Information Security Policy of KMF Bank JSC

Business owner:	Information Security Unit of the Security Department
Approved by:	Minutes of the Board of Directors dated November 12, 2025, No. 3(9).
Put into effect on:	November 12, 2025
Recognized void on:	Information Security Policy of JSC “KMF Bank,” approved by the Minutes of the Board of Directors of JSC “MFO (KMF)” No. 6 dated July 15, 2026
Internal Regulation Access Level:	Unlimited access

Almaty, 2025

Table of Contents

Section 1. General Provisions 4
Section 2. Information Security 5
Section 3. Organization of the Information Security Management System 5
§1.Definition of the Information Security Management System 5
§2.Objectives of the Information Security Management System 6
§3.Tasks of the Information Security Management System 6
§4.Principles for Establishing the Information Security Management System 6
§5.Scope of the Information Security Management System 7
§6.Implementation of the Information Security Management System 7
§7.Areas for Development and Improvement of the Information Security Management System 8
§8.Requirements for Managing Access to Information Created, Stored, and Processed within the Bank's Information Assets 9
§9.Requirements for Monitoring Information Security Activities and Implementing Measures to Identify and Analyze Threats, Counter Attacks, and Investigate Information Security Incidents 10
§10.Requirements for the Collection, Consolidation, and Storage of Data about Information Security Incidents 11
§11.Requirements for the Analysis of Data about Information Security Incidents 12
Section 4. Final Provisions 13

Section 1. General Provisions

1. This Information Security Policy of KMF Bank JSC (the "Policy") is an internal regulation that forms the foundation of the information security management system at KMF Bank JSC (the "Bank").
2. The Policy has been developed in accordance with the legislation of the Republic of Kazakhstan, including the Requirements for ensuring information security of banks, branches of non-resident banks of the Republic of Kazakhstan, and organizations performing certain types of banking operations, approved by Resolution No.48 of the Management Board of the National Bank of the Republic of Kazakhstan dated March 27, 2018, as well as the ISO/IEC 27000 series of international standards on information security and the Bank's internal regulations.
3. The purpose of this Policy is to formally state the Bank's official position approved by its management with regard to information security. It defines the goals, objectives, principles, and strategic direction for the development of the Bank's information security management system.
4. The Management Board of the Bank initiates, supports, analyzes and monitors the implementation of processes of the information security management system. These processes aim to create the conditions necessary for sustainable business growth, maintain an acceptable level of information security risk, enhance competitive advantage, ensure financial stability and profitability, and improve the Bank's rating.
5. The Board of Directors of the Bank provides strategic oversight in the area of information security. It ensures that information security considerations are integrated into the Bank's overall strategy and operational activities. When forming the Bank's budget, the Board of Directors considers the resources required to maintain information security, taking into account the Bank's strategic goals, legal and regulatory requirements, the current and anticipated threat landscape, and commitments to stakeholders.
6. The information security requirements outlined in this Policy are aligned with the Bank's development strategy, embedded in its business processes, and focused on minimizing information security risks. Information security risks are recognized as a part of the Bank's operational risks and are acknowledged as having a significant impact on both financial sustainability and operational stability.
7. The requirements set forth in this Policy apply to all processes, resources, and entities within the scope of the information security management system set by this Policy.
8. This Policy is a publicly accessible document and is published on the Bank's corporate website for the benefit of all interested parties.
9. The following terms and definitions are used in this Policy:
    1) access – the ability to utilize the Bank's information assets;
    2) information security incident – any isolated or recurring failure within the information and communication infrastructure or its components that poses a threat to their proper functioning and/or creates conditions for unauthorized acquisition, copying, distribution, modification, destruction, or blocking of electronic information resources;

3) information asset – a combination of information and the components of the information and communication infrastructure used for its storage and/or processing.
4) information and communication infrastructure (the "information infrastructure") – the set of components of the information and communication infrastructure designed to support the technological environment required for generating electronic information resources and providing access to them.
5) information security risk – the potential for harm resulting from breaches of confidentiality or deliberate violations of the integrity or availability of the Bank's information assets.

