networks.

7.7.7. The Bank shall deploy Host-based Detection and Prevention System (HDPS) solutions on workstations and critical servers that provide the following functions:

- detection of malicious activity through monitoring of processes, applications, files, and operating system registries;

- monitoring of inbound and outbound network traffic;

- configuration of security settings for specific ports, applications, and IP addresses;

- protection against network attacks and analysis of suspicious network activity;

- support for multi-platform environments and protection of file servers operating on Linux and Windows platforms, including clustered servers;

- protection against attacks involving malicious software;

- vulnerability scanning and detection.

As an HDPS solution, the Bank shall use its anti-malware protection system equipped with additional HDPS functionality.

To ensure the effective operation of the HDPS, anti-malware software shall be appropriately configured on workstations and servers.

7.7.8. For the purpose of controlling access to the Bank’s information resources and information systems, an Access Control Matrix shall be developed in accordance with the Rules for Developing an Access Matrix for Information Resources set forth in Appendix 8 to this Policy.

7.7.9. Within the Bank, user authentication when accessing protected assets shall be performed using passwords and other identifiers in accordance with the Instruction on Password Protection and User Authentication in Information Systems set forth in Appendix 5 to this Policy.

7.7.10. The following anti-malware protection measures and controls shall be implemented by the Bank:

1) deployment of malware protection solutions (anti-malware software) on information processing facilities, including mobile devices, capable of detecting, blocking, and recovering from malware-related incidents, as well as notifying users of identified threats;

2) adoption of an Anti-Malware Protection Policy establishing mandatory malware protection requirements for all Bank employees;

3) identification and remediation of vulnerabilities that may be exploited by malicious software;

4) blocking the use of USB ports on information processing facilities.

7.7.11. The processes for organizing and maintaining anti-malware protection, as well as the procedures for establishing and enforcing employee

compliance with malware protection requirements, shall be governed by the Anti-Malware Protection Instruction set forth in Appendix 6 to this Policy.

7.7.12. The Bank shall use the following technical information security controls:

- a vulnerability management system and corporate infrastructure security scanners shall be used as security monitoring and assessment tools;
- a Data Loss Prevention (DLP) system shall be used to protect confidential information against leakage;
- a Security Information and Event Management (SIEM) system shall be used for monitoring and managing information security incidents;
- a Privileged Access Management (PAM) system shall be used to monitor and control the activities of privileged users (administrators);
- cryptographic protection of information shall be implemented using Cryptographic Information Protection Tools (CIPTs).

The technical information protection methods and controls used by the Bank shall be determined by the Rules for Organizing Technical Information Protection set forth in Appendix 23 to this Policy.

7.7.13. Within the Bank, cryptographic information protection tools shall be used when providing digital banking services to the Bank's corporate customers through the BSS DBO Internet Banking System for the generation and verification of Electronic Digital Signatures (EDS), as well as by Bank employees when using the MyAnor.uz Electronic Document Management System.

For the use of EDS within the BSS DBO system, corporate customers of the Bank's digital banking services shall use EDS private keys and EDS public key certificates issued by the Electronic Digital Signature Key Registration Center of the State Tax Committee of the Republic of Uzbekistan.

Within the MyAnor.uz Electronic Document Management System, Bank employees shall likewise use EDS private keys and EDS public key certificates issued by the Electronic Digital Signature Key Registration Center of the State Tax Committee of the Republic of Uzbekistan.

Cryptographic information protection tools shall also be used within the secure e-mail system utilized by employees of the Bank's Secretariat Department.

In addition, cryptographic information protection tools shall be used to establish secure network connections within the Bank's corporate network and when interacting with third-party information systems.

The Bank shall use only those cryptographic information protection tools that have been certified by the authorized certification body for cryptographic information protection tools in accordance with Resolution of the President of the Republic of Uzbekistan No. PD-614 dated April 3, 2007.

The application of cryptographic information protection methods and tools within the Bank shall be carried out in accordance with the Instruction on the Organization of Cryptographic Information Protection set forth in Appendix 13 to this Policy.

