APPROVED:

By Order of the General Director
of PrimeTech LLC
dated November 19, 2024, No. 4
(Seal)

RULES OF THE PAYMENT SYSTEM OF PRIMETECH LLC

Bishkek, 2024

1. GENERAL INFORMATION

1.1. These Rules of the "PrimeTech" Payment System (hereinafter referred to as the "Rules") establish uniform conditions for the activities of PrimeTech Limited Liability Company and set forth the standard rights, obligations, and responsibilities of the Participants of the "PrimeTech" Payment System.

The Participants of the Payment System are the Payment System Operator (Payment Organization), Payment Agents/Sub-agents, Goods/Services Providers, and users. Any individual entrepreneur or legal entity that has declared its accession to the Rules and signed the corresponding agreement may become a Payment Agent/Sub-agent, provided that such person accepts the terms of the Rules in their entirety, in accordance with Article 387 of the Civil Code of the Kyrgyz Republic. Each Party guarantees to the other Parties that it possesses the necessary legal capacity, as well as all the rights and powers necessary and sufficient for accession to the Rules and the fulfillment of obligations in accordance with their terms.

1.2. These Rules govern the procedure and conditions for the functioning of the System, the interaction of Participants, establish the legal and organizational foundations for the construction and functioning of the System, the conditions and procedure for accession to the System, the conditions and procedure for the provision and use of the System's Services for the purpose of making Payments, as well as other provisions necessary for the functioning of the System. The Payment System Operator exercises control over compliance with the System Rules by Participants.

1.3. Within the framework of monitoring compliance with the Rules in accordance with the requirements of legislation, the Payment System Operator:

- monitors compliance with these Rules, the current rules and procedures of the System, as well as their compliance with the requirements of the legislation of the Kyrgyz Republic;
- establishes requirements for the necessary technical and software means for making payments to other Participants of the payment system;
- maintains a database of Agents, Sub-agents, and Goods/Services Providers of the payment organization;
- assesses and manages risks in the payment system;
- ensures the secure functioning of information processing facilities;
- ensures a unified approach to incident management and maintains an incident register;
- ensures timely delivery of information on Payments accepted into the system to the Goods/Services Provider in the event of an emergency situation in accordance with the terms of the agreement and the requirements of regulatory legal acts of the National Bank of the Kyrgyz Republic.

1.4. In the event that amendments to regulatory legal acts governing the activities of the Operator and the payment system come into force, the provisions of which contradict the requirements and clauses set forth in these Rules, including the Appendices, the legislative norms that have come into force shall apply, and the Rules shall be brought into compliance with the established requirements by making amendments and additions.

1.5. The Payment System Operator (Payment Organization) has the right to unilaterally make amendments and additions to these Rules by publishing a new version of the Rules containing information about such amendments on the System's website www.primetek.kg. Amendments shall come into force upon the expiration of 15 (fifteen) business days from the date of publication, unless a different effective date for the amendments is additionally specified upon their publication. A System Participant undertakes either to accept the amendment to the terms of the Rules, or to provide the Operator with a response declining the amendment to the terms of the Rules before the amendment comes into force. In the event that no response declining the proposal is submitted, the proposal to amend the terms of the Rules shall be deemed accepted by the Participant. In the event of a Participant's disagreement with amendments to the terms of the Rules, the parties have the right to terminate the Payment System Participant Agreement, having first completed all settlements.

1.6. The Payment System Operator (which combines its activities with the activities of a Payment Organization) is PrimeTech Limited Liability Company, which is the Payment System Operator and combines its activities with the activities of a Payment Organization.

1.7. PrimeTech Limited Liability Company carries out its activities on the basis of the following licenses:

- Payment organization license No. 3061051224 dated 5th day of December, 2026 for the provision of services for accepting and processing payments and settlements for goods and services that are not the result of its own activities, in favor of third parties through payment systems based on information technologies and electronic means, and methods of making payments; and
- Payment system operator license No. 2059051224 dated 5th day of December, 2026 for the provision of services for receiving, processing, and issuing financial information (processing, clearing) on

payments and settlements of third parties to participants of the payment system of this processing and clearing center.

1.8. For the purposes of these Rules, PrimeTech LLC is referred to as the Payment System Operator (Payment Organization).

1.9. The Internet address of the "PrimeTech" Payment Acceptance System: https://primetek.kg/

1.10. The call center number of the Payment System Operator (Payment Organization): +996 703 355 388 and for the agent network +996 703 355 388. Telephone number of the Payment System Operator (Payment Organization): +996 703 355 388

1.11. Trademarks, logos, and other symbols of the Payment System Operator (Payment Organization).

---

2. ARCHITECTURE AND OPERATING SCHEME OF THE PAYMENT SYSTEM

2.1. The technological base of the Company's payment system shall include:

2.1.1. Development of a scalable platform based on cloud technologies to ensure high availability and reliability of the service.

2.1.2. Use of modern encryption algorithms (e.g., AES and RSA) to protect transactions and user data.

2.2. Architecture and operating scheme of the system

The System has the capability of external integrations via API and can be integrated with the Customer's IT environment. The general architecture of the System is presented below. The System consists of three levels; the functions of each level of the System are described in detail below.

The System is built on the principle of a three-tier architecture to provide greater scalability:

- **Level 1.** Applications for interaction with payment and/or money transfer participants and payment system participants;

- **Level 2.** Applications providing the business logic of the payment acceptance system. A set of software and hardware means ensuring the execution of payments;
- **Level 3.** Database management system. Applications ensuring the processes of reading, writing, storing, and backing up data.

Applications at each level of the System can be deployed multiple times independently of other levels, thus ensuring the possibility of horizontal scaling of the System and the possibility of multiple use of applications. As a consequence, the System's applications have the following properties:

- Interchangeability;
- Extensibility;
- Multiple configuration options.

An information system consisting of such applications is easier to maintain and develop.

2.3. Encryption Algorithm

2.3.1. The Company's payment system implements a combined encryption process based on asymmetric RSA and symmetric AES encryption. Each transaction has its own unique random file key, which is created when the transaction is created.

2.3.2. Advanced Encryption Standard (AES) is one of the most commonly used and most secure encryption algorithms. The algorithm is based on several substitutions, permutations, and linear transformations, each of which is performed on data blocks of 16 bytes. The Company's payment system uses an AES-256 key length, which is the preferred encryption standard for governments, banks, and high-security systems worldwide.

2.3.3. Additionally, the Company's payment system uses RSA 1024 encryption, which is the most successful asymmetric encryption system to date. Unlike traditional symmetric encryption systems, RSA operates with two different keys: public and private. Both complement each other, meaning that a message encrypted with one of them can only be decrypted by its complementary counterpart. Since the private key cannot be computed from the public key, the latter is generally available to the public.

2.4. The System is a complex of hardware and software means, the main purpose of which is to unite goods/services providers (cellular operators, banks, utilities, etc.) with payers, to ensure information interaction between them, as well as to receive, process, and transmit financial and non-financial information between system participants.

The system participants are:

- **service providers** — merchants (MSPs) that connect to the system in real-time mode, as well as in offline mode. Service providers (MSPs) have access to the system via a web interface.

- **users** — individuals and legal entities/individual entrepreneurs using the system to obtain non-financial information and making payments for services of service providers.
- **payment agents** — payment organizations, banks, and other legal entities/individual entrepreneurs connecting to the system for accepting payments in favor of service providers through the system.

The operation of the system is based on electronic invoices created at the user's request in favor of agents. The request for issuing an electronic invoice can be made either in a fully automatic mode using the API, or in manual mode through a mobile application — an interface available to the user/goods/services provider.

Information about the receipt of payment/payment of an electronic invoice is delivered to the goods/services provider within a few seconds in real-time mode.

Connection of payment systems is carried out by connecting them to the electronic gateway of the system, which has the capability of interacting with various types of payment systems (payment agents) used worldwide, such as: internet acquiring of bank cards, cash payment acceptance systems (banking organizations, web cash registers for service payments, POS terminals, communication salons, money transfer systems), payment acceptance systems, and mobile payments.

One of the features of the system is a fully automated back office that allows monitoring the System's operation, connecting new goods/services providers and payment agents as quickly as possible, setting security configurations and changing them depending on the needs of a particular system participant, as well as conducting mutual settlements and reconciliations in real-time mode.

2.5. Procedure for the movement of funds through payment agents/sub-agents

To carry out activities for accepting and processing payments in favor of the System, a payment agent replenishes the balance (prepayment) by transferring funds to the Payment System Operator for crediting to its balance.

