For official use

Resolution No. 24/17 of the
Board meeting of "SendMN NBFI" LLC on October 22nd 2024,
Attachment 3

RISK MANAGEMENT POLICY OF "SENDMN NBFI" LLC

YEAR 2024

Document Code: SE/BD/IA/POL/01/24

Document title: Risk Management Policy of “SendMN NBFI” LLC

Version: 01

Revision Date: 2024

Classification: For Official Use

Revision history:

Version	Approval date, resolution number	Description of revision	Prepared by	Reviewed by
01		Initial version developed	Internal Audit and Risk Manager B. Namuundari	Risk and Audit Committee, Executive Director B. Turbold

CONTENTS

1. GENERAL PROVISIONS

1.1. The purpose of this policy is to establish the risk management system of "SendMN NBFI" LLC (hereinafter the "Company"); to identify, monitor, prevent, mitigate and control the risks that may arise in the course of its activities; to determine the level of acceptable risk; to create a control framework that ensures effectiveness; and to define the principles governing its implementation.

1.2. The risk management system shall consist of the types and scope of risks that may arise in the Company's operations; the levels of risk acceptance; risk assessment, monitoring, and response; reporting; the organizational structure, roles and responsibilities, functions and processes; and the policies, procedures, guidelines, and methodologies governing them.

1.3. The risk management policy is a fundamental document applicable to all employees and to their process as well as their decision making at every level of the Company, and is essential for establishing the risk management system.

1.4. In implementing this policy, the Company shall comply with the laws governing non-bank financial activities, the regulations and guidelines issued by the Financial Regulatory Commission on non-bank financial operations, other relevant legal acts of Mongolia, and the requirements of the international standard on risk management systems.

1.5. This policy and any additions or amendments thereto shall be approved by the Company's Board of Directors (hereinafter the "Board"), based on the recommendations of the Risk and Audit Committee (hereinafter the "Committee").

1.6. Glossary:

1.6.1. "Risk" means any event that may positively or negatively affect the Company's objectives, targets or other considerations;

1.6.2. "Business unit" means any department, team or branch of "SendMN NBFI" LLC;

1.6.3. "Risk governance" means the collective knowledge, attitudes and competencies of the Board of Directors, Executive Management and employees regarding their respective roles, responsibilities and active participation in the risk-management process;

1.6.4. "Key risk indicator" means a principal metric used to measure and monitor risk performance;

1.6.5. "Risk tolerance" means the maximum level of risk that may be assumed without exceeding the limits set by the regulator under current conditions;

1.6.6. "Risk acceptance level" /Risk appetite/" means the level of risk that the Company is willing to accept in order to achieve its business plan and strategic objectives;

1.6.7. "Risk limit" means the quantitative amount of risk that the company is willing to accept — directed at risks distributed across business units, specific risk categories and other levels — for the purpose of effective implementation of the company's approved risk exposure.

1.6.8. “Code of conduct” means the written document that defines the optimal standards of ethical and professional behavior to be observed on a day-to-day basis by the Company’s Board of Directors, Executive Management Team and all employees.

TWO. RISK MANAGEMENT SYSTEM

2.1. The company's risk management shall be implemented based on the "Three Lines of Defense" principle aligned with the goals and objectives of the company. Participation in risk management according to the three lines of defense shall be as follows, and risk shall be managed at an appropriate level. This includes:

2.1.1. First Line of Defense - This line comprises the business units responsible for owning and managing risks directly — namely, the primary risk-management implementers who, on a daily basis, identify, detect, respond to, monitor and control risks arising in connection with their operations.

2.1.2. Second Line of Defense - This line comprises the personnel responsible for implementing risk-management controls. Their duties include defining the risk-management framework; developing, reviewing and approving risk-management policies, procedures and guidelines; determining, approving and overseeing risk-acceptance levels and limits; and performing control and monitoring activities. The risk-management officer is also charged with organizing the First Line’s risk-management and control arrangements, monitoring its operations, and providing them with guidance and recommendations.

2.1.3. Third Line of Defense - This line provides independent assurance and is fulfilled by the Internal Audit department. The Internal Audit department independently evaluates and verifies that the risk-management and control processes implemented by the First and Second Lines of Defense are properly designed and operating effectively; it examines whether risk-management frameworks and related controls meet prescribed requirements; identifies weaknesses, deficiencies and opportunities for improvement; assesses root causes and the validity of outcomes; and reports its findings and recommendations to the Board of Directors’ Risk and Audit Committee.

2.2. The units responsible for implementing risk management shall, in conjunction with the Company's business strategy, plan, and budget, identify, measure, and manage the risks arising from the Company's daily operations, and work by aligning operational management with policy, determining whether the Company's risk management policy, procedures, and acceptable risk levels are appropriate, and making improvements.