7.7.14. The list of hardware, software, information security controls, network and server equipment, and software used by the Bank is provided in Appendix 18 to this Policy.

7.8. Security Measures for Interaction with External Users

7.8.1. For the purpose of protecting the Bank's information assets, information security measures shall be applied when interacting with third-party organizations and when working with clients who are granted access or the possibility of obtaining access to the Bank's information assets.

Third-party organizations may be granted both physical and logical access to the Bank's information assets, whereas the Bank's clients may obtain access to the Bank's information assets exclusively at the logical level.

The Bank acknowledges that granting such access, or the possibility of obtaining such access, may result in a breach of information security or a reduction in the level of information security.

7.8.2. Information security measures shall be considered in the following cases of interaction with third parties:

1) when services are provided or work is performed by third parties (contractors, suppliers, and other organizations);

2) when a Bank information system interacts with an information system of a third-party organization;

3) when receiving representatives of external organizations and conducting meetings with them.

7.8.3. Information security measures shall also be established for clients using digital banking services (online services).

7.8.4. When interacting with third-party organizations that provide services or perform work, the Bank shall implement the following information security measures:

1) prior to entering into an agreement, define requirements applicable to the third-party organization and its personnel who will be granted access to, or authorized to work with, the Bank's protected assets;

2) incorporate information security requirements into agreements concluded with third-party organizations;

3) execute separate confidentiality agreements with third-party organizations or include relevant confidentiality provisions within contractual agreements;

4) determine the list of information and protected assets to which the third-party organization will be granted access in the course of providing services or performing work, as well as identify the employees of the third-party organization who will receive such access;

5) establish procedures for granting access to third parties, specifying the types of access and the procedures for granting such access;

6) communicate the Bank's information security requirements to the personnel of the third-party organization before the commencement of work;

7) prior to granting access to information and protected assets, ensure the implementation of appropriate security controls and physical and/or logical access control mechanisms;

8) ensure physical segregation between information processing facilities managed by the Bank and information processing facilities managed by the third-party organization;

9) monitor, control, and manage the third-party organization's access to information processing, transmission, and protection facilities;

10) ensure the continuous presence of a Bank employee while the third-party organization performs work on protected assets;

11) provide the third-party organization with unique access identifiers that prevent the use of privileged access rights known to Bank employees;

12) upon completion of the work performed by the third-party organization, revoke the granted access rights, verify data integrity, and review equipment configurations;

13) approve the use and placement of technical equipment owned by the third-party organization.

The above measures, the procedures for their implementation, and any other information security requirements of the Bank shall be defined in the agreement concluded with the third-party organization.

The Non-Disclosure Agreement (NDA) concluded with a third-party organization shall establish confidentiality obligations and the liability of the third-party organization in the event of disclosure of confidential information through its fault, including compensation for damages incurred by the Bank as a result of such disclosure.

The requirements of the NDA shall remain binding throughout the entire term of the agreement and for a period of not less than 5 (five) years following its termination.

7.8.5. When a Bank information system interacts with an information system of a third-party organization, or when employees of a third-party organization are granted access to the Bank's information system, the following information security measures shall be applied:

1) establishing information security requirements for the connection of the third-party information system and/or its personnel;

2) implementing security measures and controls by the Bank to prevent unauthorized logical access by the third-party organization to the Bank's information systems;

3) establishing secure connections for information exchange and implementing other necessary security measures.

The above measures shall be formalized in bilateral agreements concluded between the parties.

The establishment of secure connections shall be carried out in accordance with the requirements of the Regulation on the Organization of the Corporate Network and Secure Network Connections set forth in Appendix 1 to this Policy.

When connecting third-party organizations and their information systems to the Bank's information systems, firewall protection measures shall be applied in accordance with the Regulation on Information Security at the Network Infrastructure and Firewall Level set forth in Appendix 2 to this Policy.