The Agent replenishes its balance by transferring funds to the Operator's bank account.

The Payment System Operator (Payment Organization) replenishes the Agent's balance using its operational account.

The Agent (sub-agent), within the available balance, processes payments in favor of the system.

The Agent has access to operations within the established limits.

2.6. Processing Procedure

1. The Payer makes a payment through the system. When making a payment, the Payer enters the details in the Client part of the "PrimeTech" system web cash register. Details refer to the name of the Provider in whose favor the Payment is made, the Personal Account, as well as the amount payable for the purpose of ensuring the fulfillment of the Subscriber's obligations to the Service Provider/Payment Recipient;

2. The Payer makes a payment through the Operator's Agent. The Payment Agent, using the "Agent" subsystem, transmits the User's instruction to the Payment System Operator (Payment Organization);

3. If the Payment Limit of the Agent through which the payment is made (web cash register, "Agent" subsystem) is greater than or equal to the amount of the payment being made, then the Payment Information (payment details) is transmitted to the Processing Center (hardware and software complex) of the Operator. The transmission of Payment Information is carried out according to the Operator's internal Protocol for data exchange between the web cash register/payment acceptance point and the Processing Center. In the case of a web cash register, periodic checking of the Agent's balance is performed by each of the Agent's web cash registers to determine whether the Agent's balance exceeds the critical limit. If the Agent's balance does not exceed the critical limit, acceptance of payments through the web cash register is blocked until the Agent's Payment Limit once again becomes greater than or equal to the critical limit;

4. The Operator's Processing Center transmits the Payment Information to the Provider's hardware and software complex. The Provider's hardware and software complex, based on the data received (payment details) from the Operator, processes the Payment. If the transmitted Information (payment details) is correct, the Provider fulfills the discharge of the Payer's obligations to the Provider in the amount received from the Operator for this Payment. Otherwise, the fulfillment of the Payer's obligations to the Provider does not occur. The transmission of Payment Information from the Operator to the provider occurs in accordance with the regulations for interaction between the Operator's and Provider's hardware and software complexes;

5. The Provider's Hardware and Software Complex notifies the Operator's Processing Center of the success or failure of the Payment processing. Notification occurs according to the regulations for interaction between the Operator's and Provider's hardware and software complexes agreed upon by the Parties;

6. The web cash register receives from the Operator's Processing Center a response on the result of the Payment processing according to the Operator's internal Protocol for data exchange between the web cash register and the Processing Center;

7. In the event of successful processing of the Payment by the Provider, the Provider, if such functionality is available in its hardware and software complex, sends a notification to the Payer about the fulfillment of the Payer's obligations to the Provider in the amount of the Payment.

3. PROCEDURE FOR CONNECTING A PARTICIPANT TO THE PAYMENT SYSTEM

3.1. System participants connect to the system by signing an agreement with the Payment System Operator on participation in the system/accession to the Rules, establishing a connection with the Operator's Hardware and Software Complex, and creating an account.

3.2. These Rules are an integral and constituent part of the Agreement concluded with a System Participant and are irrevocably recognized and accepted by Participants as mandatory for execution in full without any exclusions or exceptions.

3.3. When concluding agreements and forming a database of Agents, Sub-agents, and Goods/Services Providers, the Payment System Operator obtains the following mandatory information from the Participant:

- name of the legal entity / full name of the individual entrepreneur;
- data on state registration of the legal entity, passport data of the individual entrepreneur, patent, certificate of registration;
- location / residential address, address of business activity;
- information about managers;
- contact details;
- information about owners / founders (for legal entities);
- information about beneficial owners (for legal entities);
- information about the type of activity of the legal entity/individual entrepreneur (banking, utilities, etc.);
- current list of addresses where web cash registers are installed (this information must be updated monthly during the term of the agreement) of agents/sub-agents.

3.4. Procedure for concluding an agreement with Goods/Services Providers.

3.4.1. The Goods/Services Provider provides copies of the following documents to the Payment System Operator (Payment Organization):

- charter;
- memorandum of association (if available);
- decision on the creation (or re-registration) of the legal entity;
- decision on the appointment/election of the executive body of the legal entity;
- passport of the head of the legal entity;
- certificate of state registration;

- if the activity of the Goods/Services Provider is subject to licensing, a copy of the corresponding license;
- information about beneficial owners in accordance with the requirements of the legislation of the Kyrgyz Republic.

All copies of the above documents are certified by the signature of the head and stamped with the seal of the legal entity.

3.4.2. If the Provider is an individual entrepreneur, copies of the following documents are provided:

- passport of the individual entrepreneur;
- certificate of state registration of the individual entrepreneur and Notice to the Payer of social contributions to the Social Fund of the Kyrgyz Republic; or
- patent and insurance policy with the attachment of corresponding payment receipts;

3.4.3. In exceptional cases, other documents may be requested from the Goods/Services Provider for the conclusion of the Agreement.

3.5. When concluding the Agreement with the Goods/Services Provider, the Parties determine:

- the procedure and conditions for the fulfillment of monetary obligations of the Payment Organization to the Goods/Services Provider for Payments accepted by the Payment Organization and/or its Agents;
- the procedure and conditions for connecting the Goods/Services Provider to the System;
- the Technical Regulations for interaction between the hardware and software of the Operator and the Goods/Services Provider;
- the procedure for providing data (Payment registers) for conducting regular reconciliations of information on Payments accepted by the Operator and/or its Agents based on information contained in the Operator's hardware and software complex and data on payments accepted by the Operator contained in the Provider's hardware and software complex.

3.5.1. The Parties carry out the integration of the Operator's hardware and software with the hardware and software of the Goods/Services Provider in accordance with the Technical Regulations and Data Exchange Protocol adopted by the Parties.

3.5.2. Upon completion of integration, the Operator enters the necessary data into the System to enable the acceptance of payments for the Goods/Services Provider by the Operator and/or its Agents/Sub-agents.

3.5.3. The Agreement with the Goods/Services Provider may have other procedures and conditions for concluding the Agreement with the Goods/Services Provider.

3.6. The Operator sends notifications to Agents about the connection of a new Goods/Services Provider to the System, providing information (including information about the conditions of financial relations between the Operator and the Agent for the given Goods/Services Provider) objectively necessary for the Agent to accept Payments in favor of the Goods/Services Provider.

3.7. Procedure for concluding an Agreement with an Agent and other participants of the Payment System:

3.7.1. Before commencing activities related to making Payments, a Payment System Participant is required to register with the Payment System by signing/acceding to the Payment System Agreement, in the form established by the Operator. Providing the Operator with a signed Agreement/consent to accede to the Rules in the appropriate form constitutes confirmation that the Payment System Participant agrees to the Rules and undertakes to comply with the terms of the Rules and the Agreement. After submitting a signed Payment System Participant Agreement/consent to accede to the Agreement to the Operator, the Payment System Participant may not claim that they have not familiarized themselves with the Rules or do not recognize their binding nature in contractual relations with the Operator.

3.7.2. The Agent provides the Operator with copies of documents certified by the head and stamped with the organization's seal, if the Agent is a legal entity:

- charter of the legal entity;
- decision (or minutes) on the creation of the legal entity;
- certificate of state registration of the legal entity with the Ministry of Justice;
- certificate of registration of the legal entity with the tax authority (with parameters);
- document (decision, minutes) on the election of the head of the organization (General Director, Director);

If a legal entity acts through a representative, a power of attorney is provided to the authorized representative of the Payment Agent for signing the agreement and/or other documents (indicating passport data, date of issue and validity period of the power of attorney, with the attachment of the passport of the authorized person);

- information (copies of passports and other data in accordance with the legislation) about beneficial owners (if any);
- current list of addresses where web cash registers are installed, if applicable.

3.7.3. List of documents for an individual entrepreneur:

- certificate of state registration and notice to the payer of insurance contributions;
- passport of the individual entrepreneur;
- patent and insurance policy with the attachment of payment receipts;
- current list of addresses where web cash registers are installed, if applicable.

3.8. After registration, a personal account is created for the Participant in the System, which is assigned an individual ID number.

3.9. The Operator has the right to refuse registration to any Participant, as well as to decline to sign the Payment System Participant Agreement if the person does not meet the requirements of the legislation and these Rules.

