APPROVED:
By Order of the General Director of PrimeTech LLC dated October 29, 2024, No. 1

POLICY
on Risk Assessment and Management in the Payment System of PrimeTech LLC

Bishkek, 2024

1. GENERAL PROVISIONS

1.1. This Policy on Risk Assessment and Management in the Payment System (hereinafter — the Policy) of PrimeTech LLC (hereinafter — the Company) defines the objectives, tasks, fundamental principles of the risk management system and the organization of internal control, providing for the application of risk control methods that ensure effective identification, assessment, and limitation/mitigation of the Company's risks to maintain the reliability and efficiency of the payment system.

1.2. This Policy establishes the minimum requirements for risk management related to the Company's activities. Risk management in the PrimeTech payment system is aimed at ensuring uninterrupted functioning of the payment system of the Kyrgyz Republic through identification, assessment and analysis, monitoring, prevention, and mitigation of risks.

1.3. The Policy has been developed in accordance with the current legislation of the Kyrgyz Republic and the regulatory legal acts of the National Bank of the Kyrgyz Republic (hereinafter — NBKR).

1.4. For the purposes of implementing this Policy, instructions and procedures shall be developed for the implementation of measures aimed at limiting risks and making management decisions on the regulation of the PrimeTech payment system operating on the territory of the Kyrgyz Republic.

2. KEY DEFINITIONS

2.1. The following concepts and terms are used within the framework of this Policy:

"Risk" — the probability that expected or unforeseen events may have a negative impact on the Company's capital or its income.

"Risk Management System" — internal organizational measures that establish the risk management process consisting of the following four main stages: risk identification, risk measurement, risk control, and risk monitoring, and also includes an additional element for the implementation of risk management measures. **"Risk Management"** — a process that includes identification, risk assessment, development and implementation of risk management measures, as well as risk monitoring.

"Risk Level" — an assessment of the significance of a risk depending on the probability and the extent of potential damage from its realization.

"Business Process" — several related tasks or procedures that collectively achieve a specific objective of current activities within the existing organizational structure of the Company.

"Risk Owner" — a structural unit or an official responsible for managing the respective risk, including identifying and ensuring sufficient risk response methods and control procedures, and ensuring their operational effectiveness. The risk owner is responsible for the implementation of risk management measures and risk monitoring.

"Risk Map/Matrix" — a graphical and textual description of the company's risks arranged in a rectangular table. The risk map includes risk assessment criteria, namely the level of damage from risk realization and the probability of the risk event occurring within a defined period of time.

"Risk Register" — a table containing structured information about risks: risk names, risk descriptions, key causes and factors of risk occurrence, description of potential consequences of risk realization, risk assessment, risk owners, risk management measures, timelines and status of their implementation.

"Risk Management Measures" — actions developed based on one of the following management methods:

1. Risk avoidance;
2. Risk mitigation;
3. Risk transfer (redistribution);
4. Risk acceptance.

"Risk Identification" — the process of detecting and describing potential risks, their causes and consequences.

"Risk Monitoring" — systematic updating of information on the risk level and external or internal factors affecting the risk level, as well as on the status of risk management measures.

"Risk Assessment" — the process of determining the risk level by assigning to each risk a magnitude of potential damage and the probability of such damage occurring, for the purpose of further development of risk management measures.

"Uninterrupted Functioning of the Payment System" — the organization and provision of payment system operation to prevent violations of legislation requirements, payment system rules, concluded contracts and agreements, use of information and communication technologies, technical maintenance of the payment system during interaction of payment system participants, as well as restoration of proper functioning of the payment system in case of their violation.

"Risks in the Payment System" — the probability of adverse events and risks that may negatively impact or result in improper fulfillment of the objectives, tasks, and functions of the payment system as a whole.

"Components of the Payment System" — payment systems designed for conducting interbank payments and settlements (large-value payment system, retail payment systems), and other interrelated payment system technologies through which payments and settlements are made within the rules of the payment system.

3. OBJECTIVES AND TASKS

3.1. The main objective of the Policy is to minimize the Company's risks to ensure uninterrupted functioning and reduce the degree of influence of risk factors on systemic risk, which will generally contribute to increased efficiency and security.

3.2. Achieving risk management objectives in the PrimeTech payment system involves the following tasks:

- Forecasting adverse events, the realization of which could disrupt uninterrupted functioning of the payment system;
- Prevention and avoidance of the possibility of risk realization;
- Identification (detection) of risks and determination of the causes of their occurrence;
- Assessment of risk levels;
- Continuous monitoring and analysis of risks;

- Organization of a process for timely elimination of the consequences of risk realization and creation of mechanisms for system recovery in case of disruption.