7.8.6. When the Core Banking System (CBS) interacts with information systems of third-party organizations, the following measures shall be applied:

a) connection of the CBS to information systems of third-party organizations shall be carried out through the Central Bank Banking Telecommunication Network (BTN);

b) connection of the CBS to external communication channels for interaction with information systems of third-party organizations shall be implemented through firewalls and IDS/IPS controls;

c) secure IPSec VPN channels shall be established when connecting the CBS to external information systems.

7.8.7. When receiving and conducting meetings with representatives of third-party organizations, the Bank shall implement the following measures to prevent unauthorized physical access to the Bank's protected assets:

a) meetings with representatives of third-party organizations shall be conducted in reception areas (Bank meeting rooms) or in specially designated premises located at a distance from the Bank's protected zones and having an enhanced level of security;

b) representatives of third-party organizations shall be escorted by Bank employees while present within the Bank's premises;

c) restrictions shall be imposed on granting representatives of third-party organizations the right to use workstations connected to the Bank's local or corporate network or the Bank's information systems, as well as restrictions on connecting their devices to the Bank's network and information systems.

7.8.8. The following information security measures shall be applied when working with clients:

- establishing and implementing information security requirements that are mandatory for clients when using digital banking services;
- defining the allocation of responsibilities between the Bank and its clients in relation to the use of digital banking services;
- providing users with authorized methods of access, as well as establishing procedures for the management and use of unique user identifiers and passwords;
- revoking access rights in the event that a user violates information security requirements;
- informing users of the risks arising from non-compliance with information security requirements when using digital banking services.

The above security requirements, as well as the risks associated with non-compliance therewith, shall be reflected in agreements concluded with clients.

7.8.9. Requirements for implementing information security measures when interacting with third-party organizations and working with clients shall be established by the Information Security Department.

The Information Security Department shall also monitor compliance with such requirements by the Bank's structural units and employees.

8. INFORMATION SECURITY INCIDENT RESPONSE

8.1. One of the key processes of the Bank's integrated Information Security Management System (ISMS) is the information security incident management process.

The Bank shall apply a consistent, effective, and systematic approach to information security incident management.

The objectives of information security incident management within the Bank are as follows:

- minimizing losses and damages incurred by the Bank as a result of information security incidents;
- taking prompt and effective measures to contain incidents, mitigate threats, and eliminate their consequences within the shortest possible time;
- deriving lessons learned from incidents, reducing the likelihood of their recurrence, and preventing similar incidents in the future;
- minimizing the adverse impact of incidents on the Bank and its operations;
- ensuring integration of the incident response process with relevant elements of crisis management and business continuity management, including processes for interaction with external organizations;
- identifying and assessing information security vulnerabilities and ensuring their timely remediation in order to prevent or reduce the number of incidents associated with such vulnerabilities.

The established objectives of information security incident management shall be communicated to employees responsible for information security incident management and shall be used as priorities when responding to incidents.

8.2. The Bank shall apply the following information security incident management procedures:

a) incident monitoring and detection;

b) incident analysis, assessment, and reporting;

c) incident recording and registration;

d) incident notification and communication;

e) threat containment or termination of the threat that caused the incident;

f) incident impact assessment;

g) post-incident recovery and remediation of consequences;

h) incident analysis and determination of root causes;

i) development and implementation of measures to prevent recurrence of incidents;

j) collection, analysis, and preservation of evidence, as well as the conduct of investigations;

k) holding accountable the persons responsible for the occurrence of the incident and its consequences.

8.3. All protected assets defined in Section 4 of this Policy shall be subject to monitoring.

Monitoring shall be conducted for the purpose of detecting information security incidents and shall be performed on a 24/7 basis.

The sources of information regarding information security incidents affecting protected assets shall include:

- data generated by the Information Security Incident Monitoring and Management System (hereinafter referred to as the SIEM System);
- data from system logs (audit logs and log files) of information systems, equipment, and software;
- data obtained from information security controls;
- results of visual inspections of the operational status of equipment and the Bank's corporate network infrastructure, information resources, and information systems;
- results of internal and external information security audits;
- information and reports received from Bank employees;
- requests, complaints, and reports received from the Bank's clients and third-party organizations interacting with the Bank;
- identified cases of theft, cyberattacks, information leakage, unauthorized access, and other information security violations.

