Information Security Policy of VTB Bank (Kazakhstan) Subsidiary Joint Stock Company

VTB Bank (Kazakhstan) Subsidiary Joint Stock Company (hereinafter referred to as the "Bank") has developed and the Bank's Board of Directors has approved an Information Security Policy (hereinafter referred to as the "Policy"), which defines the approaches, principles, and rules for building an effective information security (hereinafter referred to as "IS") management system at the Bank, as well as identifies the Bank's bodies and subdivisions responsible for implementing the provisions of the Policy.

The Policy has been developed in accordance with the current legislation of the Republic of Kazakhstan, the requirements of the Agency of the Republic of Kazakhstan for the Regulation and Development of the Financial Market, and the National Bank of the Republic of Kazakhstan, as well as the Bank's internal documents.

The Policy defines:

1) The goals, objectives, and fundamental principles for building the IS management system;
2) The scope of the information security management system;
3) Requirements for managing access to information created, stored, and processed in the Bank's information assets;
4) Requirements for monitoring information security activities and measures to identify and analyze threats, counter attacks, and investigate IS incidents;
5) Requirements for the collection, consolidation, and storage of information on IS incidents;
6) Requirements for analyzing information on IS incidents;
7) The responsibility of Bank employees to ensure IS while performing their assigned functional duties.

Goals, objectives, and fundamental principles for building the IS management system

The main objectives of IS management at the Bank are to establish an effective IS management system (hereinafter referred to as the "ISMS") that corresponds to the external operating environment, the Bank's strategy, the Bank's organizational structure, the volume of assets, the nature and level of complexity of the Bank's operations, and is aimed at minimizing IS risks, as well as the objectives set forth in the Bank's Policies.

The primary objective of the ISMS is to minimize the IS risks to which the technologies and automated information systems (hereinafter referred to as the AIS) used by the Bank to achieve its business objectives are exposed, as well as to ensure the effectiveness of measures to mitigate the adverse consequences of the implementation of IS threats and potential incidents.

To ensure an appropriate level of the ISMS, as well as its development and improvement, the Bank achieves a number of key objectives:

1) Implementing measures to protect information assets from IS threats;
2) Optimizing the cost of ownership of IS means;

3) Preventing and/or reducing damage from actual IS threats to an acceptable level;
4) Compliance with legislative, regulatory, and contractual requirements in the field of IS;
5) Enhancing the stability of the Bank's operations in the event of potential implementation of IS threats;
6) Controlling the status of the Bank's ISMS and continuously improving it;
7) Continuous monitoring of and response to IS incidents, including the cyber intelligence process;
8) Training and professional development of employees to ensure a rapid response to IS incidents;
9) Participating in the implementation of a unified IS development strategy for VTB Group members, and introducing transparent, standardized processes for IS control, assurance, and management;
10) Improving the efficiency and quality of interaction with the Parent Bank on IS issues.

Fundamental Principles for Building the IS Management System

To achieve maximum effectiveness of the ISMS, the Bank is guided by the following fundamental principles:

1) **Integrity** – the security of AIS is an integral property (characteristic) of the systems, not an additional service;

2) **Comprehensiveness** – the coordinated application of diverse tools is necessary when building a holistic information protection system that covers all channels through which threats may be implemented and contains no vulnerabilities at the interfaces between its individual components;

3) **Systematic Approach** – Information protection activities must be strictly and comprehensively regulated;

4) **Continuity** – information protection is not a one-time event nor a simple collection of implemented measures and installed security tools, but a continuous, purposeful process involving the adoption of appropriate measures at all stages of the Bank's information systems lifecycle, starting from the earliest stages of their design, and not only during the operational phase;

5) **Adequacy** – the methods and means of information protection used must be adequate to the threats of its destruction, leakage, or distortion;

6) **Identification and assessment of assets** – the implementation of the "Adequacy" principle must be based on the identification of all information assets and the determination of their value for the Bank's goals and objectives;

7) **Flexibility and manageability** – security systems must allow for varying the level of protection for AIS;

8) **Timeliness** – the development of IS subsystems must proceed concurrently with the development of the system being protected;

9) **Prevention** – the focus of the IS system should be on preventing (preventive measures) IS incidents that could affect the integrity, availability, and confidentiality of information;

10) **Controllability** – the mandatory and timely detection and suppression of attempts to violate established information security rules;

11) **Legality** – information protection activities must be carried out in strict compliance with the current legislation, the requirements of supervisory and regulatory authorities, and regulatory acts in the field of information protection;