4. RISK MANAGEMENT SYSTEM

4.1. Participants and Their Functions

4.1.1. The risk management structure in the Company includes the involvement of the following bodies, officials, and structural units:

- General Director and Executive Management Body;
- Heads of structural units;
- Other employees.

4.1.2. The General Director / Executive Management Body of the Company:

- Is responsible for organizing effective risk management that allows identifying, assessing, and managing the Company's risks;
- Approves the Company's risk map and risk register;
- Approves the list of measures for managing existing risks;
- Approves the list of risk owners;
- Designates a risk management coordinator (official) (the Risk Management Coordinator may be any employee of the organization who will aggregate and update risk information in the Company on an annual basis);
- Uses risk information in making management decisions.

4.1.3. Heads of Structural Units:

- Ensure compliance with the Procedure provisions by employees of their structural units;
- Provide risk information within their area of competence to the RM Coordinator for updating the risk map and risk register;
- Ensure timely development and implementation of risk management measures approved by the General Director;
- Allocate resources when necessary for taking prompt risk management actions or reducing the negative consequences of already realized risks;

- Optimize business processes to reduce the level of risks or the consequences of their realization;
- Use risk information in setting the objectives of the structural unit.

4.1.4. Risk Management Coordinator:

- Coordinates the work of structural units on risk identification and assessment, as well as the development of risk management measures;
- Ensures updating of the Risk Management Procedure;
- Aggregates risk information and prepares risk reporting for the Company in accordance with this Procedure;
- Develops and conducts activities aimed at fostering a risk management culture in the Company (as necessary).

4.1.5. Other Employees:

- Carry out risk identification within their area of competence;
- Implement approved risk management measures;
- Monitor risk levels within their area of competence.

4.2. RISK MANAGEMENT PROCESS

4.2.1. Risk Identification

4.2.1.1. Risk identification (detection) is a process in which internal or external events are determined, the realization of which may negatively affect the Company's achievement of its set objectives.

4.2.1.2. The Company's risks must be identified as needed and updated on an annual basis.

4.2.1.3. Risks may be identified in the following ways:

- Within the framework of a strategic session when defining objectives and tasks for the current or following year. The RM Coordinator is responsible for preparing and coordinating the part of the discussion dedicated to risk identification;
- Within the framework of working groups dedicated to identifying risks associated with the implementation of the Company's strategy. The RM Coordinator is responsible for organizing and conducting working meetings;

- Within the framework of individual interviews with the heads of the Company's structural units. The RM Coordinator is responsible for organizing such interviews, keeping minutes, and aggregating risk information.

4.2.1.4. Based on the results of risk identification activities, information on identified risks for subsequent assessment and management, with the designation of owners, is entered into the risk map, which is approved by the General Director.

4.2.2. Risk Assessment

4.2.2.1. Risk assessment is conducted to determine risk levels and identify the most significant (critical) risks that may negatively affect the Company's activities and the achievement of strategic objectives.

4.2.2.2. Assessment of identified risks is carried out by risk owners and aggregated by the RM Coordinator.

4.2.2.3. Risk assessment may be conducted in the following ways:

- Collectively, in the format of a risk assessment working meeting, where heads of structural units / risk owners assess risks;
- Individually, by completing the relevant sections of the risk register, which is sent to risk owners with a list of identified risks and criteria for risk assessment.

4.2.2.4. For each identified risk, it is necessary to assess the damage to the Company from the realization of such risk and the probability of its realization.

4.2.2.5. Damage from risk realization is assessed on a three-point scale:

- **High** — risk realization may lead to suspension of payment operations for more than 2 days, a significant (above 40%) decrease in income or increase in the Company's expenses, and/or significant reputational damage to the Company;
- **Medium** — risk realization may lead to suspension of payment operations from 2 hours to 2 days, a moderate (20%) decrease in income or increase in the Company's expenses, and/or insignificant reputational damage;
- **Low** — risk realization may lead to suspension of payment operations for up to 2 hours, an insignificant (< 5%) decrease in income or increase in the Company's expenses.

4.2.2.6. The probability of risk realization is assessed on a three-point scale:

- **High** — the risk has already been realized repeatedly in the past, there is a high degree of uncertainty regarding the probability of risk realization, or there are internal or external prerequisites indicating that the risk is likely to be realized within a year;
- **Medium** — the risk is likely to be realized within a year;
- **Low** — it is unlikely that the risk will be realized within a year.