Monitoring shall be carried out by employees of the Information Security Department, the General Security Department, and the Information Technology Department of the Bank.

For monitoring and detecting information security incidents, the Bank shall use the SIEM System specified in Appendix 18 to this Policy.

8.4. Analysis and assessment of an information security incident shall be conducted for the purpose of determining whether the relevant event should be classified as an information security incident.

Within the Bank, the following events shall be classified as information security incidents:

1) emergencies and disaster situations (man-made threats, natural disasters, civil disturbances, and other similar events);
2) disruptions in the operation and functioning of the Bank's information systems, including failures of server and network equipment and software malfunctions;
3) breaches of the confidentiality, integrity, and availability of the Bank's confidential information, as well as violations of information protection requirements;
4) theft, attacks, information leakage, and other unauthorized actions resulting in material damage, including cases involving loss or theft of assets, funds, information media, and confidential information;
5) disruption of connectivity with external networks, failures of the Bank's corporate and local networks, technical malfunctions of network equipment, damage to communication cable infrastructure, and other similar events;

6) failure of information security controls for any reason, including technical malfunctions and errors caused by human factors;

7) unauthorized physical or logical access by third parties to the Bank's information systems and information resources;

8) DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks;

9) network attacks detected by information security controls;

10) detection of dangerous computer viruses and malicious software;

11) unauthorized connection of devices and network nodes to local and corporate networks;

12) unauthorized entry of unauthorized persons into protected premises;

13) detection of unlawful activities involving the collection, copying, extraction, or exfiltration of information.

The Information Security Department shall be responsible for the analysis and assessment of information security incidents, their classification as information security incidents, and the determination of their criticality level.

8.5. All information security incidents occurring within the primary and backup data centers, as well as within the Bank's Head Office, IT Office, and branch offices, shall be subject to mandatory recording.

Recording of identified information security incidents shall be performed through the SIEM System.

For information security incidents not detected by the SIEM System, a separate electronic database of information security incidents shall be maintained.

The Information Security Department shall be responsible for recording identified information security incidents and maintaining the Bank's electronic database of information security incidents.

The format of the electronic information security incident database is set forth in the Information Security Incident Response Procedure contained in Appendix 15 to this Policy.

The recording of information security incidents is necessary for determining the causes of their occurrence, conducting incident analysis, and performing information security risk assessments within the Bank.

Information security incidents assigned a "High" Criticality Level shall be subject to separate registration.

For the registration of such incidents, information relating thereto shall be entered into the Bank Security Emergency Register, the format of which is established by the Information Security Incident Response Procedure set forth in Appendix 15 to this Policy.

The Information Security Department shall be responsible for registering information security incidents with a "High" Criticality Level and for maintaining the Bank Security Emergency Register.

8.6. The following parties shall be notified of information security incidents:

- management of the Bank's structural units responsible for the operational site or business process affected by the incident;

- management of the structural unit, or the specialist (administrator), responsible for supporting the affected protected asset;

- the Bank's management;

- external interested parties and organizations.

8.7. The threat that caused the incident shall be contained or neutralized in order to minimize damage, facilitate recovery of operations, and ensure the continuation of other Bank functions and processes that have not been affected by the information security incident.

8.8. During the assessment of the consequences of an information security incident, the extent of the damage caused and the volume of losses incurred as a result of the incident shall be determined.

Following the containment or neutralization of the threat, the following activities shall be performed:

- recovery of operations and remediation of the consequences of the incident;

- analysis of the incident;

- identification and clarification of the sources and causes of the incident;

- collection of evidence.

When analyzing an information security incident, it shall be necessary to determine:

- the characteristics of the threats that led to the incident and the frequency of occurrence of the identified threat types;

- the causes of the incident and the sources of the threats;

- whether vulnerabilities were exploited in the course of the incident;

- existing deficiencies and weaknesses in the information protection system and the incident management system;

- the effectiveness of employee actions, as well as the effectiveness of incident management procedures and processes.