---

4. RIGHTS AND OBLIGATIONS OF PARTICIPANTS

4.1. Rights of the Payment System Operator (Payment Organization):

4.1.1. The Payment System Operator (Payment Organization), on behalf of and at the expense of the Goods/Services Provider, has the right to accept Payments from Payers through its agent network and undertakes to transfer the accepted payment to the Goods/Services Provider (or otherwise lawfully settle with the Goods/Services Provider) in the manner prescribed by these Rules and the Agreement with the Goods/Services Provider; in turn, the Goods/Services Provider undertakes to pay the Payment Organization a fee in the manner prescribed by these Rules and the Agreement with the Goods/Services Provider, if such payment is provided for by the Agreement with the Goods/Services Provider. The amount of the fee is determined by the Agreement with the Goods/Services Provider.

4.1.2. The Payment Organization has the right to accept payments personally or to entrust the acceptance of payments to third parties — Agents, while remaining fully responsible to the Goods/Services Provider.

4.1.3. The Payment Organization and/or Agents have the right to accept (receive) Payments from Payers by any means not prohibited by law (cash; non-cash funds); as well as through other payment systems and instruments not prohibited by the legislation of the Kyrgyz Republic.

4.2. The Payment System Operator (Payment Organization) must:

- have procedures to ensure the security and continuity of functioning of personnel workstations;
- have procedures for reserving data transmission communication channels;
- have procedures to ensure the confidentiality of data transmitted and received from the payment system in accordance with the legislation of the Kyrgyz Republic;
- ensure that the capacity of lines and other terminal equipment through which power supply is provided for the operation of systems meets the power requirements of the systems;
- in cases of power supply interruptions, ensure autonomous power supply for the systems;

- have procedures regulating the time of autonomous operation of the system, as well as ensuring compliance with requirements for the duration of autonomous operation of the system from the moment of power supply cessation until the subsequent switchover to the backup hardware and software complex of the system;
- in the event of hardware or software failures, ensure the use of alternative and/or backup means in accordance with its internal procedures;
- in the event of a failure of the main communication channel, perform switchover to the backup communication channel in accordance with its internal procedures;
- to reduce the risk of internal fraud, have a fraud and unauthorized access protection system at the hardware and software complex level (use of passwords and access rights to the system, cryptography, encryption, etc.), qualified personnel to work in the system, as well as approved job descriptions defining the responsibilities, rights, and obligations of personnel.

4.2.1. In the event of internal fraud affecting the terms of the concluded Agreement, the Payment System Operator, together with the participants, conducts an internal investigation into the fraud and notifies each other in writing of the results of such investigation. Claims of the parties arising as a result of internal fraud are resolved within the framework established by the legislation of the Kyrgyz Republic.

4.2.2. In order to insure possible risks of Goods/Services Providers, the Payment Organization ensures:

- placement of an insurance deposit in the amount of 50 (fifty) percent of the average daily turnover for the last quarter for each goods/services provider for goods/services providers fully or partially in state ownership, communal enterprises, and budgetary organizations where contractual relations do not provide for prepayment, an irrevocable bank guarantee, or a deposit placed in the goods/services provider's bank account;
- the Agreement with the Goods/Services Provider provides that the insurance deposit shall be used only for its intended purpose in the event of the Operator's failure/breach of obligations to transfer accepted payments to the settlement account of the Goods/Services Provider, as well as the conditions for monitoring the bank account in which the insurance deposit is placed and/or the possibility of direct debit of funds by the Goods/Services Provider;
- placement in a bank account for deposits on other terms of return in a commercial bank of an insurance deposit or provision by the Operator of an irrevocable bank guarantee in favor of the Goods/Services Provider for goods/services providers where contractual relations do not provide for prepayment to the Goods/Services Provider. The amount of the insurance deposit or bank guarantee must be not less than 10 (ten) percent of the Operator's average daily turnover for the last quarter for each Goods/Services Provider.

4.3. The Payment System Operator (Payment Organization) undertakes:

4.3.1. to prepare software that enables, in accordance with the requirements of the Technical Regulations, the interaction of the Operator's hardware and software with the Provider's hardware and software for the purpose of ensuring the transmission of Payment Information;

4.3.2. to register the Provider in its electronic database and assign it a payment recipient code;

4.3.3. to ensure the transfer of Payments accepted independently and/or by Agents in the course of performance of the Agreement with the Provider, based on the data of the Register of Payments accepted by the Operator and/or the Operator's Agents, in regular unified consolidated payments. At the same time, the obligations of the Payment Organization to transfer payments accepted in favor of the Goods/Services Provider shall be deemed fulfilled from the moment the corresponding amount of funds is debited from the bank account of the Payment Organization. The period within which the Payment Organization is obliged to make the transfer of accepted payments, as well as the transfer procedure, is determined by the Agreement with the Provider;

4.3.4. The Payment System Operator and the Provider sign a Reconciliation Statement for the reporting period. The procedure and timing for providing the Statement, reviewing the Statement, and signing it are determined by the Agreement with the Provider.

4.4. Rights and Obligations of the Goods/Services Provider. The Goods/Services Provider is obliged to:

4.4.1. prepare the necessary equipment and software enabling interaction with the Operator's hardware and software in accordance with the requirements of the Technical Regulations;

4.4.2. for the purposes of registering the Goods/Services Provider in the Operator's electronic database and carrying out payments correctly, as well as for the purposes of interaction between the parties in the performance of the Agreement with the Goods/Services Provider, communicate to the Operator the information and provide the documents stipulated in Section 4 of these Rules;

4.4.3. notify the Operator of changes in Payment parameters that may affect the identification of the Payer and the overall correctness of the Payment processing, in the manner and within the timeframes determined by the Agreement with the Goods/Services Provider;

4.4.4. monitor and account for the Operator's funds deposited by it (the Operator) as prepayment to the Goods/Services Provider on account of future Payments made by the Operator;

4.4.5. in the event of an erroneous transfer of funds by the Operator in favor of the Goods/Services Provider, transferred by the Operator in the course of fulfilling the Operator's obligations to the Goods/Services Provider, which (payments) arose as a result of any technical error, return the erroneously transferred funds to the Operator upon its written request within three (3) banking days from the receipt of the corresponding demand. Individual Agreements with Goods/Services Providers may contain other conditions for the return of funds erroneously transferred by the Operator in favor of the Goods/Services Provider;

4.4.6. in the event of an erroneous payment due to the fault (including negligence) of the Payer (incorrect indication of the personal account number, incorrect indication of the payment amount, incorrect indication of the phone number, etc.), upon the Operator's written request, return the erroneously transferred funds to the

Operator, or change the payment parameters, if such a return and such a change of payment parameters are possible and feasible;

4.4.7. reconcile and sign the monthly Reconciliation Statement for the corresponding reporting month. The procedure and timing for receiving the monthly Statement are determined by the Agreement with the Goods/Services Provider;

4.4.8. pay the Operator a fee in the manner and amount established in the Agreement with the Goods/Services Provider, if such a fee is provided for in the Agreement with the Goods/Services Provider;

4.5. The Goods/Services Provider must:

4.5.1. have on staff specialists performing the functions of accepting payments (transfers), as well as the functions of exchanging other messages within the payment system.

4.5.2. have on staff system maintenance specialists ensuring the uninterrupted functioning and security of the technical infrastructure.

4.5.3. have procedures to ensure the confidentiality of data transmitted to and received from the payment system in accordance with the legislation of the Kyrgyz Republic;

4.5.4. in the event of a failure of the main communication channel with the Operator, perform switchover to its own backup communication channel in accordance with its internal procedures;

4.5.5. to reduce the risk of internal fraud, have qualified and vetted personnel to work in the system, as well as approved job descriptions defining the responsibilities, rights, and obligations of personnel;

4.5.6. in the event of internal fraud affecting the terms of the concluded Agreement, the Parties conduct an internal investigation into the fraud and notify each other in writing of the results of such investigation. Claims of the parties and all dispute situations arising as a result of internal fraud are resolved within the framework established by the legislation of the Kyrgyz Republic.

4.6. Rights of the Goods/Services Provider:

4.6.1. demand from the Operator the timely fulfillment of financial obligations incurred by the Operator for the acceptance by the Operator and/or its Agents of Payments of the Goods/Services Provider;

4.6.2. demand from the Operator the proper performance of obligations stipulated by these Rules and the Agreement with the Goods/Services Provider;

4.6.3. in the event that the Operator fulfills its obligations to the Goods/Services Provider on a prepayment basis, the Goods/Services Provider has the right, upon a properly executed request from the Operator, to provide a credit limit for payments made by the Operator, except for payments to the budgets of the budget system of the Kyrgyz Republic. In this case, the Parties determine the amount of the credit limit, as well as the procedure and terms for its repayment, unless otherwise specified in the Agreement with the Goods/Services Provider. The risk of non-payment of the Operator's obligations to the Goods/Services Provider arising in this case is borne by the Goods/Services Provider.