Section 2. Information Security

10. Information security refers to the state of protection of the Bank's electronic information resources, information systems, and information infrastructure from both internal and external threats. These threats may result in financial losses, reputational harm, or other negative impacts on the interests of the Bank, its customers, employees, and shareholders.
11. Information security is also defined as the continuous process of preserving confidentiality, maintaining integrity and availability of the Bank's information assets.
12. The following are the core attributes maintained to ensure information security:
    1) confidentiality – an information attribute ensuring that information is not disclosed to or accessed by unauthorized subjects. Measures to ensure confidentiality are aimed at preventing unauthorized disclosure of information.
    2) integrity – an information attribute maintaining the completeness, consistency and accuracy of information during storage, processing, and transmission. Measures to ensure integrity are designed to prevent and detect unauthorized creation, modification, or deletion of information.
    3) availability – an information attribute ensuring that information is accessible and usable by authorized users upon request. Measures to ensure availability focus on maintaining access to information despite potential disruptions, including system failures or deliberate attempts of breaching availability.
13. The primary objective of the Bank's information security efforts is to protect its information assets ensuring minimal level of potential damage to the Bank's business processes. To achieve this objective, the Bank has implemented, operates and continuously enhances an information security management system.

Section 3. Organization of the Information Security Management System

§1. Definition of the Information Security Management System

14. The information security management system is a part of the Bank's overall management system, designed to manage the process of ensuring information security.
15. The information security management system enables a systematic, justified, and controlled approach to decision-making in the field of information security by leveraging risk management mechanisms.

16. The information security management system encompasses the Policy, organizational structure, processes, resources, and documented information that collectively support the effective management of information security.
17. The Bank ensures maintaining the operation, appropriate maturity level, development and continuous improvement of the information security management system.

§2. Objectives of the Information Security Management System

18. Primary objectives of the Information Security Management System are to:
    1) establish and maintain conditions in the Bank under which risks related to security of information assets are controlled and manageable;
    2) ensure compliance with legal, regulatory requirements, industry standards, and best practices in information security;
    3) support continuity of business processes and the stable operation and sustainable development of the Bank;
    4) enhance trust of customers, counterparties, partners, investors, and community in general to the Bank, upgrade its rating and strengthen its investment attractiveness.

§3. Tasks of the Information Security Management System

19. To achieve these objectives of the information security management system, the Bank ensures efficient implementation of the following key tasks:
    1) identification and classification of information assets;
    2) assessment, processing and monitoring of information security risks;
    3) definition and documentation of applicable information security requirements and procedures for their implementation;
    4) training Bank employees in information security procedures, raising their awareness and establishing responsibility for information security issues;
    5) regular evaluation of the compliance of the information security management system with applicable internal and external requirements through internal audits and analysis by the Bank's management;
    6) communication with stakeholders on the Bank's approach to ensuring information security, incident management, and findings of independent audits of the Bank's information security.

§4. Principles for Establishing the Information Security Management System

20. The information security management system of the Bank is designed and operated in accordance with the following core principles:
    1) legality – all actions taken to ensure information security of the Bank are conducted in strict accordance with applicable legislation, using permitted methods, tools, and mechanisms for managing, ensuring and controlling information security;
    2) adequacy – information security measures taken are defined based on risk analysis, considering both business needs and threat levels;
    3) continuity – ensuring the stability, reliability, and availability of technical and organizational measures for managing information security;

4) personal responsibility – every employee of the Bank is accountable for fulfilling his/her duties and complying with requirements imposed on him/her as part of the operation of the information security management system;
5) minimization of authorities – access to information is granted only to the extent necessary for Bank employees to perform their official functions and duties;
6) elimination of conflicts of interest – employee responsibilities are assigned in a manner that ensures elimination of a possible conflict of interest. In particular, no employee should have the authority to perform critical operations alone;
7) comprehensiveness – development of the information security management system is based on the coordinated application of various information security management measures covering all key threat channels and eliminating vulnerabilities at component interfaces.

