Approved by
the Record of the Resolution of
the Supervisory Board of
MFO «KMF» LLC
dated January 31, 2024
to be effective
from February 1, 2024

KMF
МИКРОҚАРЖЫЛЫҚ ҰЙЫМЫ
МИКРОФИНАНСОВАЯ ОРГАНИЗАЦИЯ

INFORMATION SECURITY POLICY

Microfinance organisation "KMF"

Limited Liability Company

2024

CONTENTS

CHAPTER 1. GENERAL PROVISIONS

1.1. This Information Security Policy (hereinafter, the "Policy") shall serve as a fundamental document of the Information Security Management System (hereinafter, the "ISMS") of MFO "KMF" LLC (hereinafter, the "Company"), which defines the information security priorities and principles in the light of current threats inherent and essential to the Company's systems and information assets such as: hacking, virus, fishing and DDoS attacks, theft and disclosure of confidential and personal information, unauthorised actions in the Company's information systems.

1.2. This Policy has been developed in accordance with the laws of the Republic of Kazakhstan in the area of information security, ISO/IEC 27000 series of international information security standards, COBIT methodology, ITIL, Resolutions of the Management Board of the National Bank of the Republic of Kazakhstan dated 27 March 2018, Nos. 47 and 48, current state and prospects for near-term development of the Company's information infrastructure, as well as up-to-date methods of organisational and technical information protection.

1.3. Management of the Company shall realise the importance of/need for development and improvement of information security measures and tools in the context of development of legislative regulations, further development of globally implemented technologies, expectations of the Company's customers and other stakeholders. Compliance with the information security requirements shall enable the Company to create competitive advantages for the Company, ensure its financial stability, effectiveness, compliance with the legal, regulatory and contractual requirements and improve its image.

1.4. Information security requirements set by the Company shall comply with the Company's Strategy and mean to reduce the information security risks to the acceptable level. Information security risks faced by the Company shall pertain to its corporate governance (management), arrangement and implementation of business processes, relationship with the counterparties and customers, the Company's internal economic activity. Information security risks of the Company shall represent a part of operational risks of the Company thus affecting its core business.

1.5. The requirements of this Policy and other internal rules and regulations applicable to information security shall be binding on all employees of the Company.

1.6. This policy shall be a document accessible to any employee of the Company and users of its resources and represent a system of views with regard to the task of ensuring the information security officially adopted by the Company management, and establish the principles of building the information security management system.

CHAPTER 2. COMPANY'S CONTEXT

§1. **Overview of the Company and its business**

2.1. MFO "KMF" LLC is the largest microfinance organisation in Kazakhstan and one of the leaders of the microfinance sector in Central Asia; it is a company with international participation that has a wide regional network; its branches are located not only in the large cities but also in remote rural areas of Kazakhstan. The Company offers credit products intended to support business, improve the people welfare and promote development of agriculture.

2.2. The Company focuses on building the long-term partnership relations with the customers based on mutual trust, understanding and respect.

2.3. Since 1997, the Company has opened 14 branches in the following cities of the Republic of Kazakhstan: Astana, Almaty, Taldykorgan, Aktobe, Shymkent, Kyzylorda, Turkestan, Kostanai, Pavlodar, Petropavlovsk, Taraz, Uralsk, Ust-Kamenogorsk, Kokshetau.

2.4. Each branch has operating offices and sub-offices in rural areas (totally, more than 110 offices and sub-offices operating all over Kazakhstan).

§2. **Mission and objectives of the Company**

2.5. The Company shall contribute to growing the welfare of representatives of micro-, small business and agrobusiness by providing an access to quality microfinance services.

2.6. The Company's priorities shall be as follows:

1) Promote access to financial services and widen a coverage of representatives of micro-, small- and agro-businesses all over Kazakhstan including rural areas;
2) Provide professional microfinance services and improve continuously the quality of the services through a feedback and assessment, thus developing the microfinancing service culture;
3) Contribute to the good of the society by supporting business and improving wellbeing of the customers through earning profit.

§3. **Overview of needs and expectations of the stakeholders**

2.7. Taking into consideration the Company's mission of providing the services, the Company shall exert every effort to identify the needs and expectations of all stakeholders.

2.8. The stakeholders shall comprise:
1) the National Bank of the Republic of Kazakhstan;
2) other governmental and legislative bodies, which regulate the Company's activity;
3) customers of the Company;
4) creditors and investors;
5) internal users – employees of the business units who interact while the Company carries out its operations;
6) service providers.