2.3. The unit responsible for implementing risk management (the employee responsible for risk management) shall align it with the Company's strategic plan, business plan, the laws of Mongolia, regulations, and other international standards and requirements, and with the aim of ensuring the implementation of the improved policy and procedures, shall organize training, provide support and advice, promote it, present it, and oversee the implementation of risk management and the

acceptable risk levels within the scope of their respective duties, and work by monitoring from an independent standpoint.

2.4. The Internal Audit department shall, from an independent and impartial position, provide an evaluation of the effectiveness of the risk management framework and its systems.

2.5. The Executive Management and other authorized shall cultivate the Company's risk culture; guide and direct each employee's engagement and role responsibilities; and manage the Company's business operations within the risk-acceptance limits approved under this policy.

THREE. TYPES OF RISK

3.1. In order to ensure the continuity of the company's operations and business, the following types of risks are identified:

3.1.1. Strategic Risk – The risk that the Company's business strategy, strategic objectives or strategic plans become unachievable due to changes in the business environment, including, but not limited to, risks arising from competitor's risk, organizational risk, and political risk.

3.1.2. Financial Risk – The risk that the Company may be unable to generate sufficient operating income or meet its expenditure obligations, including, but not limited to, capital risk, liquidity risk, market risk and other related financial exposures.

3.1.3. Operational Risk – A risk of loss that may negatively impact the company's business objectives arising from inadequate or failed internal processes, people, and systems or the potential risk of financial and non-financial losses arising from external events. This includes, for example, process-related risk, human-resources risk, information-technology risk and risks associated with third-party relationships.

3.1.4. Compliance Risk - This refers to the risk of fines, penalties, or damages to reputation arising from violations of laws, policies, procedures, regulations, standards, and the company's internal rules, or from failure to comply with specific permits.

3.1.5. Credit Risk - The risk of financial loss arising when the Company's debtor or counterparty fails to perform its debt obligations, including the risk of loans not being repaid and other payment defaults.

3.1.6. Technology and Information Security Risk - This is the risk related to the information management system and includes the risk of failure of the information management system, incomplete resources, and loss of data and confidentiality.

3.2. The evaluation of the risk management system shall be a measure of its culture, and the joint participation, responsibility, and influence of all participating units on the decisions made shall be considered.

3.3. In the risk management system, all participating units shall manage their respective risks in accordance with the company's code of conduct and procedures.

FOUR. RISK ACCEPTANCE LEVELS

4.1. Within its risk-bearing capacity, the Company shall determine the amount of risk necessary to achieve its strategic objectives and business plan, establish the target level at which those activities are to be executed, and issue a definition of the corresponding risk amount.

4.1.1. The Company’s financial and non-financial resources determine its risk-bearing capacity.

4.1.2. Financial resources are defined by its own capital and profit; non-financial resources are defined by employees’ capabilities, knowledge, information-technology systems, internal policies, procedures, instructions, controls and reporting systems.

4.1.3. The Company shall not accept risks in excess of the limits set by its international agreements, conventions, laws or regulatory requirements, and its risk-bearing capacity shall comply with those limits.

4.2. Risk Appetite:

4.2.1. The Company’s risk appetite shall be aligned with its business and strategic plans and shall not exceed its risk-bearing capacity.

4.2.2. The First Line of Defense shall define, measure and report the risk appetite applicable to its responsibilities, and with the Second Line of Defense monitoring.

4.2.3. The risk appetite shall be determined for each specific circumstance—taking into account market conditions and the Company’s business decision-making—and shall ensure that it does not exceed the risk-bearing capacity.

4.3. Risk Limits:

4.3.1. To maintain risk exposure at appropriate levels, the officer responsible for Risk Management shall develop risk limits—based on the Company’s approved risk-acceptance thresholds and the opinions of each business unit or activity—and submit them to the Chief Executive Officer for approval.

4.3.2. Risk limits shall set boundaries within the overall risk-acceptance level and the distribution and allocation of risk across different business units.

4.3.3. Risk limits must be measurable, aimed towards the future and aligned; in this way, risks will remain within the Company’s risk-bearing capacity and aligned with its protective framework.

4.4. Risk Measurement

4.4.1. Risk measures shall be calculated by evaluating each risk against its applicable risk limits, approved risk-acceptance levels and the Company's overall risk-bearing capacity.

4.4.2. Risk assessments shall be conducted using a methodology based on the likelihood of each event and its potential impact. The Risk Management Officer shall provide assessment methods, make improvements and work to offer and monitor units guidance and instruction on how to develop such assessments.