4.7. Rights of the Payment System Operator (Payment Organization):

4.7.1. demand from the Goods/Services Provider the proper performance of obligations stipulated by these Rules and the Agreement with the Goods/Services Provider;

4.7.2. demand from the Goods/Services Provider the payment of the due fee in the manner and within the timeframes determined by the Agreement with the Goods/Services Provider for Payments accepted by the Operator and/or the Operator's Agents, if such payment is provided for in the Agreement with the Goods/Services Provider;

4.7.3. in the event of erroneous payments, the correction and cancellation (reversal) of payments shall be carried out in accordance with the procedures (procedure) described in the Agreement with the Goods/Services Provider;

4.7.4. The Payment Organization and/or Agents/Sub-agents have the right to charge Payers a fee for the use of Operator's hardware and software complex (HSC) resources when accepting and processing Payments, the amount of which (fee) is determined by the Agreement with the Goods/Services Provider;

4.8. The Payment System Operator (Payment Organization) and the Goods/Services Provider have the right to place each other's trademarks using their own information resources solely for the purpose of advertising the goods (works, services) of the trademark owners.

4.9. Liability of the Parties in the Interaction between the Payment System Operator (Payment Organization) and the Goods/Services Provider.

4.9.1. The Parties are liable for improper performance of their obligations in accordance with the provisions of these Rules, as well as the Agreement with the Goods/Services Provider, and in cases not provided for by the Rules and the Agreement — in accordance with the legislation of the Kyrgyz Republic.

4.9.2. In the event of the Operator's breach of obligations to transfer Payments accepted in the course of performance of the Agreement with the Goods/Services Provider to the Goods/Services Provider, the Operator undertakes to pay the Goods/Services Provider a penalty in the amount, procedure, and timeframes determined in the Agreement with the Goods/Services Provider.

4.9.3. In the event of the Goods/Services Provider's breach of the procedure for payment of the fee provided for in the Agreement with the Goods/Services Provider and/or in its corresponding appendices (amount, terms), the Goods/Services Provider undertakes to pay the Operator a penalty in the amount, procedure, and timeframes determined in the Agreement with the Goods/Services Provider.

4.9.4. In the event of a temporary suspension or termination of the acceptance of Payments by the Operator, including in connection with the termination of the Agreement with the Goods/Services Provider, the Goods/Services Provider is not entitled to demand, and the Operator is not obliged to compensate the Goods/Services Provider for any indirect damages (lost profits, lost income (profit), etc.), unless otherwise provided by the Agreement with the Goods/Services Provider;

4.9.5. The Operator shall not be liable for the untimely transfer of accepted Payments to the Goods/Services Provider in the event of untimely notification by the Goods/Services Provider of changes in its details, as well as in the event of a failure in the operation of electronic systems of the servicing bank.

4.9.6. The Operator shall not be liable for errors made by the Payer when making a Payment.

4.9.7. In the event of losses caused to any Party or any third party due to a violation of the requirements of the Technical Regulations, such losses shall be fully compensated to the injured Party and/or the corresponding third party by the Party that violated the requirements of the Technical Regulations.

4.10. Rights and Obligations of the Agent and other System Participants. The Agent/Participant is obliged to:

- pay for the Processing services of the Payment System Operator (Payment Organization) in respect of Goods/Services Providers specified in the Agent's/Participant's Personal Account;
- any operation for the transfer of Payment data is only possible using the "PrimeTech" System;
- the Participant/Agent is obliged to transmit to the Payment System Operator (Payment Organization) in real-time mode data on each accepted Payment;
- a payment agent is obliged, after accepting a Payment, to provide the Payer with a notice confirming the Payment, in the form established by applicable law and the Payment System Operator;
- pay a Guarantee Deposit to the Operator's settlement account before commencing the acceptance of Payments;
- the Agent/Participant is obliged to notify the Payment System Operator (Payment Organization) of any changes to any data provided by the Agent/Participant during registration with the Payment System, including legal and actual address, postal address, email address, contact phone numbers, changes in authorized representatives of the Agent/Participant, changes in bank details, transition of

the Agent/Participant to a different tax regime, etc. The notification must be sent by the Agent/Participant by email to the supervising manager within 3 (three) days from the date of change of the relevant data, and also attached in writing to the Work Completion Certificate for the month in which the corresponding changes occurred;

- not to compromise or infringe on the Operator's Trademark rights;
- timely inform the Operator of the occurrence, existence, or change of any circumstances that are relevant to the performance of these Rules;
- in the event of termination (suspension) of the Agent's/Participant's authority to use the "PrimeTech" System, the Agent/Participant is obliged to immediately cease accepting Payments and using the "PrimeTech" System, as well as remove all advertising materials;
- the Agent/Participant is obliged to carry out subsequent settlements with the Operator in accordance with the concluded agreement, these Rules, and applicable law;
- provide any information requested by the Operator regarding agency activities, including a current list of addresses where web cash registers are installed (if any);
- ensure unimpeded access for the National Bank for the purpose of inspecting the Operator's agents and sub-agents for compliance with the requirements of regulatory legal acts of the National Bank and providing the necessary documents related to the inspection of activities carried out as an agent, provided that representatives of the National Bank have a document confirming the right to conduct such inspection;
- if there is a suspicion of financing of terrorist activities and legalization (laundering) of criminal proceeds and other predicate offenses as a result of making a payment/payments, carry out identification and verification of the payer and report to the Operator.

4.11. The Agent/Participant has the right to:

- use the Operator's Trademarks for advertising purposes with the written consent of the Operator. Trademarks are not transferred for use to the Agent/Participant;
- charge the Payer an Additional fee, subject to the restrictions established by the Operator.

4.12. Rights and Obligations of the Operator in Interaction with the Agent/Participant. The Operator is obliged to:

- after completion of registration, the Operator undertakes to provide the Agent with a login and password for the Agent's/Participant's Personal Account;
- pay the Agent/Participant a fee, unless otherwise provided by the Agreement with the Agent;
- timely inform the Agent/Participant of the occurrence, existence, or change of any circumstances that are relevant to the performance of the Rules;

4.13. The Operator undertakes to:

- when concluding the Payment System Participant Agreement, determine the fee rates of the Agent/Participant for accepting Payments in favor of the relevant Goods/Services Providers; develop internal regulatory documents to ensure the uninterrupted functioning of its information system and the security of payment processing. Software and technical means used in settlement systems must comply with the requirements of the National Bank of the Kyrgyz Republic for ensuring information security;
- implement organizational, procedural measures and the use of technical means for the purpose of detecting, as well as preventing, hindering, and combating fraud;
- implement an information protection system that must provide continuous protection of information during payment acceptance and at all stages of its generation, processing, transmission, and storage in the System;
- ensure internal control for the purpose of counteracting the legalization (laundering) of criminal proceeds and the financing of terrorist and extremist activities;
- ensure the recording of all transactions between System participants;
- store, for five years, relevant information about transactions in the System in a form that allows verification of its integrity.

4.14. The Operator, in interaction with the Agent/Participant, has the right to:

- in the absence of funds in the Guarantee Fund balance, suspend the technical ability to accept Payments;
- refuse to provide services under these Rules in cases provided for by the legislation of the Kyrgyz Republic and these Rules;
- verify at any time the progress of the Agent's/Participant's fulfillment of obligations related to these Rules, without interfering in its economic activities;
- the Operator has the right to unilaterally amend the Rules by publishing a document containing information about such amendments on the System's website. Amendments shall come into force upon the expiration of 5 (five) business days from the date of publication, unless a different effective date for the amendments is additionally specified upon their publication. The Agent/Participant undertakes either to accept the amendment to the terms of the Rules, or to provide the Operator with a response declining the amendment to the terms of the Rules before the amendment comes into force. In the event that no response declining the proposal is submitted, the proposal to amend the terms of the Rules shall be deemed accepted by the Agent/Participant. In the event of the Agent's/Participant's disagreement with amendments to the terms of the Rules, the parties have the right to terminate the Payment System Participant Agreement, having first completed all settlements;
- in the event of non-fulfillment (improper fulfillment) by the Agent/Participant of any of the obligations stipulated by these Rules, the Operator has the right, without prior notice, to disconnect/block the Agent/Participant in the "PrimeTech" System and demand in writing the immediate elimination of violations, as well as compensation for damages;
- demand from the Agent/Participant that the Guarantee Fund balance be maintained not lower than the projected amount of payments daily accepted by the Agent/Participant, and reserves the right, in the absence of funds in the Guarantee Fund balance, to suspend the technical ability to accept Payments;

- in the event that the requirements to eliminate the violation are not fulfilled by the Agent/Participant within 3 (three) business days, the Operator has the right to unilaterally terminate the Payment System Participant Agreement;
- notification of termination of the Payment System Participant Agreement on the above grounds is sent by the Operator to the Agent/Participant in writing. The authority of the Agent/Participant to use the "PrimeTech" System shall cease from the moment of notification by the Operator to the Agent/Participant, and the Payment System Participant Agreement is deemed terminated from the moment of notification of the Agent/Participant.