12) **Following the best practices** – when implementing IS measures, it is recommended to consider the requirements of VTB Group, as well as domestic and international IS standards, as best practices;

13) **Analysis and improvement** – it is necessary to continuously assess the effectiveness and improve IS measures and tools based on an analysis of information system operations, changes in methods and means of information interception and their impact on system components, changes in regulatory requirements for protection, and domestic and international experience in the field of information protection;

14) **Minimization of Authority** – The granting of access rights to users is determined solely by operational necessity. Access to information must be granted only to the extent necessary for an employee and third parties to perform their official/contractual duties;

15) **Separation of functions –** when defining the composition of roles used to assign access rights, it is prohibited to combine within a single role a set of functions (concentration of authority) that would allow a single employee to independently perform critical operations or obtain full and uncontrolled access to any of the Bank's systems;

16) **Personalization** – all actions by Bank employees must be performed on behalf of a personalized account. Accounts not assigned to a specific employee are not permitted;

17) **Everything that is not permitted is prohibited** – access to any object in the information system must be granted only with the appropriate authorization (rule) as documented in the project documentation, business process regulations, and information security settings. Any access not explicitly authorized must be prohibited;

18) **Ease of use of security measures and tools** – the security tools used must be intuitive and easy to use. Their application must not entail significant additional effort during the normal work of information system users (employees and customers);

19) **Resilience of security measures** – the level of resilience of the measures used and the effectiveness of IS measures must be determined by the value of the

protected object, and must require an attacker to expend disproportionately large amounts of time and computing power to overcome them;

20) **Layered security**—one must not rely on a single line of defense, no matter how reliable it may be considered. In addition to perimeter security measures, systems must be used to protect the internal network, servers, workstations, databases, etc.;

21) **Diversity of security measures**—to reduce overall security dependence on suppliers, providers, and partner companies, as well as to mitigate failures and outages of individual systems, it is advisable to use solutions from different vendors. The use of antivirus software from different vendors on workstations, servers, and firewalls is mandatory;

22) **Specialization and Professionalism** – specialized organizations must be engaged for the development, implementation, maintenance of tools, and implementation of IS measures; those best prepared for the specific type of activity involved in ensuring the security of information resources, possessing practical experience, the necessary licenses to provide services in this field, holding partner status with the vendors of the implemented solutions, and employing highly qualified staff;

23) **Awareness** – the awareness of employees and customers regarding IS issues is a prerequisite for the secure operation of systems;

24) **Personal Responsibility** – responsibility for ensuring the security of information and the systems that process it rests not only with the Information Security Department but also with every Bank employee within the scope of their authority;

25) **Staff loyalty** – creating a supportive atmosphere within the teams of all Bank departments, where compliance with IS requirements is not perceived by employees as an additional burden to be avoided, but as a conscious necessity and an integral part of corporate ethics;

26) **Management engagement** – the Bank's management recognizes the need to ensure IS and directly participates in strategic decision-making regarding the operation of the IS system, including decisions on IS risk acceptance;

27) **Interaction and Coordination** – Effective IS is achieved through interaction and coordination with all other concerned departments of the Bank, the Head Office's IS department, and other relevant ministries, agencies, organizations, and associations;

28) **Technological Independence –** upon selecting software and hardware, including IS tools, consideration is given to any restrictions on their use imposed by developers (manufacturers) or other parties. Information security tools must be backed by warranty and/or technical support for the entire duration of their operation.

The Policy applies to all Bank employees and describes the conceptual foundations and requirements for organizing IS activities, as well as sets out the main vectors for their implementation in the following areas:

1) Identification of information assets, categorization of protected information;
2) Building network security, including countering attacks;
3) Establishing anti-fraud mechanisms;
4) Ensuring access control to the Bank's AIS and information resources;
5) Ensuring the protection of servers, data centers, and server rooms;
6) Providing antivirus protection for the information infrastructure in the manner prescribed by the Bank;
7) Ensuring protection of automated workstations;
8) Ensuring IS at all stages of the application software/Bank's AIS lifecycle;
9) Ensuring IS when conducting activities in a virtual environment;
10) Ensuring the protection of database management systems;
11) Ensuring/implementing content control when using the Internet and email;
12) Ensuring protection against the impact of malicious code;
13) Ensuring cryptographic protection of information;
14) Implementing backup and storing backup copies;
15) Raising employee awareness of IS issues;
16) Monitoring IS and managing IS events and incidents;
17) IS management.