4.4.4. At the company level, the Risk Management Officer shall organize and conduct risk assessments at least once annually, and the assessment results together with the risk-mitigation action plan shall be approved by the Executive Director's official order.

4.4.5. Based on the risk assessment, the Company shall identify its key risks at the organizational level and may adjust and recalibrate the limits and risk-acceptance levels for those risks.

FIVE. PRINCIPLES OF RISK MANAGEMENT

5.1. The following principles shall govern the risk-management framework, with the objective of improving operational outcomes and performance, enhancing the Company's value and economic returns:

5.1.1. Value creation – Risk management must protect the Company's core values; respect law and order, improve strategic implementation, increase competitiveness, improve performance, and be a company with a high reputation and value that is accepted by the public.

5.1.2. Responsibility to the customer – The company shall strive to fulfill its obligations to its shareholders and all customers and partner organizations, in addition to calculating the risks that may arise in its own operations.

5.1.3. To be an integral part of all operations – Risk management shall be the responsibility of the Company's Executive Management and authorized officials, and they shall have the duty to comply with and monitor it in their daily operations.

5.1.4. To be part of the decision-making process – Risk management aims to enable employees to make decisions based on information rather than intuition, and to prioritize and address the most critical or high-risk issues first.

5.1.5. To be systematic, coherent, and timely, and to work towards creating consistent, reliable, and positive results.

5.1.6. To be based on reality – Risk management shall be based on and implemented with factual information such as historical data, feedback from other units, observations, forecasts, and risk assessments.

5.1.7. To be adaptive – Events and risks may change depending on external and internal environmental conditions. Therefore, risk management approaches will be updated and improved.

5.1.8. To be transparent – To anticipate and identify potential future risks to the company and to ensure that every employee is aware of all known risks.

5.1.9. To ensure the involvement of all parties – To appropriately involve all company employees in the implementation of risk management. To create conditions where risk management is relevant to every member of the company, and to establish an environment where every employee can express their opinions and voice their ideas in identifying risks.

5.1.10. To balance risk and return – The company shall maintain and control the optimal balance of risk and return in all its operations.

5.1.11. To be independent and autonomous – The implementation of risk management shall be assessed and evaluated from an independent and impartial standpoint.

5.1.12. To report – Every employee of a unit shall promptly report any identified risk to their direct supervisor. All levels of management shall regularly and accurately report on risks related to their responsible unit and its activities to the 2nd line of defense and the unit responsible for risk.

5.1.13. Continuous improvement – Risk management must be constantly improving through learning and experience. New circumstances, experiences, mistakes, violations, and shortcomings that arise during the implementation of risk management shall be incorporated each time, making necessary amendments and improvements to the risk management policy. It is also required to adjust and update in line with changes in the legal environment and policy documents.

5.2. Risk Culture – All employees of the Company shall adhere to the risk management policy, procedures, and instructions, be knowledgeable and informed about risk, and have a duty to identify, assess, and manage potential risks when carrying out their responsibilities and duties. To foster a risk culture, the Company shall organize training for all employees aimed at changing attitudes towards risk, in addition to teaching risk management techniques.

SIX. IMPLEMENTATION OF RISK MANAGEMENT

6.1. The Company shall implement risk management through the following process.

6.1.1. Defining Risk Management Functions – By defining the functions of risk management, the 1st and 2nd lines of defense will jointly determine the plan, functions,

and duties for how to identify, assess, respond to, and monitor risk, depending on the type of risk and operations.

6.1.2. Identifying/Defining Risk – The 1st line of defense shall define the risks that may occur in operations within the scope of its responsible activities and functions, and every risk identified at this stage shall be recorded in the Risk Register and reported to the 2nd line of defense on each occasion.

6.1.3. Risk Assessment – As the company cannot manage every identified or defined risk, risks will be assessed using qualitative and quantitative indicators to determine the risk level, and a classification for taking response measures will be established by prioritizing the specific risks.

6.1.4. Prioritizing Risk – Based on the risk level, a risk score will be determined, and the requirement and priority for taking response measures for that specific risk will be determined based on the risk score.

6.1.5. Response measures – Based on the identified risks and their assessment, the Company shall plan and implement response measures to protect against risks in the following areas. These include:

- Preventive measures, or measures aimed at protecting against the occurrence of a risk, reducing the probability of its occurrence, and mitigating it.
- Risk reduction measures, or measures aimed at reducing the consequences of a risk that has occurred.

6.2. In managing risk, one or more of the following measures may be implemented together, based on the consideration of the acceptable level of risk.