2.9. Needs and expectations of all stakeholders shall be monitored on the continuous basis by means of surveys and feedback, and analysed to perform current operations. When planning the Company development, the demands, expectations and needs of all stakeholders shall serve as a basis for implementation of changes and development of existing and new business areas of the Company, introduction of new services.

§4. **The Company's capacities**

2.10. The Company shall have the following abilities to guarantee achievement of the ISMS expected outcomes:
1) competent and experienced personnel receiving professional trainings and regular advanced training;
2) necessary infrastructure and data processing centres have been determined, maintained and kept in proper working order;
3) high transparency of the activity and social responsibility of the Company;
4) strong management system that meets the highest up-to-date standards and best global practices.

CHAPTER 3. INFORMATION SECURITY CONCEPT, GOALS AND OBJECTIVES

2.11. Information security shall mean protection of information and facilities for its processing against occasional or deliberate impact of natural and artificial nature.

2.12. Information security shall not be a goal in itself, it shall be required to ensure an adequate protection of the Company's information assets (information, hardware and software system used for its storage and (or) processing), mitigation of risks and economic loss related to threats to the Company's information assets and resources (the Company's main information systems and databases; data on loans issued; the Company's methodology; computer, telecommunication and server equipment).

2.13. The following main attributes of information shall be supported as part of the information security (Figure 1):
1) *Confidentiality* ensures that information can be read and interpreted only by the authorised people and under the authorised processes. Ensuring confidentiality includes procedures and measures intended to prevent disclosure of information by unauthorised users.
2) *Integrity* ensures that information shall remain unchanged, correct and authentic. Ensuring integrity intends to prevent and identify unauthorised creation, modification or deletion of information.

3) *Availability* ensures that the authorised users may have access and use information assets, resources and systems, which they need, and in this case the required performance is supported. Ensuring of availability includes measures to support availability of information regardless of possible interferences, including the system failure and deliberate actions relating to availability breach.

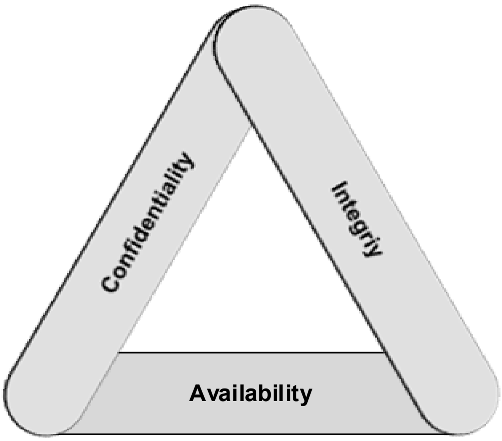

Figure 1. Main attributes of information security (CIA Triad)

2.14. Main objectives of information security shall be to:

1) ensure proper protection of information depending on its value for the Company;
2) ensure information confidentiality, integrity and availability and personal data protection;
3) prevent unauthorised physical and logical access, corruption and intervening the Company's information and data processing facilities;
4) ensure information security as inseparable part of information systems throughout their life cycle;
5) ensure continuous and result-based approach to information security incident management, including reports concerning security events and information security weaknesses.

2.15. To achieve the information security objectives, the Company shall provide the effective handling of the following tasks:

1) stock-taking and classification of the Company's information assets (by the information assets owners of all business units covered by ISMS);
2) identification and assessment of information security risks and likelihood of their occurrence (based on the IS threat model);
3) development of measures for information security risk management (including both the methodological manual and automated control tools);
4) building and optimization of the Information Security Management System, including processes for information security assessment and analysis (both internal and external ISMS assessment and audit);
5) identification and documentation of main requirements and procedures to ensure information security;
6) implementation and adjustment of information security tools;
7) holding information security trainings for the Company's staff;
8) prompt identification and elimination of vulnerabilities in the Company's assets, thus preventing a risk of damage and disruption of normal operation of the Company's business processes as a result of information security threats;
9) minimisation of the Company's potential damage to an acceptable level once the information security threats have occurred, including reduction in time to repair business processes after possible interventions;
10) monitoring and processing of information security events and incidents;
11) planning and optimization of the Company's information security costs.