4.2.2.7. Based on the assessment results, the Company's risks can be divided into three levels:

- **High risks** — such risks are unacceptable for the Company and require active management action. Decisions on mitigating such risks are made at the level of the General Director of the Company. Decisions on these risks have the highest priority in terms of implementation timelines and financial resource allocation;
- **Medium risks** — decisions regarding such risks are made at the level of the Company's structural units and risk owners. Implementation timelines are established based on the availability and financing schedule of management decisions, as well as the optimal time required for implementing a specific measure;
- **Low risks** — these risks are acceptable for the Company and do not require significant financing. Decisions taken are limited to the implementation of procedures that ensure prevention and reduction of the negative consequences of risk occurrence. Risk boundaries are defined, and risk monitoring is carried out to take action in case of a change in the risk level.

4.2.2.8. Each risk is graphically displayed on the risk map based on information about the damage and probability of risk realization obtained from risk owners:

Damage from risk	High			
	Medium			
	Low			
		Low	Medium	High
		Probability		

4.2.2.9. Information obtained during the risk assessment process is reflected in the risk register.

4.2.2.10. Based on the results of risk identification and assessment, the risk map and risk register are submitted to the General Director for approval.

4.2.3. Development and Implementation of Risk Management Measures

4.2.3.1. For risks that fall into the red zone on the map, action plans for managing these risks are developed, including implementation timelines and responsible persons.

4.2.3.2. Risk management measures must be developed based on one of the following methods:

- **Risk avoidance** — risk avoidance implies refusal to perform certain actions, refusal of assets characterized by high risk. Risk avoidance is applied in exceptional cases as a risk coverage method and is used when the cost of risk impact is too high or when such impact will not reduce the risk to an acceptable level, as well as when the risk cannot be effectively transferred to a third party;
- **Risk mitigation** — impact on risk by reducing the probability of risk realization and/or reducing negative consequences in case of risk realization in the future;
- **Risk transfer (redistribution)** — transfer or partial transfer of risk to another party (for example, through insurance contracts, hedging, outsourcing, etc.), which reduces the negative impact on the achievement of the Company's objectives;
- **Risk acceptance** — the Company acknowledges the possibility of adverse risk consequences with the identification of specific sources to cover damage from such consequences.

4.2.3.3. The most acceptable method of risk management is avoidance or mitigation. If risk mitigation is impossible or impractical, employees of structural units must develop alternative measures for risk transfer or acceptance. The least effective method of risk management is risk acceptance.

4.2.3.4. After receiving information on risk management measures from risk owners, the corresponding sections of the Company's risk register are updated, after which the updated register is submitted for approval by the General Director of the Company.

4.2.4. Risk Monitoring

4.2.4.1. As part of monitoring, the risk map and risk register (including risk management measures) are updated at least once a year. They may be updated more frequently if necessary.

4.2.4.2. As part of risk monitoring:

- New risks not documented in the risk map and risk register are identified;

- The risk level assessment is reviewed;
- The status of implementation and effectiveness of risk management measures is reviewed. Additional risk management measures are developed if necessary.

4.2.5. Risk Reporting

4.2.5.1. As necessary, responsible employees prepare a report for the General Director of the Company and other management bodies.

5. LIQUIDITY RISK MANAGEMENT

5.1. Liquidity risk is a risk arising from the inability of a payment system participant to ensure the full fulfillment of its obligations due to insufficient or lack of funds. Liquidity risk does not mean that the payment system participant is insolvent. It is able to make settlement on its obligations, but not at the precisely established deadlines in the future. The probability of this type of risk is associated with an imbalance between the financial assets and financial liabilities of the payment system participant.

5.2. Liquidity Risk Management System

5.2.1. Liquidity risk management in the Company is ensured by:

- General Director;
- Chief Accountant;
- Operations Accountant.

5.2.2. The General Director, for the purpose of effective liquidity risk management, performs the following functions:

- Defines and adopts the liquidity management strategy in the Company;
- Determines the frequency of payments to suppliers and the amount (limits) of guarantee sums;
- Controls the Company's continuous and effective liquidity management;
- Determines the format and frequency of information provided to him for monitoring liquidity in the Company;
- Approves additional procedures and instructions for minimizing liquidity risk (as necessary).

5.2.3. The Chief Accountant and Operations Accountant:

- Conduct monitoring of account balances with payment system participants on an ongoing basis;
- Conduct ongoing monitoring of guarantee sum contributions covering the volume of payments processed by the system participant; when changes are necessary, submit proposed limits for consideration by the General Director;
- When necessary, coordinate with the General Director all deviations from established limits.