Response Measure	Implementation Measure
Protection from Risk	Manage the risk, rather than avoid it. Focus on taking measures that would yield an identical outcome, or consider not implementing by selecting alternative methods.
Reducing Risk	Improve management control and operations, and reduce the probability of occurrence.
	Develop and implement a strategy to reduce negative consequences to the lowest possible level – For example, contingency plans, business continuity plans, and protection of contractual liability.
Transferring Risk	On a contractual basis, transfer the liability in whole or in part to the other party/a third party, or to insurance.
Accepting Risk	Accept the risk if internal controls are considered adequate, formalize the monitoring, and develop a contingency plan for necessary parts.

SEVEN. RIGHTS AND RESPONSIBILITIES OF STAKEHOLDERS

7.1. The Company's units shall participate with the following functions. These include:

7.1.1. Board of Directors:

- Approve, revoke, and oversee the implementation of the risk management policy;
- Assign the duty and oversee the implementation of the Risk Management system to ensure it is fully executed by promptly identifying instances where risk limits and restrictions have been exceeded, managing them effectively, and taking reduction measures.
- Lead and participate in fostering a risk culture within the company.

7.1.2. Executive Director:

- Approve acceptable risk levels that are consistent with the company's short and long-term strategic plans, business plans, capital planning, risk appetite, and restrictions set by regulatory bodies;
- Oversee and provide guidance for the effective implementation of the risk management system by promptly identifying, effectively managing, and reducing instances of material risks that have exceeded or are approaching their limits;
- Oversee whether the risk limits, strategic plans, financial plans, and decision-making processes of business units are consistent with the acceptable level of risk;
- Provide appropriate oversight to ensure that the process of identifying, measuring, monitoring, and reporting risks is implemented continuously and effectively and is capable of supporting business units;
- Organize and furnish all types of resources and specialists—spanning risk management, financial accounting, and information technology infrastructure—required to ensure the efficiency of the risk-management framework;
- Report to the Board, without delay, any material risk events that exceed established risk limits or anticipated thresholds;
- Monitor the execution of the risk-management policy.

7.1.3. Internal Auditor:

- Conduct an independent assessment of the implementation of the Risk Management Framework at the company-wide level and within each business line and process; report the results to Executive Management and submit a report to the Board of Directors.

- Provide recommendations and advice to the First and Second Lines of Defense for improving the Risk Management Framework.
- Investigate the root causes of unauthorized risks; develop proposals for corrective measures to be taken by the responsible personnel; and notify Management, the Human Resources Department, and Executive Management of these proposals.

7.1.4. Risk Management Officer (Second Line of Defense):

- Define the scope of acceptable risk in alignment with the Company's short- and long-term strategic plans, business plans, capital planning, risk-bearing capacity and the limits set by regulators; present these accepted risk levels to the Chief Executive Officer.
- Secure the Board's approval for the accepted risk levels and risk limits; continuously monitor compliance; and report on them to the Board's Risk and Audit Committee.
- Develop and implement methodologies for risk identification, assessment, and measurement.
- Prepare a comprehensive risk-management plan that is true and complete and present it to Executive Management.
- Provide all company employees with training and information on risk-management principles;
- Monitor whether material risks that have exceeded or are approaching established risk limits are being managed effectively by business units.
- Promptly inform the Chief Executive Officer of any material risk events—or anticipated occurrences—that exceed the risk appetite and could materially impair the company's financial condition.

7.1.5. Units in the First Line of Defense:

- Implement and maintain an effective risk-management framework within their own business unit, including processes for risk identification, monitoring, reporting and system development;
- Monitor and enforce compliance with approved risk-tolerance levels, business-unit plans and decision-maker mandates;
- Foster a risk-aware culture throughout the company by embedding approved risk tolerances and limits into day-to-day operations;
- Value and support the oversight functions of the Risk Management Officer and Internal Audit—sharing findings and collaborating on remediation;

- Effectively manage and mitigate any material risks that have breached or may breach established limits, and promptly notify the Chief Executive Officer and Risk Management Officer of such events;
- Provide timely risk-related information and reporting to the Second Line of Defense.

EIGHT. INTERNAL AUDIT AND ASSURANCE

8.1. Through continuous monitoring, Internal Audit shall provide independent assurance on the design and operating effectiveness of the Company's Risk Management Framework and its implementation; serve as a key contributor to its ongoing enhancement by evaluating the efficiency and effectiveness of internal controls; and support the Company in establishing a robust internal-control system through continual improvement.

8.2. In accordance with the annual plan and programs approved by the Board's Risk and Audit Committee, assess the outcomes of the Company's risk-management activities and provide recommendations for improvement to the First and Second Lines of Defense.