CHAPTER 4. PRINCIPLES OF INFORMATION SECURITY ASSURANCE

4.1. The main principles to ensure the Company's information security shall be:

1) *Legitimacy* – any actions to ensure information security are taken based on the valid legislation, using all methods permitted by law to detect, prevent, localise and minimise any adverse impact on the Company's information security facilities;
2) *Consistency* – all interrelated, interacting and changing over time elements, conditions and factors critical to the Company's information security support are considered.
3) *Integration* – agreed on usage of heterogeneous devices in building up an integrated protection system, which covers all existing channels of information security threat and does not have any weaknesses at the interface between its separate components.
4) *Continuity* – ongoing support for physical, hardware and software tools as well as ongoing control over fulfilment of the requirements to maintain information security without interruption or suspension in the Company's current business processes.
5) *Timeliness*– timely detection of information security threats, forecasting of potential threats landscape, assessment of their impact on business processes and usage of information security measures, when and where they are appropriate.
6) *Adequacy* – information security measures are effective and comparable with information security risks, inclusive of costs to implement such measures and cover amount of possible loss from such threats.
7) *Succession and improvement* – continuous improvement of protection measures and tools based on succession in organisational decisions, engineering solutions and succession planning.
8) *Flexibility* – the Company ISMS can respond to changing in external environment and conditions of the Company's operations.
9) *User-friendliness* – possible difficulties that users may experience while operating protection devices and implementing critical information security procedures are considered and minimised if possible.
10) *Formalisation* – all information security requirements and measures as well as results of activities directed towards ensuring the information security are properly documented.
11) *Information security awareness and aptitude* – the Company maintains the information security culture and the Company's employees are aware of the information security requirements to the extent that is relevant to their job duties and know access requirements to the Company's information resources, and are governed by the above requirements in their daily work.
12) *Knowing the clients and employees* – the Company has information about its clients, carefully selects employees and service personnel, develops and maintains corporate ethics thus creating an enabling and trusted environment for the Company's operations related to information assets management.

CHAPTER 5. ORGANISATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

§1. **Definition of ISMS**

5.1. ISMS shall be a part of the Company's general management system, which is based on assessment of information security risks and designed to develop, implement, operate, monitory, analyse, support and improve the Company's information security.

5.2. ISMS shall comprise an organisation structure, policies, development of plans, allocation of responsibility, instructions, processes and resources.

§2. **ISMS Scope**

5.3. ISMS scope shall cover the Company's key business processes related to customer services and provision of financial services (including, in addition to the customer services in the offices, sub-offices and branches, the back offices processes related to risk management, accounting for transactions, material and technical support and information support, marketing and business development), all tangible and information assets of the Company, the Company employees and persons that provide/receive services to/from the Company.

5.4. The objects to be protected shall be:

1) all information assets required for the Company to operate, irrespective of the form and type of their presentation
2) all elements of IT infrastructure, including information technologies; hardware and software for generation, processing, transfer, storage (including archiving) and use of the information, including libraries, archives, databases; traffic and telecommunication channels; information protection systems and tools; facilities and premises, where there are located the elements of the Company's IT infrastructure being protected;
3) all business units of the Company;
4) all processes, regulations and procedures of information processing in the Company;
5) personal data of the customers, employees and suppliers of the Company.

§3. **ISMS Implementation**

5.5. Implementation and operation of the Company's ISMS shall rely on the process-based approach. ISMS building shall be a cyclic process, to which a continuous improvement model is applied (Fig.2).

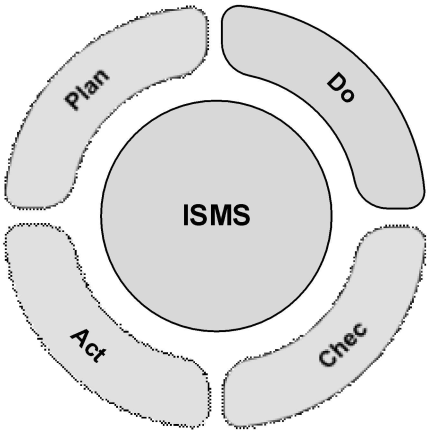

Fig. 2. Shewhart-Deming Cycle (Plan-Do-Check-Act) (PDCA)

To realise and support information security in the Company, four groups of processes shall be implemented:

1) "Plan" means to determine this Policy, goals, objectives, frameworks, processes, procedures, hardware and software related to management of the information security risks and information security improvement; to work out a plan for obtaining results in accordance with the general strategy and goals of the Company;
2) "Do" means implementation and maintenance of this Policy, control mechanisms, procedures, hardware and software, training and raising of awareness of the Company's employees;
3) "Check" means assessment of ISMS effectiveness and where applicable, measurement of characteristics of process execution in accordance with this Policy, goals and practical experience, analysis of changes in the external and internal factors affecting the protection of information resources, submission of the reports to management for analysis;
4) "Act" means taking of corrective and preventive measures based on results of internal and external checks of status of information security requirements on the part of the management, and other factors, to ensure ongoing improvement of the information security system.