4.14.1. The Operator, in cases of concluding an agreement with a new Goods/Services Provider, or changing the terms of work with a Goods/Services Provider, or for other reasons specified in these Rules, reserves the right to unilaterally change both the list of Goods/Services Providers in whose favor Payments may be accepted and the fee rates of the Agent/Participant for accepting Payments of a specific Goods/Services Provider, by publishing in the Agent's/Participant's Personal Account a news item about the implementation of the changes listed in this clause. Changes made to the list of Goods/Services Providers and Tariff Plans shall come into force for the Agent/Participant after the expiration of one day from the date of posting the news item about the changes in the Agent's/Participant's Personal Account, unless a different effective date is specified by the Operator. New conditions are deemed accepted by the Agent/Participant upon acceptance of Payments by them after the effective date of the changes.

4.15. Liability of the Parties in the Interaction between the Operator and the Agent/Participant.

4.15.1. The Parties are liable for improper performance of their obligations in accordance with the provisions of these Rules, as well as the Agreement with the Agent/Participant, and in cases not provided for by the Rules and the Agreement — in accordance with the legislation of the Kyrgyz Republic.

4.15.2. In the event of a violation of the terms of the Rules by one of the Parties, as a result of which the other Party suffered damages, the guilty Party shall compensate them in full.

4.15.3. The Agent/Participant independently and at its own expense resolves disputed situations with Payers related to the non-processing of a Payment in the "PrimeTech" System due to the lack of necessary software or hardware, as well as other reasons caused by the culpable actions/omissions of the Agent.

4.15.4. The Agent/Participant who, in violation of applicable law, has not fulfilled the obligations specified in these Rules, shall bear the measures of liability established by the relevant regulatory legal acts, and also undertakes to compensate damages incurred by the Operator as a result of actions of regulatory authorities caused by the Agent's/Participant's failure to fulfill said obligations.

4.15.5. The Operator shall not be liable for direct or indirect losses of the Agent/Participant, including lost profits, incurred by the parties due to the fault of the communications operator, including a temporary decrease in communication quality and/or failure of network equipment.

4.15.6. The Operator shall not be liable in the event of unauthorized access to the Agent's/Participant's Personal Account in the "PrimeTech" System by third parties.

4.15.7. The Parties are liable for the actions of their personnel related to violation of the provisions of these Rules and/or Appendices thereto, if they resulted in non-fulfillment or improper fulfillment of the Parties' obligations.

4.15.8. The recovery of any penalties and sanctions, as well as the submission of a claim for damages, is a right and not an obligation, and is exercised by the Parties at their own discretion.

4.15.9. The right of a Party to recover damages, penalties, and sanctions is exercised by sending a written claim to the guilty party. The Operator has the right to offset the debt for all monetary obligations of the Agent/Participant against the fee payable to the Agent/Participant or deduct the amount of the debt from the amounts of the Agent's/Participant's Guarantee Fund, as well as apply a claim procedure for the recovery of said debt.

4.15.10. The payment of penalties and compensation for damages does not release the Parties from the proper fulfillment of accepted obligations and compliance with these Rules.

---

5. PROCEDURE FOR CLAIMS HANDLING

Procedure for Processing Client Requests

5.1. All disagreements arising in the process of executing the Agreement with Participants shall be resolved by the Parties through negotiations.

5.2. Any unresolved disputes arising from these Rules or from the Agreement with a Participant, including those relating to its violation, termination, cancellation, or invalidity, shall be resolved in the court of the Kyrgyz Republic in accordance with the applicable substantive law of the Kyrgyz Republic at the location of the Payment System Operator.

5.3. The procedure for processing requests and complaints of Participants is carried out in a general manner:

5.3.1. Processing of all requests received by phone call to the Call center;

5.3.2. Processing of all requests received by email and in person.

5.4. When receiving requests and complaints, mandatory conditions are the registration of the reason for the request, details of the claim of the Payment System Participant. An analysis based on staff interviews, study of system logs, and determination of conditions for preventing such situations in the future is organized for each request.

5.5. All decisions on requests from Payment System Participants must be communicated by the Payment System Operator to the addressee with a full explanation of the examined circumstances.

Procedure for Cancellation and Correction of Erroneous Transactions

5.6. Correction or cancellation of a corresponding payment is permitted only if, among others, all of the following conditions are met:

5.6.1. the discrepancy between the erroneous details of the corresponding payment and its correct details does not exceed two (2) characters (digits);

5.6.2. the deadlines and form of application submission according to the requirements of the Service Provider have been observed;

5.6.3. the maximum timeframes within which it is objectively possible to change the details of the corresponding payment or cancel the payment have not expired;

5.6.4. there are no prohibitions (restrictions) regarding the change of payment details or cancellation of the payment, established by the relevant Providers for payments for certain services (goods, works), as well as by other Recipients;

5.6.5. the amount of the payment made, or part thereof, has not been used by the person in whose details the payment was made, regarding the change of whose details or cancellation of which a cancellation request has been received;

5.6.6. the data specified in the application correspond to the reporting data of the Operator's Payment Acceptance and Processing System.

5.7. If, when reviewing the Application, the Operator determines that the correction or cancellation of the corresponding payment is objectively within the competence of the Provider, such Application is forwarded by the Operator to the Provider.

5.8. If there are grounds for changing the payment details or canceling the payment, the Operator, independently or in agreement with the relevant Provider or other person in whose favor the payment was

made, changes the payment details and credits the payment using the new (correct) details or cancels the payment, if correction of the payment is inadmissible and its cancellation is objectively possible (permissible) in accordance with the requirements of the relevant Provider, as well as the requirements of the Agreement, including all its appendices.

5.9. In the event of cancellation of the corresponding payment, its amount is subject to return by the Operator to the Payer at the expense of the Provider, but only if such return is objectively possible (permissible) and meets the requirements of the relevant Recipients and the Operator, as well as the requirements (provisions) of the Agreement, including all its appendices.

5.10. The deadlines for submitting an Application to change payment details or cancel a payment, as well as the maximum timeframes within which it is objectively possible to change payment details or cancel the payment, depend on each provider individually.

---

6. PROCEDURE FOR PARTICIPANTS' WITHDRAWAL FROM THE PAYMENT SYSTEM

6.1. Procedure for withdrawal of a Goods/Services Provider from the payment system.

6.1.1. The Agreement with the Goods/Services Provider comes into force from the date of its signing by the Parties and is valid until its termination by agreement of the Parties or for the period specified in the Agreement with the Goods/Services Provider.

6.1.2. The Agreement with the Goods/Services Provider may be terminated unilaterally, based on an application (initiative) of the Operator, in the following cases:

- violation by the Goods/Services Provider of the terms of the concluded agreement and/or these Rules;
- adoption by the relevant authorized state body of a regulatory legal act prohibiting or restricting the business activity of Providers; in the event that force majeure circumstances last more than sixty (60) calendar days, unless otherwise provided by the Agreement with the Goods/Services Provider;
- in the event that force majeure circumstances last more than 60 (sixty) calendar days.

6.1.3. The Agreement with the Goods/Services Provider may be terminated unilaterally, based on an application (initiative) of the Goods/Services Provider, in the following cases:

- violation by the Operator of the terms of the concluded agreement and/or these Rules;
- in the event that force majeure circumstances last more than sixty (60) calendar days, unless otherwise provided by the Agreement with the Goods/Services Provider.

6.1.4. In the event of termination of the Agreement with the Goods/Services Provider, the monetary obligations of the Parties, as well as obligations determining liability for violation of these Rules or the Agreement with the Goods/Services Provider, remain in effect until their fulfillment.

6.2. Procedure for withdrawal of an Agent/Participant from the payment system.

6.2.1. The Agreement with the Agent/Participant comes into force from the date of its signing by the Parties and is valid until its termination by agreement of the Parties or for the period specified in the Agreement, provided that the term of the Agreement with the Agent/Participant does not exceed the validity period of these Rules.