5.2.4. In case of liquidity difficulties, with the General Director's approval, the following liquidity risk management methods may be implemented:

- Liquidity planning across various time horizons;
- Monitoring the ratio of liquid assets to short-term liabilities;
- Conducting assessment, monitoring, and control of the liquidity position by currency, managing liquidity in foreign currencies (if foreign currency operations exist);
- Daily monitoring and measurement of cash inflows and outflows, as well as daily monitoring of maturity gaps between highly liquid assets and short-term liabilities to control daily needs for short-term and instant liquidity and ensure fulfillment of short-term obligations;
- Forecasting required short-term and instant liquidity.

6. CREDIT RISK MANAGEMENT

6.1. Credit risk is a risk arising from the inability of a payment system participant to fulfill its financial obligations for payment for rendered payment infrastructure services to other participants when payment falls due or at any subsequent time. Credit risk poses a threat to the financial stability of payment system participants, which may affect the uninterrupted functioning of the payment system. Credit risk may arise when interacting with suppliers to whom the Company makes advance payments for future payments.

6.2. Credit Risk Management System

6.2.1. Credit risk management in the Company is ensured by:

- General Director;
- Chief Accountant;
- Operations Accountant.

6.2.2. The General Director, for the purpose of effective credit risk management, performs the following functions:

- Defines and adopts the Company's Credit Strategy;
- Determines the frequency of reviewing the amount of advance payments and the composition of suppliers with whom the Company will work on a prepayment basis;
- Controls the Company's continuous and effective credit risk management;
- Determines the format and frequency of information provided to him for monitoring credit risks accepted by the Company;
- Approves additional procedures and instructions for minimizing credit risk (as necessary).

6.2.3. The Chief Accountant and Operations Accountant:

- Monitor the financial condition of suppliers with whom the Company works on a prepayment basis;
- Conduct ongoing monitoring of payment amounts required to cover established advance limits and, when changes are necessary, submit proposed limits for consideration by the General Director.

7. OPERATIONAL RISK MANAGEMENT

7.1. Operational risk is a risk arising from disruption of hardware and software systems, improper actions of payment system entity personnel, as well as the impact of external factors, the realization of which causes the inability to process payments and settlements due to technical failures in hardware and software systems and communication channels, malfunction of technical infrastructure, violations of payment system rules, information protection requirements, or the inability of the payment system to function as a whole.

7.2. Technological Risks — Hardware and Software System Failures and Malfunctions

7.2.1. To minimize technological operational risks in the system, there must be procedures in place to ensure the functioning of the payment system in the event of emergency situations and other failures and malfunctions.

7.2.2. For these purposes, the Technical Director ensures and controls:

- **Business continuity of the Company**; effective procedures and actions for contingencies and business continuity plans must be developed, taking into account information backup, as well as permanent storage of such backup information in a separate location, with the following:
  - Duplication of hardware and software at the primary node;
  - Duplication at the backup center of the primary node's hardware and software complex;
  - Duplication of communication channels to ensure continuous communication between the primary node and automated workstations of participants;
  - Organization of uninterrupted power supply for primary and backup nodes;
- **Information protection** from unauthorized access, secure information transmission and computer network security, preservation of software and databases;
- **Monitoring** of unauthorized actions in information systems, maintenance of electronic registration logs for failures, malfunctions, and emergency situations.

7.2.3. The Technical Director develops and submits to the General Director for consideration the policies and procedures to ensure the tasks specified in clause 7.2.2.

7.3. Human Resources Risk

7.3.1. The primary method of minimizing operational risk controlled at the Company level is the development of an adequate organizational structure, clear distribution of authority among units and employees, and development of internal rules and procedures.

7.3.2. Special attention must be paid to compliance with the principles of separation of duties, approval (authorization) procedures, accountability and cross-checking procedures in all Company operations.

7.3.3. Control and minimization of operational risk involves the following:

- Heads of structural units and Company officials control compliance with established limits and authority boundaries by Company employees;
- Heads of structural units ensure proper selection and training of personnel, conclusion of necessary contracts and agreements on full financial liability.

7.3.4. Fraud risk arises from unlawful actions of employees and officials of payment system participants, including abuse of official position, unauthorized use of official information, theft of funds, intentional concealment of facts of transactions within the payment system, as well as

unlawful actions of third parties against the payment system, such as theft of personal data, obtaining confidential information, database intrusion for the purpose of stealing funds, etc.