§5. Scope of the Information Security Management System

21. The scope of the information security management system encompasses all processes, resources, and entities within the Bank that are subject to requirements on ensuring information security.
22. Scope of the information security management system includes the following components:
    1) business processes ensuring sustainable functioning and achievement of strategic objectives of the Bank;
    2) information assets, including electronic information resources, databases, documentation, and software;
    3) information infrastructure, including data centers, servers, networks, storage devices, end-user devices, communication channels, and other technological means involved in information processing, storage, and transmission;
    4) Bank employees, including interns and trainees, who have access to information assets;
    5) internal processes and procedures, related to information handling, access control, incident management, auditing, and performance evaluation;
    6) counterparties, suppliers, and external IT service providers, if they are involved in processing, transmitting, or storing the Bank's information.
23. The scope is subject to regular revision and clarification, as necessary.

§6. Implementation of the Information Security Management System

24. The information security management system is built and developed through a cyclical process based on the Deming–Shewhart model of continuous improvement (PDCA: Plan–Do–Check–Act), which consists of the following stages:
    1) Plan – defining the scope of the information security management system, formalizing the information security risk management framework, identifying and allocating resources, designing information security management measures;
    2) Do – implementing the planned security measures and decisions, including those made in follow up of the previous cycles; the ongoing assessment and processing of information security risks;

3) Check – evaluating performance of the information security management system to ensure its effectiveness, adequacy in addressing current threats, and compliance with internal and external factors that have an impact on the Bank's activities;
4) Act – making decisions on corrective actions and actions to implement the identified possibilities for improvements based on findings from the "Check" stage to enhance the overall effectiveness of the information security management system.

§7. Areas for Development and Improvement of the Information Security Management System

25. This Policy identifies the following key areas for the ongoing development and improvement of the information security management system:
1) arranging information security activities – identifying and allocating roles, responsibilities and authorities for ensuring information security in the Bank. This includes effective communication of this information to all relevant parties;
2) documented information management – managing documents related to the information security management system, including creation, coordination, approval, storage, transfer, and destruction.
3) information security risk management – identifying, assessing, processing, and monitoring information security risks;
4) performance evaluation – monitoring, measuring, analyzing, and evaluating the performance of the information security management system, including conducting internal audits and reviews by the management;
5) ensuring personnel security – applying information security compliance measures at hiring, during the employment period and upon transfers and terminations;
6) information asset management – identifying and classifying information assets, defining acceptable use policies, and assigning responsibilities for their protection;
7) access management – ensuring access to information assets is restricted to authorized individuals only, preventing unauthorized access;
8) cryptographic protection – employing cryptographic techniques to ensure the confidentiality, integrity, and authenticity of information;
9) physical and environmental security – preventing unauthorized physical access, theft, and damage to information assets, and ensuring protection against factors that may impact business operations of the Bank;
10) secure operation of information infrastructure – maintaining reliable and secure operation of information processing means, including malware protection, backups, audit trail log management and protection, software and vulnerability management;
11) network security management – ensuring information security upon its transmission of information across internal and external networks of the Bank;
12) information security throughout the information system lifecycle – ensuring compliance with information security requirements at all stages of the

information system lifecycle – from design and development to implementation, operation, modification, and decommissioning, including the protection of test data;

13) supplier relationships – establishing and monitoring information security requirements within all agreements and contracts with suppliers who have access to the Bank's information assets;

14) information security incident management – maintaining a consistent and effective approach for monitoring, identifying, responding to, and investigating information security incidents;

15) information security in business continuity management – ensuring the integrity and availability of information and information processing means during the execution of business continuity and recovery plans;

16) compliance with legal requirements, regulatory requirements, industry standards, contractual obligations, and the provisions outlined in this Policy, as well as other internal regulations of the Bank related to information security.

26. Information security requirements are further clarified and detailed in the internal regulations of the Bank, developed as part of the information security management system based on this Policy.

§8. Requirements for Managing Access to Information Created, Stored, and Processed within the Bank's Information Assets

27. The objective of information access management is to ensure the confidentiality, integrity, and availability of information assets of the Bank, and to prevent unauthorized access, modification, or destruction of information.