8.9. The results of information security incident analyses and the conclusions derived from their review shall be used for the development and implementation of measures aimed at preventing the recurrence of similar incidents or reducing the likelihood of their occurrence in the future.

Such measures shall be aimed at eliminating identified deficiencies, improving the effectiveness of the information protection system, remediating vulnerabilities, and enhancing information security methods and controls.

8.10. Containment and neutralization of threats, assessment of incident consequences, recovery of operations and remediation of incident impacts, as well as the analysis of information security incidents, shall be performed by the Bank's Information Security Incident Response Team.

The composition of the Information Security Incident Response Team shall be approved by a Bank Order and shall be reviewed as necessary (including in cases of employee transfers, dismissal of responsible personnel, or the hiring of new qualified specialists).

Where necessary and subject to the approval of the Chairman of the Management Board, employees of other structural units of the Bank or

representatives of interested organizations may be involved in carrying out the above procedures.

8.11. Within the framework of information security incident management, evidence collection shall be aimed at identifying, collecting, examining, and preserving information that may be used as evidence in judicial and other proceedings, as well as serve as a basis for holding responsible persons liable or applying disciplinary measures.

Evidence collection shall be carried out during the incident investigation process.

For the purpose of conducting an incident investigation, a special commission (working group) shall be established by decision of the Bank's management, and its composition shall be determined by the relevant administrative document.

8.12. The procedures for implementing the information security incident management processes specified in Clause 8.2 of this Policy, the responsibilities of management, incident response personnel, and Bank employees within the framework of information security incident management shall be determined by the Information Security Incident Response Regulation set forth in Appendix 15 to this Policy.

When managing information security incidents, the Bank may interact with the following external organizations:

1) The Central Bank of the Republic of Uzbekistan - with respect to reporting incidents that have occurred, measures taken, and the status of their implementation;

2) Interested third-party organizations with which the Bank interacts in the course of its activities (partners, service providers, equipment suppliers, and solution providers) - with respect to incident notification, containment, remediation of consequences, and the development of joint measures to prevent the recurrence of similar incidents;

3) Law enforcement authorities - with respect to initiating and investigating cases related to information security incidents;

4) Emergency management authorities - with respect to reporting events that resulted in an emergency situation, participating in mitigation of the consequences, and investigating the causes of such events;

5) The Bank's clients - with respect to informing them about service disruptions, expected remediation timelines, corrective actions taken, restoration of services, and other matters related to information security incidents.

The procedures for interaction with third-party organizations in the course of information security incident management shall be governed by the Information Security Incident Response Regulation set forth in Appendix 15 to this Policy.

9. COMMUNICATION CHANNEL SECURITY

9.1. Within the Bank, power and network cabling used for data transmission shall be protected against damage in order to prevent information interception and compromise of data integrity.

To mitigate these risks, the Bank shall implement the following protective measures:

1) power and telecommunication cables shall, where feasible, be routed underground, through cable ducts, utility tunnels, or within buildings, or otherwise be adequately protected against unauthorized physical access;

2) network cables shall, where feasible, be routed separately from power cables to prevent mutual interference and other adverse effects;

3) network cable routing shall be designed to avoid public access areas wherever possible; where such routing is technically impracticable, network cables shall be protected by dedicated conduits, cable trays, or metal ducts;

4) unused network cable connectors shall be sealed or protected with dedicated security caps;

5) cross-connect and switching equipment to which network cables are connected shall be located in protected premises or secured communication cabinets;

6) unused network ports shall be disabled through telecommunication and server equipment management tools;

7) inspections (including network scanning and physical inspections) shall be conducted to detect unauthorized device connections to the cabling infrastructure.