7.4. Risks of Illegal Use of Information Resources and Software / Hacker Attack Risk

7.4.1. Hacker attack risk is a risk arising from the impact on information resources and information and telecommunication facilities of the payment system through unauthorized access to information systems, deployment of special technical means, infection with computer viruses and other malware in order to obtain personal information of payment infrastructure service users (passwords, PIN codes, bank card numbers, electronic signature equivalents, personal user data), destruction and breach of database integrity, blocking and disabling information computer systems.

7.4.2. To minimize hacker attack risk, the Technical Director ensures and controls:

- Compliance with established information access procedures, provision of authorization and authentication means for system participants and personnel, protection of the Company's material assets, and specialized premises within the Company;
- Information security, implementation of measures to protect client information from unauthorized access, ensuring information integrity, timely updating and upgrading of information security systems, detection of vulnerabilities in information systems, and application of antivirus protection measures.

7.4.3. The Technical Director develops and submits to the General Director for consideration the policies and procedures to ensure the tasks specified in clause 7.4.2.

8. COMPLIANCE RISK MANAGEMENT

8.1. The objective of compliance risk management is to ensure compliance with the requirements of the legislation of the Kyrgyz Republic, NBKR regulatory documents, and legislation on the prevention of terrorist financing and money laundering.

8.2. Legal risk is a risk arising from non-compliance with the requirements of the legislation of the Kyrgyz

Republic, regulatory legal acts of the NBKR, terms of contracts and agreements, internal documents of banks, operators, and participants of payment systems, payment organizations

that define the norms and rules for the functioning of payment systems, imperfections in the legal system, frequency of changes in legislation, as well as the presence of legal uncertainty in relations with other payment system participants, which may serve as grounds for and lead to litigation between payment system participants.

8.2.1. All internal regulatory documents and contracts concluded by the Company, as well as client contract templates, undergo legal review by the Company's Lawyer for compliance with legislative requirements.

8.2.2. Heads of structural units are responsible for using the approved form of contract with clients and other parties.

8.3. Organization and Control of Compliance Risk Management for CFT/AML

8.3.1. For effective compliance risk management in combating the financing of terrorism (CFT) and anti-money laundering (AML), an assessment mechanism based on a risk-based approach is established for conducting regular general assessment and reassessment of risks, for the effective distribution and control of CFT/AML risks.

8.3.2. The General Director of the Company ensures an effective compliance risk management system for the prevention of terrorist financing and money laundering (hereinafter — CFT/AML).

8.3.3. The Compliance Control Department organizes an effective internal control system for CFT/AML and develops special policies and procedures for managing and minimizing CFT/AML compliance risk.

8.3.4. The detailed risk assessment methodology and risk management procedure are established in a specialized internal regulatory act of the Company.

8.3.5. CFT/AML compliance risk assessment is carried out according to the following categories:

- Risk by client category;
- Risk by types of products and services;
- Risk by type of delivery channel or service provision;
- Risk by geographic (country) classification.

8.3.6. Risk levels are defined as high, medium, and low.

8.3.7. Within the framework of the CFT/AML compliance risk minimization and management plan, the Compliance Control Department must conduct the following actions and describe them in special policies and procedures:

- Client identification and verification;
- Document collection and storage;
- Reporting on transactions above the threshold amount (if defined);
- Reporting suspicious and other required transactions to the authorized government body;
- Reporting in accordance with the legislation of the Kyrgyz Republic on CFT/AML;
- Screening procedures when hiring new employees;
- Ongoing employee training plan;
- Regular review of CFT/AML compliance risk and changes in the legislation of the Kyrgyz Republic.

9. REPUTATIONAL RISK MANAGEMENT

9.1. Reputational risk is a risk arising from the formation of a negative perception of the stability of the payment system, a negative assessment of the quality of services provided in the payment system, including as a result of the dissemination of false information, leading to a loss of trust in the payment system or payment system participants.

9.2. Reputational risk management is carried out by:

- General Director;
- Lawyer;
- Control Manager;
- Head of the Client Relations Department;
- Compliance Control Department — through establishing in the Company (via the General Director) a system for:
- Effective corporate governance and internal control regulating ethics and professional conduct toward clients and the Company;
- Prevention of terrorist financing and money laundering.

9.3. When assessing the level of reputational risk, the Company is guided by the following indicators:

- Changes in the Company's financial condition (sharp changes in profitability, asset and liability structure);
- Changes in the number of complaints and claims against the Company;

- Negative reviews and reports about the Company;
- Detection within the internal control system for the prevention of terrorist financing and money laundering of cases of non-compliance with legislative requirements and signs of possible involvement of the Company or its employees in such activities;
- Detection of facts of theft, forgery, fraud in the Company, and employees' use of confidential information obtained from clients for personal purposes.