5.6. The Company management, being aware of the significance of information security ensuring matters, shall initiate, support, analyse and monitor execution of the ISMS processes that contribute to establishment of conditions for further business development with acceptable risks.

CHAPTER 6. ISMS DEVELOPMENT AND IMPROVEMENT

6.1. This Policy shall determine the following key directions in the ongoing development and improvement of the ISMS:

1) *Allocation of functions and responsibility of the Company's employees in the area of information security ensuring* among the IT function, business function, management, risk management function and information security function*;*

2) *ISMC documentation management* – preparing, execution, approval, registration, storage, transfer and destruction of the ISMS-related documentation;

3) *information security risk management* – analysis of probable information security risks and probable consequences of occurrence thereof; making decisions on the actions to be taken by the Company to reduce risk up to acceptable level;

4) *monitoring, analysis of efficiency and improvement of ISMS processes* – ISMS analysis, which takes into consideration the results of security checks, statistics and additional information on the information security incidents occurred, results of assessment of efficiency of information security processes, and proposals and comments from all parties concerned;

5) *ensuring of information security when dealing with the personnel* – raising the awareness of the Company's employees in the information security matters at the time of recruitment, during the employment contract term or transfer to another position;

6) *increasing the level of knowledge and control of the knowledge of the Company's employees in the area of information security* – regular advanced trainings for employees of the business units, which fall within the ISMS scope, through delivery of trainings, information mailout, testing, etc.

7) *arrangement of work with the third party organisations* – ensuring of information security in work with the third party organisations, when providing access to the Company's information assets;

8) ensuring physical security and equipment protection;

9) *technical and organisational measures to ensure information security* – operation and improvement of mechanisms of information security ensuring;

10) *management of the Company IT infrastructure* – information security ensuring as part of the entire life cycle of IT infrastructure components;

11) *information security incident management* – ensuring monitoring of information security events and incidents and response mechanisms;

12) *business continuity management* – reduction of potential losses caused, inter alia, by accidents and failures in the Company IS, up to acceptable level by combining the preventive and corrective measures;

13) compliance with the legal requirements;

14) use of a licenced software;

15) *information security internal audits* – regular conduct of ISMS internal audits with a view to check the ISMS processes and control mechanisms.

CHAPTER 7. CONTROL OVER COMPLIANCE WITH REQUIREMENTS

7.1. Responsible business units of the Company shall exercise control, within the frameworks of their powers, over application and compliance with all provisions, procedures and standards of information security in accordance with the Company's internal regulations and legislation of the Republic of Kazakhstan.

CHAPTER 8. RESPONSIBILITY

8.1. Responsibility for ensuring the information security of the Company shall be imposed on all business units within the frameworks of their powers and according to the provisions set by this Policy and documents developed on the basis thereof.

8.2. Heads of the business units shall bear responsibility:

1) for timely communicating the requirements of the Company’s internal regulations in the area of information security to the employees of their respective business units to the extent related thereto;

2) for fulfilment by employees of their business units of the requirements of the Company’s internal regulations in the area of information security.

8.3. All employees of the Company shall bear personal responsibility for their actions when working in the Company’s information infrastructure and dealing with the protected information assets of the Company, as well as for compliance with the information security requirements set by this Policy and regulations drafted on its basis.

8.4. Responsibility shall be provided for the violation of the requirements of this Policy and documents drafted on its basis, in accordance with the internal regulations of the Company and legislation of the RK.

CHAPTER 9. REVIEW AND AMENDMENT PROCEDURE

9.1. Provisions of this Policy shall be reviewed on a regular basis but not less than once every two years.

9.2. Unscheduled review of this Policy shall take place in the following cases:

1) changes in the regulatory legal acts of the RK and internal regulation of the Company, which determine the information security requirements;
2) identified decrease in the general level of the Company’s information security (based on results of the internal audit or external audit);
3) significant changes in the organisation structure and/or infrastructure, resources and business processes of the Company;
4) identification of material weaknesses in the implementation of arrangements regulated by this Policy, and contradiction of its provisions with other internal documents of the Company.

9.3. This Policy shall be reviewed and amended in accordance with the procedure established by the Company.