The scope of the ISMS covers:

1) All of the Bank's business processes;
2) All of the Bank's structural subdivisions;
3) All buildings of the Bank's head office and branches.

Requirements for managing access to information created, stored, and processed in the Bank's information assets

Requirements for managing access to information created, stored, and processed within the Bank's information assets cover all stages of the user access lifecycle, from the initial registration of new users to the final deregistration of users who no longer require access to the AIS and services.

An employee is assigned a role (or a list of roles) based on a documented request signed by the head of his/her Bank structural subdivision and approved by the business process owner.

A user must be granted only the minimum powers necessary to perform his/her functional duties, and upon a change in job responsibilities or the dismissal of a Bank employee, all rights must be revoked.

Third parties requiring access to the Bank's AIS in accordance with the terms and conditions of a contract or agreement (technical support for equipment, support for the implementation of information systems) must enter into a confidentiality agreement (including with partners).

In the event of the transfer of information assets to third parties (placement of the Bank's server capacity in third-party data centers, use of external data processing and/or storage services), the Bank shall take the following IS measures:

1) Inclusion in the relevant agreement/contract with the third party of requirements regarding the protection of the Bank's information assets and the Bank's right to verify compliance with such requirements, as well as provisions regarding compensation for damages arising from a breach of IS and the operational integrity of the automated information system;
2) Preventing third parties from accessing information that may not be disclosed to them under the civil and banking laws of the Republic of Kazakhstan, as well as the laws of the Republic of Kazakhstan on personal data and its protection.

Requirements for monitoring IS activities and measures to identify and analyze threats, counter attacks, and investigate IS incidents

The procedure for responding to IS incidents consists of the following stages, including but not limited to:

1) Monitoring of IS events and detection of IS incidents (hereinafter referred to as the monitoring and detection stage);
2) Localization and mitigation of the IS incident (hereinafter referred to as the response stage);
3) Internal investigation of the IS incident (hereinafter referred to as the internal investigation stage).

During the monitoring stage of IS activities, the following measures are carried out by the IS subdivision:

1) Monitoring and analysis of IS events;
2) Classifying IS events as IS incidents in accordance with the established procedure for classifying IS events as IS incidents;
3) Classification and prioritization of IS incidents;
4) Forwarding information about the IS incident to the response phase.

During the IS incident response phase, standard response procedures are applied; however, in cases where standard response procedures prove ineffective, operational measures are taken to respond to IS incidents, including but not limited to the following:

1) Informing and involving Bank employees, as well as third parties if necessary, in the response process to ensure effective countermeasures against the IS incident;
2) In consultation with business process owners, implementing additional control measures to partially or fully suspend the business process at the Bank;
3) Collecting data from the software and hardware involved in the IS incident;
4) Analyzing the IS incident, containing it, and mitigating its consequences;
5) Conducting a retrospective analysis of IS events;
6) Identifying indicators of compromise and vulnerabilities discovered during the response to IS incidents, and implementing corrective measures aimed at preventing similar IS incidents in the future;
7) Deciding on the need to conduct an internal investigation of the IS incident.

During the internal investigation of the IS incident, the Bank ensures:

1) involving responsible employees and/or Bank subdivisions involved in the IS incident response process, as well as third parties, in the internal investigation of the IS incident;

2) The collection and analysis of materials necessary for conducting the internal investigation of the cybersecurity incident;
3) Determining the causes of the IS incident and the sequence of events leading to it;
4) Assessing the scope of the impact and damage resulting from the incident;
5) Analyzing the effectiveness of the response measures taken in relation to the investigated IS incident;
6) Preparing a report on the results of the investigation of the IS incident, which includes information about the incident as well as recommendations for corrective actions to reduce the likelihood and potential damage from a recurrence of the IS incident.

Requirements for conducting an analysis of information on IS incidents

The main objectives of analyzing information on IS incidents are as follows:
1) Ensuring the completeness and accuracy of information about the IS incident;
2) Identifying the consequences and damage caused;
3) Identifying attack methods and controls capable of preventing recurrence of IS incidents;
4) Identifying actions that can be taken to fully eliminate the IS threat;
5) Identifying the root cause of the IS incident.

This Policy is mandatory for all Bank employees and third parties, and is communicated to service providers with access to the Bank's information assets and internal documents, to the extent that such access is directly related to the Bank and its activities.

This policy is subject to revision in the event of amendments or additions to the legislation of the Republic of Kazakhstan and/or the Bank's internal documents.