9.2. To ensure the confidentiality of information during transmission over external telecommunication networks and the corporate network, the following security measures shall be implemented:

1) use of a dedicated Fiber-Optic Communication Line (FOCL) between the Head Office (primary data center) and the backup data center, as well as the establishment of IPSec VPN connections between the primary and backup data centers;

2) establishment of IPSec VPN connections for connecting the IT Office and principal branch offices to the Head Office (primary data center) through the Bank’s corporate network;

3) use of IPSec VPN connections established through the Central Bank’s Banking Telecommunication Network (BTN) to facilitate interaction between the Bank’s Core Banking System (CBS) and third-party information systems, including the Central Bank’s banking systems, the HUMO and UzCard processing systems, and other systems;

4) use of secure connections based on the SSL/TLS protocol when providing access to the Bank’s web resources through the corporate network and the Internet, including the official website, Internet banking resources, and CBS information system web applications;

5) use of secure connections based on the TLS protocol when mobile users access the Bank’s mobile banking system through mobile applications;

6) use of secure SSH connections when administrators remotely connect from workstations through the Bank’s corporate network and VPN gateway to network and server equipment located in the primary and backup data centers.

9.3. Requirements for the establishment of secure network connections within the corporate network shall be governed by the Regulation on the Organization of the Corporate Network and Secure Network Connections set forth in Appendix 1 to this Policy.

9.4. Within the Bank, employee access to the Internet shall be provided through the Bank's Internet gateway installed at the boundary between the Head Office (primary data center) and the external Internet network.

9.5. Guest Wi-Fi networks shall be deployed at the Head Office service area to provide Bank visitors with Internet access.

In addition, Wi-Fi networks shall be deployed for employees of the Head Office and the IT Office.

Such Wi-Fi networks within the Bank shall comply with the following requirements:

- absence of any physical connection between Wi-Fi networks and the local networks of the Head Office, IT Office, branch offices, or the Bank's corporate network;
- use of a dedicated Internet connection provided by a local service provider for Wi-Fi networks;
- connection of Wi-Fi networks to the Internet through a dedicated firewall with mandatory user authentication by username and password.

10. ROLES AND RESPONSIBILITIES

10.1. In order to establish and maintain an information security regime, responsibilities for ensuring the security of individual Bank assets, as well as for implementing the relevant information protection procedures aimed at ensuring business continuity and recovery of the Bank's operations, shall be clearly documented.

10.2. Responsibility for the allocation of resources and the implementation of information security procedures shall rest with the Bank's Management and the Information Security Department.

The primary responsibilities of the Bank's Management in the field of information security shall include:

1) establishing information security objectives and principles that meet the Bank's requirements;
2) defining and modifying the organizational structure of the Bank's information security management framework;
3) allocating functions and appointing persons responsible for information security;
4) allocating and providing the resources necessary to ensure the Bank's information security;
5) coordinating and supporting initiatives of the Bank's structural units and employees in the field of information security;
6) approving information security projects of the Bank;

7) ensuring the inclusion of information security requirements in all Bank projects;

8) assessing the appropriateness of, and coordinating the implementation of, specific information security management measures for new Bank systems and services;

9) reviewing the results of information security incident investigations and making decisions regarding the accountability of responsible persons;

10) supporting and incentivizing employees who contribute to improving the effectiveness of information security, as well as performing other functions in this area.

10.3. Direct responsibility for organizing and ensuring the effective operation of the Information Security Management System (ISMS) shall be assigned to the Information Security Department.

The functions and responsibilities of the Information Security Department shall be defined by the Regulation on the Information Security Department attached to this Policy.

10.4. The following units participate in the Bank's information security processes:

- the General Security Department, which is responsible for ensuring physical security within the Bank;

- the Information Technology Department, which is responsible for the operation, maintenance, and technical support of software, hardware, and software-hardware components of the Bank's information assets.

10.5. To ensure maintenance, technical support, and the continuous operation of the Bank's information assets, responsible employees of the Information Technology Department shall be assigned to each information asset to provide support and development of the relevant software.