28. The general approach to access management is guided by the following principles:

1) least privilege: access rights are granted strictly based on necessity, limited to the volume required to perform assigned job responsibilities;

2) role-based access control: using a role-based access model according to positions and job functions, user categories, and the confidentiality level of the information;

3) ongoing control and review: regular review to ensure that access rights remain relevant and their changes or revocations are made in a timely manner;

4) personalized access: all actions within information systems must be performed using personalized user accounts;

5) access logging: all access events and user activities must be logged to support follow-up analysis and incident investigations;

6) The requirements to the access management processes include the following:

7) procedures for granting, modifying, and revoking access rights must be formalized and documented, including coordination with the respective information asset owners;

8) wherever feasible, access management should be supported by automated tools, integrated with identity and authentication management systems;

9) periodic reviews must be conducted to verify that actual access aligns with approved user rights and roles;

10) all access management actions must be recorded, including dates, justifications, and responsible personnel;

11) special access procedures must be in place for handling situations, such as incidents, emergencies, or the need for emergency access (including privileged access).

29. Access management must be carried out in accordance with the requirements of this Policy, internal regulations of the Bank, and applicable international standards for information security.

§9. Requirements for Monitoring Information Security Activities and Implementing Measures to Identify and Analyze Threats, Counter Attacks, and Investigate Information Security Incidents

30. Monitoring of information security activities is aimed to ensure ongoing compliance with the established requirements of the information security management system, achieve the information security objectives (tasks) and detect deviations, incidents or ineffective measures of information security management promptly.

31. General approach to monitoring is based on the following principles:

1) regularity and systematic approach: monitoring must be performed continuously, in alignment with approved processes and procedures;
2) evidence-based: all monitoring outcomes must be documented, verifiable, and available for further analysis;
3) objectivity and independence: data analysis should be impartial and, where appropriate, involve independent specialists or structural subdivisions of the Bank;
4) focus on improvement: monitoring results are used to initiate corrective and preventive actions.

32. The requirements to the monitoring processes include the following:

1) monitoring must be organized and conducted by the Information Security Unit of the Security Department, in collaboration with other relevant structural subdivisions of the Bank;
2) data on the implementation of information security management measures, incidents, deviations and non-conformities must be collected, stored, and analyzed;
3) monitoring results should be presented as reports and analytical materials for the management and regulatory authorities;
4) automated control tools, such as centralized security information and event management (SIEM) systems, must be used;
5) every stage of the monitoring process must be documented, including methods used, issues identified, and corrective actions taken.

33. Measures are aimed to maintain readiness, minimize potential damage, and prevent recurrence of information security incidents by proactively identifying and analyzing threats, effectively countering attacks, and thoroughly investigating incidents.

34. General approach to identifying and analyzing threats, countering attacks, and investigating information security incidents is built on the following principles:

1) proactiveness: implement preventive measures and early threat detection to prevent risks attacks;
2) timely response: ensure swift action when incidents are detected;
3) comprehensive approach: review incidents considering all relevant factors and vulnerabilities;
4) evidence and traceability: record all information about incidents for analysis, accountability, and further improvement;
5) continuous improvement: use obtained insights to enhance the Bank's tolerance against information security threats.

35. Requirements to measures on identifying and analyzing threats, countering attacks, and investigating information security incidents include:
    1) threat identification and analysis: collect and process information on potential and real threats using technical and analytical tools such as intrusion detection systems, SIEM, and internal/external activity reports;
    2) attack prevention and countering: implement preventive information security management measures, configure and use security tools (such as firewalls, antivirus, intrusion detection and prevention systems), and follow prompt response procedures;
    3) incident investigation: determine the cause, scope, and impact of incidents, and develop corrective actions;
    4) incident logging: record all information security incidents with mandatory indication of detection time, nature, root causes, actions taken, responsible individuals, and response outcomes;
    5) trend and recurring incident analysis: utilize accumulated data to identify recurring patterns, analyze threat dynamics, update information security management measures, and adjust used approaches.
36. Monitoring of information security activities, including the identification and analysis of threats, response to attacks, and investigation of information security incidents, is carried out in compliance with this Policy, the internal regulations of the Bank and applicable international information security standards.