6.2.2. The Agreement with the Agent/Participant may be terminated unilaterally, based on an application (initiative) of the Parties, in cases of violation by the Agent/Participant of the terms of the agreement, as well as in the event that force majeure circumstances last more than sixty (60) calendar days, unless otherwise provided by the Agreement with the Agent/Participant.

6.2.3. In the event of unilateral termination of the Agreement with the Operator, the initiating Party is obliged to notify the other Party in writing no later than thirty (30) calendar days before the intended date of termination of the Agreement with the Operator, unless otherwise provided by the Agreement with the Operator.

6.2.4. In the event of termination of the Agreement with the Agent/Participant, the monetary obligations of the Parties, as well as obligations determining liability for violation of these Rules or the Agreement, remain in effect until their fulfillment.

---

7. ENSURING PHYSICAL AND INFORMATION SECURITY

7.1. The Operator, for the purpose of ensuring physical and information security of the Payment System, takes available measures to ensure compliance with the following requirements:

- restricts access to the processing center and communication channels used for transmitting payment information;
- implements data protection mechanisms both during storage and during transmission;

- ensures adequate backup of all data (real-time backup of all information or key information);
- ensures protection of the system from malicious software, regular updating of antivirus software;
- ensures the integrity and authenticity of data during their transmission via communication channels from the point of its initiation to the processing center and back;
- maintains the operability of information systems related to information security;
- ensures timely switchover/restoration/deployment of the system's functioning on the backup hardware and software complex in the event of an emergency situation;
- implements mechanisms for verifying the identity and authority of persons performing, processing, and receiving payments;
- implements mechanisms for minimizing data entry errors, data entry control that eliminates or reduces the possibility of error;
- conducts thorough testing of all system equipment and software;
- ensures protection of data and equipment in the event of automated system failures, emergency situations, or in the case of unauthorized access to data;
- monitors and controls the operability of objects connected to the processing center, sessions of access to the system's information resources;
- ensures backup of equipment and communication systems;
- ensures confidentiality of payment system information;
- ensures physical security of premises and equipment in accordance with the requirements of the legislation of the Kyrgyz Republic.

---

8. MEASURES FOR PROTECTION AGAINST FRAUD AND UNAUTHORIZED ACCESS

8.1. The Operator takes available measures for the purpose of protection against fraud and unauthorized access to the Payment System to ensure compliance with the following requirements:

- restricts access to the payment processing center and communication channels used for transmitting payment information;
- ensures encryption of data transmission channels;
- implements mechanisms for verifying the identity and authority of persons conducting, processing, and receiving payments;
- ensures segregation of duties when performing actions to change information system data and their confirmation (authorization), if necessary, by no less than 2 (two) employees;
- ensures authorization and authentication of system participants and personnel;

- assigns to each user the appropriate access rights necessary for them to perform their assigned job duties and ensure interchangeability;
- ensures control over violations of the information security regime;
- ensures physical protection of information systems;
- ensures cryptographic protection of data;
- ensures fire safety measures;
- ensures logging and checking of the technical condition of systems;
- ensures protection of supporting infrastructure and conducts personnel training;
- ensures protection against data interception, protection of mobile systems;
- uses antivirus protection at all workstations and system servers, unless otherwise provided by the technological process.

9. CRITERIA FOR UNINTERRUPTED FUNCTIONING OF THE PAYMENT SYSTEM

9.1. The Payment System Operator ensures and complies with the following criteria for uninterrupted functioning of the system (UFS):

- Level of operational continuity;
- Level of continuity of payment processing services;
- Level of continuity of settlements between payment system participants.

9.2. Factors affecting UFS:

- Financial condition of the Payment System Participants;
- Possible liquidity management methods and means of ensuring fulfillment of obligations of Payment System Participants provided for in the System (combined with requirements for the financial condition of Payment System Participants);
- Dependence on external Service Providers;
- Reliability of the technical system;
- Technological support of System Service Providers, Participants/Agents;
- Possibility of identifying unresolved legal issues concerning the relationships of Payment System Participants;
- Possibility of a conflict of interest among Payment System Participants when carrying out activities aimed at achieving their own goals and goals established within the System (including ensuring UFS);
- Market and infrastructure factors;
- Other external and internal factors, in accordance with the specifics of the System's functioning.

9.3. The UFS assurance strategy is based on the control of the following business processes:

- Assessment of possible risks inherent in the Operator's activities to ensure the continuity of the System's operations;
- Monitoring compliance with the requirements of these Rules, contractual obligations, monitoring compliance with the UFS assurance procedure by Participants;
- Verification of Participants for compliance with the conditions for making Payments and the requirements of these Rules;
- Control over the use of the Operator's name and trademarks exclusively within the framework of concluded contracts, agreements, and these Rules;
- Work to notify Participants of any deviations in ensuring the System's functioning;
- Assessment and monitoring of the financial stability of Participants, factors posing risks of loss of financial stability of Participants, including potential ones capable of leading to loss of the System's financial stability in the future;
- Investigation of events that caused operational failures, analysis of their causes and consequences;
- Analysis and evaluation of activities in accordance with the requirements of the legislation of the Kyrgyz Republic, recommendations of the NBKR;
- Ensuring the reliability, completeness, and timeliness of financial information and reporting used for decision-making, preparation of financial and regulatory reports;
- Availability of a stable telecommunication channel between the Operator and Participants within the requirements of technological interaction;
- Availability of uninterruptible power supply at key System nodes;
- Support for the uninterrupted functioning of the web cash register network management software complex;
- Support for the uninterrupted functioning of the SMS gateway;
- Support for the uninterrupted functioning of the web application;
- Support for the uninterrupted functioning of the mail service;
- Support for the uninterrupted functioning of the System servers;
- Handling of payment system incidents;
- Ensuring information protection from malicious code;
- Ensuring internal control for counteracting the financing of terrorism (extremism) and legalization (laundering) of criminally obtained proceeds;
- Ensuring information protection when conducting payment transactions and interacting with Participants;
- Identification of emergency, extraordinary, non-standard situations and determination of the procedure for interaction of Participants.

10. INCIDENT MANAGEMENT

10.1. When managing incidents, the following measures for identifying possible risks and difficulties must be taken into account by Payment System Participants, and must be mandatorily implemented by the Operator:

- The need for early detection of incidents — organization of event monitoring, as well as training users to report incidents;
- The need for incident registration;
- The need to ensure high system availability;
- Lack of resources when resolving incidents, overload with incidents, and postponement for later — when the number of incidents unexpectedly increases, there may not be enough time for proper registration.

10.2. The work in the incident management process is built according to a three-level scheme:

1) First Level — Single Point of Entry for Requests.

Registration and classification of tickets, determination of their priority and those responsible for execution, in charge of resolving standard Incidents. This support level is mainly handled by the call center, which is equipped with the necessary documents and instructions, including the process of interaction with the second level.

2) Second Level

Support engineers — conduct technical expertise and resolve non-standard incidents, are responsible for updating the application knowledge base, identify defects, and pass them to the third support level. Problem resolution is passed to the third level if the cause is related to the system architecture or its software implementation.

3) Third Level

System technical support specialists analyze complex incidents not resolved at the second level, fix defects, and test provided solutions.

---

11. PROCEDURE FOR INFORMING PARTICIPANTS

11.1. Information about disruptions and malfunctions in the operation of the Operator's Payment System and risks arising in connection therewith is communicated to System Participants if the Incident that has occurred affects the uninterrupted functioning of the payment system.

11.2. Confirmation (or denial) by the Payment System Participant (within whose area of responsibility the stated disruptions and malfunctions fall) of the violation (specifying the date, time of occurrence, time of resolution, nature of the disruptions and malfunctions, causes of their occurrence and measures taken to eliminate them, results of the investigation of said events, analysis of consequences) is made by contacting the Party via telephone communication channels or by email from designated addresses to a designated address. The Operator also uses any additional available means of communication, including informing the general public, to ensure the maximum level of awareness of all participants about the emergency situation and to take effective measures to resolve it.

11.3. The procedure for informing the NBKR, as well as the Payment System Participants, after the elimination of the emergency situation and restoration of normal system functioning is carried out within no more than 2 hours, and in the manner provided for by the parties' agreements.

11.4. In the event of an Incident that may negatively affect the continuity of the Payment System, the Payment System Participant who discovered the incident:

- notifies the party or parties at risk;
- takes measures to fulfill/complete its financial obligations to the payment system participants;
- takes measures to ensure data preservation and restoration of the payment system's operability;
- enables other Participants to fulfill their obligations.