10.6. This Policy establishes the following allocation of responsibilities for information security within the Bank:

1) the Head of the Information Security Department shall be responsible for organizing and implementing all information security measures within the Bank;

2) the Head of the General Security Department shall be responsible for ensuring the physical protection of the buildings, premises, and tangible assets of the Bank's Head Office and branch offices;

3) the Director of the Information Technology Department and employees of the Information Technology Department responsible for ensuring the continuous and proper operation of the Bank's information assets, including local area networks, the corporate network, external communication channels, information resources, and information systems, shall be responsible for the maintenance, technical support, and uninterrupted operation of such information assets;

4) Bank employees and owners of the Bank's information assets shall bear personal responsibility for any breach of confidentiality of protected information, regardless of the form in which such breach occurs;

5) Bank employees shall be responsible for actions performed within the Bank's information systems within the scope of the roles, privileges, and job responsibilities assigned to them;

6) responsibility for ensuring the information security (including physical security) of workstations, other endpoint devices, and information media shall rest with the Bank employee to whom such assets have been assigned for the performance of official duties;

7) heads of the Bank's Head Office structural units, managers of branch offices, and responsible personnel of the Bank's Administrative Department shall be responsible for compliance with fire safety and technical safety requirements, as well as for safeguarding equipment within the respective buildings and premises.

10.7. The Bank has designated the following responsible personnel:

1) Corporate Network Administrator, being an employee of the Information Technology Department, whose responsibilities include:

- ensuring the proper and uninterrupted operation of the corporate network equipment;
- establishing and maintaining secure network connections within the corporate network;
- managing network traffic, network connections, and access to information systems and information resources from the corporate network and external networks.

2) Local Network System Administrator, being an employee of the Information Technology Department, whose responsibilities include:

- ensuring the operation of the domain controller server;
- managing employee user accounts and their access to the Bank's information systems and information resources.

3) Information System Administrators, being employees of the Information Technology Department, whose responsibilities include:

- configuring and administering information system servers, monitoring their operation, and reviewing and modifying parameters of server storage systems and data storage systems;
- configuring system and application software of information systems and monitoring their operation;
- verifying parameters and configurations of server storage systems and data storage systems, as well as reviewing operational and failure logs;
- performing backup and recovery of information system servers.

4) Database Administrators, being employees of the Information Technology Department, whose responsibilities include:

- administration of database management systems;
- making changes to database structures;
- verifying databases using data integrity control mechanisms;
- performing backup and recovery of information system data.

The responsibilities specified in this clause shall be incorporated into employees' job descriptions and other internal regulatory documents of the Bank.

In the event of the absence of a responsible employee (due to annual leave, temporary incapacity for work, business travel, or other reasons), his or her duties shall be performed by an employee duly appointed in accordance with the established procedure.

Such employee shall be granted the necessary access rights and shall bear responsibility for the proper performance of the duties assigned to him or her.

10.8. For the purpose of segregation of duties and responsibilities:

1) a list shall be established of persons authorized to have physical and logical access to the Bank's equipment and information security controls, protected assets, including confidential information, data centers, server rooms and other high-security premises (Zone 3), local and corporate networks, the Core Banking System (CBS), as well as other information systems and information resources of the Bank;

2) mobile devices, information media, and data storage devices shall be assigned to Bank employees through the relevant organizational and administrative documents;

3) the Bank's Information Security Department shall monitor the performance of duties assigned to persons responsible for ensuring information security.

10.9. Bank employees shall familiarize themselves with the Bank's Information Security Policy upon its approval or revision and acknowledge such familiarization by signature in the Information Security Policy Acknowledgement Register, the form of which is set forth in Appendix 16 to this Policy.

Employee familiarization with the requirements of the Information Security Policy and their training shall be carried out in accordance with Clause 7.4.4 of this Policy.

11. POLICY REVIEW AND UPDATE PROCEDURE

11.1. The Information Security Department shall assess the relevance and effectiveness of the provisions and requirements of the Information Security Policy in the following areas:

- compliance of the Information Security Policy with the Bank's current organizational, technological, and information infrastructure, as well as with its future development plans;
- compliance of the Information Security Policy with the requirements of applicable regulatory documents;
- adequacy and reasonableness of the requirements established by the Information Security Policy;
- effectiveness of the information security methods and controls provided for by the Information Security Policy.