§10. Requirements for the Collection, Consolidation, and Storage of Data about Information Security Incidents

37. The collection, consolidation, and storage of information related to information security incidents are designed to ensure the completeness and accuracy of data needed to analyze root causes, assess damage, improve response effectiveness and prevent recurrence of incidents.
38. The general approach to the collection, consolidation, and storage of information related to information security incidents is based on the following principles:
    1) reliability: incident data must be accurate, complete, and verified through sources recorded in the accounting systems;
    2) timeliness: data must be collected, processed, and consolidated without delays, within established timeline, in accordance with the criticality of the incident;
    3) security: incident information must be protected against unauthorized access, alteration, or deletion, including using technical and organizational safeguards;

4) traceability: all modifications and activities involving incident data must be logged and made available for subsequent analysis;
5) structure: standardized forms and formats are used to ensure uniformity in data recording and storage.

39. Requirements for the processes of collection, consolidation, and storage of data about incidents include:
    1) utilization of automated systems for incident recording and logging, enabling centralized storage and data analysis capabilities;
    2) formalized procedures for collecting initial incident data, including appointment of responsible personnel, timelines for data submission and standardized data list (such as incident type, source, detection time, description, criticality classification, measures taken, etc.);
    3) maintenance of a centralized information security incident log capturing data about all recorded incidents, with features for further search and analysis;
    4) storage of incident-related information for a defined period, in line with the internal regulations of the Bank and legal requirements of the Republic of Kazakhstan;
    5) ensuring access to incident data, granted strictly according to official roles and functional responsibilities, using mechanisms for the separation of rights and maintaining audit trail logs.
40. Data on information security incidents is used to analyze causes and impacts of incidents, and make decisions aimed at improving the processes ensuring information security.
41. Collection, consolidation, and storage of data about information security incidents are carried out in accordance with the requirements of this Policy, internal regulations of the Bank, and applicable international standards for information security.

§11. Requirements for the Analysis of Data about Information Security Incidents

42. The analysis of information security incidents is conducted to identify causes, detect vulnerabilities in systems, assess damage, develop corrective and preventive actions, as well as strengthen the tolerance of the information security management system to recurring incidents.
43. The general approach to the analysis of information security incident is based on the following principles:
    1) reliability: only confirmed and verified data obtained through incident registration and investigation processes is used;
    2) systematic approach: incidents are not considered in isolation, but taking into account potential interrelationships, frequency of occurrence, and the Bank's operational environment;
    3) cause-oriented focus: the primary objective of analysis is to not just mitigate consequences, but also prevent the recurrence of similar future incidents;
    4) documentation: all stages of the analysis must be documented, including conclusions and decisions made.
44. Requirements for the process of analyzing information security incidents include:

1) conducting analysis within designated timeframes, based on incident classification and priority level;
2) identification of underlying causes and factors that contributed to the incident, including human, organizational, technical, and external influences;
3) determination of the consequences of the incident, including the extent of damage, impact on business processes, and violations of information security policies;
4) development of recommendations to address discovered vulnerabilities, corrective measures, and prevent recurrence of similar future incidents;
5) submission of incident analysis results to Bank management and other relevant stakeholders for review;
6) using the accumulated analytical materials to update the risk management system and improve the information security management system.

45. Analysis of incident data must be carried out in accordance with the requirements of this Policy, internal regulations of the Bank, and international standards for information security.

Section 4. Final Provisions

46. This Policy, along with the internal regulations of the Bank on information security, is mandatory for all Bank employees, interns, and trainees. It must also be communicated to customers and other third parties who are granted access to the Bank's information assets, to the extent relevant.
47. All Bank employees are responsible for upholding information security in the performance of their official roles and functional duties.
48. Heads of the Bank's structural subdivisions are responsible for the improper performance and violation of information security requirements by employees of the Bank's structural subdivisions.
49. The HR Department is responsible for ensuring that all Bank employees have read this Policy.
50. The provisions of this Policy shall be reviewed as needed but no less than once every two years, following the Bank's established procedures.
51. The Policy may be revised outside of the regular schedule in cases of:
    1) significant changes to the legislation of the Republic of Kazakhstan that affect the Bank's operations, organizational structure, or business processes;
    2) identification of critical deficiencies in the implementation of measures regulation by this Policy; as well as conflicts between the provisions of this Policy and other internal regulations of the Bank.
52. In matters not explicitly addressed by this Policy, the requirements of the current legislation of the Republic of Kazakhstan and the Bank's internal regulations shall apply.
53. Amendments to this Policy may only be made by the decision of the Board of Directors of the Bank.