11.5. The Operator informs the NBKR of an incident if the payment system inoperability lasts more than 2 hours.

11.6. Information about disruptions and malfunctions in the Payment System's operation and risks arising in connection therewith is communicated to the Payment System Participants if the risk levels resulting from the violation fall into the "Medium" or "High" category and affect the uninterrupted functioning of the Participants' systems.

11.7. In the event of an occurrence that is determined to be "Medium" or "High" risk level, provided that the identified operational disruptions affect the uninterrupted functioning of the Payment System as a whole, the Operator immediately notifies the Payment Systems Department of the NBKR via telephone communication channels, by email, and any other means of communication for delivering messages to the addressee.

11.8. Upon detection of facts of external threats, crimes, fraud in the Payment System that may threaten other Participants, immediate notification is made to the Payment Systems Department of the NBKR via telephone communication channels, by email, and any other means of communication for delivering messages to the addressee.

Procedure for Notification (Informing) of Payment System Participants

In the event of the most common emergency situations or the occurrence of other incidents/situations requiring notification (informing) of payment system participants, PrimeTech LLC performs the following actions:

1) **Software failure** — The responsible person, together with technical services, determines the cause of the software failure. If the error cannot be fixed independently, developers are engaged.

2) **Local Area Network (LAN) failure** — The person responsible for information security organizes an analysis for the presence of loss and/or destruction of data and network equipment. If necessary, software restoration, replacement of equipment from reserve, and data from the latest backup copy are performed.

3) **Server failure** — The employee responsible for server operation takes measures to immediately bring the backup server into operation to ensure the continuity of the company's operations. If necessary, work is carried out to restore software and data from backup copies.

4) **Data loss** — Upon detection of data loss, the person responsible for information security (system administrator), together with the Technical Director, takes measures to search for and eliminate the causes of data loss (antivirus scan, integrity and operability of software, integrity and operability of equipment, etc.). If necessary, software and data are restored from backup copies.

5) **Virus detected** — Upon detection of a virus, localization of the virus is carried out to prevent its further spread, for which purpose the "infected" computer must be physically disconnected from the LAN and the computer's condition analyzed. The analysis is conducted by a competent specialist. The result of the analysis may be an attempt to preserve (rescue) data, since after rebooting the PC, data may already be lost. After successful virus elimination, the saved data must also be checked for viruses. Upon virus detection, the operating instructions for the antivirus software in use must be followed. After virus elimination, an extraordinary antivirus scan must be performed on all company PCs using updated antivirus databases. If necessary, software and data are restored from backup copies with the drawing up of an act. An internal investigation is conducted regarding the appearance of the virus on the PC (LAN).

6) **Information leak detected (hole in the security system)** — Upon detection of an information leak, the person responsible for information security and the Technical Director are notified. An internal investigation is conducted. If the information leak occurred for technical reasons, a system security analysis is performed and, if necessary, measures are taken to eliminate vulnerabilities and prevent their occurrence.

7) **System hacking (Web server, server, file server, etc.) or unauthorized access** — Upon detection of server hacking, the person responsible for information security and the Technical Director are notified. The server is temporarily disconnected from the network, if possible, for checking for viruses and trojan horses. A temporary transition to a backup server is possible. Given that software bookmarks may not be detected by antivirus software, the integrity of executable files should be especially carefully checked in accordance with the hash functions of the reference software, as well as analyzing the state of script files and server logs. All

passwords related to this server must be changed. If necessary, software and data are restored from the reference archive and backup copies with the drawing up of an act. Based on the results of the situation analysis, the probability of penetration of unauthorized programs into the company's LAN should be checked, after which similar work to check and restore software and data on other company computers should be carried out. An internal investigation is conducted regarding the server hacking.

8) **Attempted unauthorized access** — In the event of an attempted unauthorized access, a situation analysis is conducted based on information from logs of unauthorized access attempts and previous unauthorized access attempts. Based on the analysis results, if necessary, measures are taken to prevent unauthorized access if there is a real threat of unauthorized access. It is also recommended to conduct an unscheduled password change. If software updates eliminating security system vulnerabilities appear, such updates should be applied.

9) **Key compromise** — In the event of key compromise, the operating instructions for the cryptographic protection software in use must be followed.

10) **Password compromise** — In the event of password compromise, the password must be immediately changed, the situation analyzed for the presence of consequences of the compromise, and necessary measures taken to minimize possible (or caused) damage (blocking accounts, etc.). If necessary, an internal investigation is conducted.

11) **Physical damage to LAN or PC** — The person responsible for information security is notified. An analysis for information leakage or damage is conducted. The cause of the LAN or PC damage and possible threats to information security are determined. If there is suspicion of deliberate equipment disabling, an internal investigation is conducted. Software is checked for the presence of malicious bookmark programs, integrity of software and data. Electronic logs are analyzed. If necessary, measures are taken to restore software and data from backup copies with the drawing up of an act.

12) **Natural disaster** — In the event of natural disasters, the relevant Operator documents must be followed.

13) **Procedure and timing for informing management and system personnel about the occurrence of an emergency situation** — When an emergency situation occurs, the system maintenance specialist informs management and system personnel about the occurrence of the emergency situation within 30 minutes by sending an email message and SMS to mobile phones.

14) **Registration of the fact of an emergency situation** — When an emergency situation occurs, the system maintenance specialist registers the fact of the emergency situation (date, time, description of the event) in a special log.

15) **Procedure for actions if problems are not resolved at the level of responsible system personnel within the time provided for by the procedures** — If problems are not resolved at the level of responsible system personnel within the time provided for by the procedures, the system maintenance specialist notifies the Technical Director for decision-making on further actions.

16) **Procedure for informing clients about a major incident** — In the event of a major incident, the Project Director together with the Chairman of the Board decide on the method of communication and, if necessary, inform clients and the public about what happened based on an assessment of the incident's magnitude.

17) **Procedure and timing for informing management and system personnel after elimination of an emergency situation and restoration of normal system functioning** — After restoration of normal system functioning, the system maintenance specialist informs management and system personnel about the restoration of normal system functioning within 30 minutes by sending an email message and SMS to mobile phones, registers in a special log the date, time, cause of the emergency situation, content of measures taken to eliminate it, indicating the responsible executors. Within 2 business days, the Technical Director prepares an act and expert opinion on the emergency situation.

18) **For preventive measures to reduce the risk of unauthorized operations in the payment system** — unlawful intentional acts (actions, omissions, abuse of trust) by personnel of the operator/participant of the system or a third party, aimed at unauthorized access and use of information related to banking secrecy, to obtain/transfer funds from system participants and/or their clients.

The Operator establishes an information security policy (including for the system's information resources) against unauthorized access/operations, abuse or fraudulent modification (insertion, deletion, distortion, substitution), or disclosure of data/information, and implements a set of measures to ensure system security:

- has clearly regulated tasks, requirements for ensuring confidentiality and access to information, adequacy of internal control, as well as criteria for delimitation of responsibility of relevant persons in exercising control;
- ensures timely response to the occurrence of suspicious activity/operations in the system or attempts of unauthorized access/operations, and the procedure for interaction with law enforcement authorities of the Kyrgyz Republic;
- immediately (on the same day when it becomes aware of such event) informs the National Bank in electronic form of facts of external threats, unauthorized access/operations, abuse, robbery, unstable situation, etc. In the event that the event is systemic in nature and may threaten other participants of the financial system of the Kyrgyz Republic;
- provides for the procedure for connecting and using internet resources;
- uses antivirus protection at all workstations and system servers;
- develops new methods of combating unauthorized access/operations/fraud;
- conducts regular security training for employees and system personnel on mechanisms for preventing fraud and unauthorized access.

The procedure for informing the National Bank, as well as Payment System Participants after elimination of an emergency situation and restoration of normal system functioning is carried out within no more than 2 hours, and in the manner provided for by the parties' agreements.

In the event of an incident that may negatively affect the continuity of Participants:

- notifies the party or parties at risk, agents/goods and services providers;
- takes measures to fulfill/complete its financial obligations to service users (clients)/goods and services providers and payment system participants;
- takes measures to ensure data preservation and restoration of the payment system's operability;
- enables other Participants to fulfill their obligations.

The Operator informs the National Bank of the Kyrgyz Republic of an Incident in the event of failures in the payment system lasting more than 2 hours.

Information about disruptions and malfunctions in the Payment System's operation and risks arising in connection therewith is communicated to the Payment System Participants if the risk levels resulting from the violation fall into the "Medium" or "High" category and affect the uninterrupted functioning of the Participants' systems.