11.2. The assessment of the relevance and effectiveness of the Bank's Information Security Policy shall be conducted by the Information Security Department on a regular basis, but not less than once a year.

The assessment of the relevance and effectiveness of the Bank's Information Security Policy may be carried out through an internal or external audit to evaluate

the compliance of the Bank's information infrastructure with the requirements and provisions of the approved Policy.

Based on the results of the assessment, proposals may be prepared for amendments and supplements to the Policy or for its revision.

Proposals for amendments, supplements, or revision of this Policy shall be prepared by the Information Security Department, coordinated with the relevant structural units of the Bank, and approved by the Bank's Supervisory Board.

11.3. Proposals for amendments and supplements to the Bank's Information Security Policy, or for its revision, shall be prepared in the following cases:

- where inconsistencies are identified between the provisions and requirements of the Information Security Policy and the Bank's organizational, technological, or information infrastructure;
- where individual provisions and requirements of the Information Security Policy conflict with newly adopted or amended legislative and other regulatory acts;
- where the requirements, methods, and information security controls established by the Information Security Policy are found to be insufficient or ineffective;
- where it is necessary to improve the Information Security Policy and the Bank's information security management approach;
- in the event of reorganization or restructuring of the Bank;
- in the event of changes to the structure or composition of the Information Security Management System (ISMS);
- during reconstruction or modernization of the information and communication infrastructure;
- in the event of changes to business processes, technological processes, or other similar circumstances.

11.4. Amendments and supplements to the Bank's Information Security Policy, or its revision, shall be carried out for the following purposes:

- improving information security management approaches and related processes;
- improving information security controls, management mechanisms, and security measures, as well as the objectives of their application;
- improving resource allocation and/or assignment of responsibilities, as well as increasing accountability;
- reducing information security threats to the Bank.

12. FINAL PROVISIONS

12.1. In the event that certain provisions of this Information Security Policy become inconsistent with applicable legislation and regulatory documents as a result of the adoption of new regulatory legal acts or amendments to existing regulatory legal acts, such provisions shall cease to have legal effect until the relevant amendments and supplements are made to this Information Security Policy.

Where newly adopted or amended regulatory legal acts conflict with the provisions of this Policy, the Bank shall, pending the introduction of the relevant amendments, be governed by the requirements of the applicable legislation.

In all matters not regulated by this Policy, the Bank shall be guided by the applicable legislation of the Republic of Uzbekistan.

12.2. Upon approval of this Information Security Policy of JSC "ANOR BANK", the analogous document previously approved by the Bank's Supervisory Board (Minutes No. 5 dated February 10, 2022) shall be deemed repealed and no longer in force.

Developed by:	**Head of Information Security Department**	SIGNATURE	**A.A. Abdurakhmanov**
Agreed by:	**Chairman of the Management Board**	SIGNATURE	**Sh.S. Akramov**
	First Deputy Chairman of the Management Board	SIGNATURE	**E. Nadzhimitdinov**
	Deputy Chairman of the Management Board	SIGNATURE	**E.R. Kadirov**
	Deputy Chairman of the Management Board	SIGNATURE	**A.R. Saydullaev**
	Deputy Chairman of the Management Board	SIGNATURE	**S.D. Khan**
	Deputy Chairman of the Management Board	SIGNATURE	**M.D. Nuritdinova**
	Managing Director	SIGNATURE	**A.A. Bakiev**
	Chief Accountant	SIGNATURE	**U.M. Babaev**
	Head of Legal Department	SIGNATURE	**T.F. Zanakhov**
	Director of Risk Management Department	SIGNATURE	**D.A. Ibragimova**
	Director of Internal Audit Department	SIGNATURE	**S.A. Usmanov**
	Director of Internal Control Department	SIGNATURE	**M.T. Pulatova**
	Acting Director of Human Resources Department	SIGNATURE	**A.S. Ilkhomzhonov**
	Head of Compliance Control Department	SIGNATURE	**D.I. Khushnazarov**
	Head of General Security Department	SIGNATURE	**M.I. Norkin**