In the event of an occurrence that is determined to be "Medium" or "High" risk level, provided that the identified operational disruptions affect the uninterrupted functioning of the Payment System as a whole, immediate notification is made to the Payment Systems Department of the NBKR via telephone communication channels, by email, and any other means of communication for delivering messages to the addressee.

Upon detection of facts of external threats, crimes, fraud in the Payment System that may threaten other Participants, immediate notification is made to the Payment Systems Department of the NBKR via telephone communication channels, by email, and any other means of communication for delivering messages to the addressee.

The Operator ensures timely delivery of information on payments accepted into the system to the goods/services provider in the event of an emergency situation in accordance with the terms of the agreement and the requirements of regulatory legal acts of the National Bank.

---

12. MECHANISMS FOR MANAGING DIRECTORIES OF SENDERS AND RECEIVERS FOR CLIENT VERIFICATION AGAINST INTERNATIONAL AND NATIONAL LISTS OF PERSONS INVOLVED IN CFT/AML

CFT/AML Measures

12.1. The Payment System Operator (Payment Organization) develops and implements an Internal Control Program, including ensuring the availability of Internal Control Rules for CFT/AML and other internal regulatory documents.

12.2. Application of the internal control program. The Operator applies internal control rules in accordance with the legislation of the Kyrgyz Republic in the field of CFT/AML to perform the following main CFT/AML duties:

- implementation of measures to identify, assess, monitor, manage, mitigate, and document risks;
- implementation of participant due diligence measures;
- application of targeted financial sanctions and suspension of operations (transactions);
- application of measures in respect of high-risk countries;
- timely submission to the financial intelligence unit of information and documents, as well as reports on operations (transactions) subject to control and reporting;
- ensuring storage of information and documents on operations (transactions), as well as information obtained as a result of participant due diligence;
- ensuring confidentiality of information;
- ensuring the performance of other duties provided for by the legislation of the Kyrgyz Republic in the field of CFT/AML.

12.3. Use of lists and registers. The Payment System Operator ensures the integration of the Consolidated Sanctions List of the Kyrgyz Republic, the Consolidated Sanctions List of the UN Security Council, the List of Persons, Groups, Organizations in respect of whom there is information about their involvement in the legalization (laundering) of criminal proceeds, the List of Individuals who have served sentences for the legalization (laundering) of criminal proceeds, terrorist or extremist activities, as well as for financing such activities, into the payment system for the purpose of ensuring online monitoring of identification information and their verification.

12.4. Measures to ensure transparency of beneficial owners. All legal entities that are counterparties of the Operator, established and registered in the Kyrgyz Republic, including goods and services providers, payment system operators and payment organizations, Agents/Participants are obliged to:

- form accurate and up-to-date information about the natural person who ultimately (through a chain of ownership and control) directly or indirectly (through third parties) owns the property rights of such legal entity or controls such legal entity (hereinafter — beneficial owner) based on available and accessible information, and also take all available and possible measures to establish their beneficial owner;

- the Operator stores the received information about the beneficial owner for at least five years from the date of its formation.

12.5. Application of a risk-based approach. The Operator applies a risk-based approach in its activities, namely: assesses and continuously updates its risks taking into account the specifics of its activities, the results of the national risk assessment, and typical criteria for high and low risks;

- submits information about identified risks to the relevant supervisory authority and the financial intelligence unit in accordance with the established procedure;
- develops and applies enhanced or simplified policies, as well as control measures and procedures for risk management and mitigation;
- adopts enhanced or simplified participant due diligence measures taking into account the results of risk assessment;
- classifies Participants taking into account risk criteria.

12.6. Procedure for applying the lists of the State Financial Intelligence Service (SFIS) for control and monitoring:

1) The System ensures verification of payers' identification data for the purpose of detecting matches in the List of Persons, Groups, Organizations in respect of whom there is information about their involvement in the legalization (laundering) of criminal proceeds.

2) Upon detection of a match, the System must notify the CFT/AML official of the match.

3) If the payer is included in the List of Persons, Groups, Organizations in respect of whom there is information about their involvement in the legalization (laundering) of criminal proceeds (hereinafter — the identified person), the CFT/AML official is obliged to immediately suspend the operation (payment) and notify the General Director.

4) After suspension of the payment, the CFT/AML official sends a report thereof to the financial intelligence unit within three hours from the moment of suspension of the operation (payment), in accordance with the procedure established by the Regulation on the Procedure for Submitting Information and Documents to the Financial Intelligence Unit of the Kyrgyz Republic, approved by Resolution of the Government of the Kyrgyz Republic dated December 25, 2018, No. 606.

5) For sending messages to the financial intelligence unit, the official registers on the information resource of the financial intelligence unit. The IT department ensures the installation of an Automated Workstation (AWS) — specialized software that allows automated generation and sending of reports on operations (payments) to the financial intelligence unit.

The generation and sending of an electronic message is carried out by the compliance officer to the financial intelligence unit using the AWS. The sequence of actions for generating an electronic message using the AWS, the format and structure of the electronic message, as well as the procedure for using cryptographic protection means for the electronic message, are provided for in the instructional materials included in the AWS package and additionally posted on the official website (www.fiu.gov.kg).

6) After sending the messages, the CFT/AML official checks for the presence or absence of other payments of the identified person in its storage or in the System, and if any — sends a report thereof to the financial intelligence unit within three hours.

12.7. Procedure for applying sanctions lists

1) The System ensures verification of payers' identification data for the purpose of detecting matches in the Consolidated Sanctions List of the Kyrgyz Republic and the Consolidated Sanctions List of the UN Security Council (hereinafter — the Sanctions List).

Upon detection of a match, the System must notify the CFT/AML official of the match.

2) If the payer is included in the Sanctions List (hereinafter — the identified person), the CFT/AML official is obliged to immediately freeze the payment and notify the General Director.

3) The following types of assets and funds are subject to freezing:

- any funds owned or controlled by persons, groups, organizations included in the Sanctions List;
- funds wholly or jointly owned or controlled, directly or indirectly (through third parties), by persons, groups, organizations included in the Sanctions List;
- funds obtained or generated through the use of funds wholly or jointly owned or controlled, directly or indirectly (through third parties), by persons, groups, organizations included in the Sanctions List;
- funds of persons, groups, organizations acting on behalf of or at the direction of persons, groups, organizations included in the Sanctions List;
- funds intended for the financing of terrorist and extremist activities, terrorists and extremists, terrorist and extremist organizations, or persons proliferating weapons of mass destruction;
- funds specified in the relevant resolutions of the UN Security Council.

Operations (payments) and/or funds of a natural person, legal entity, group, organization included in the Sanctions List are frozen for an indefinite period and are unfrozen when the natural person, legal entity, group, organization is removed from the Sanctions List.

The CFT/AML official ensures the protection of the rights of bona fide third parties acting with honest intentions when applying targeted financial sanctions and freezing payments and funds.

4) After freezing the payment, the CFT/AML official sends a report thereof to the financial intelligence unit within three hours from the moment of suspension of the operation (payment), in accordance with the procedure established by the Regulation on the Procedure for Submitting Information and Documents to the Financial Intelligence Unit of the Kyrgyz Republic, approved by Resolution of the Government of the Kyrgyz Republic dated December 25, 2018, No. 606.

5) For sending messages to the financial intelligence unit, the official registers on the information resource of the financial intelligence unit. The IT department ensures the installation of an Automated Workstation (AWS) — specialized software that allows automated generation and sending of reports on operations (payments) to the financial intelligence unit.

6) After sending the messages, the CFT/AML official checks for the presence or absence of other payments of the identified person in its storage or in the System, and if any — sends a report thereof to the financial intelligence unit within three hours.

7) The Compliance Officer checks the presence of officials, founders, and beneficial owners of goods/services providers, agents, and sub-agents of natural and legal persons in the Sanctions List and the List of Persons, Groups, Organizations in respect of whom there is information about their involvement in the legalization (laundering) of criminal proceeds.

If the full names of officials, founders, and beneficiaries are present in the list, based on a statement from the CFT/AML official, the General Director makes a decision to refuse the provision of any type of services, and the CFT/AML official immediately reports the information to the SFIS under the Government of the Kyrgyz Republic.

8) Unfreezing of payments and funds, as well as access to funds and payments frozen in the Company, is carried out with the coordination and participation of the CFT/AML official and the General Director of the Company, in accordance with the procedure provided for in the Regulation on the Procedure for Suspension of Operations (Transactions), Freezing and Unfreezing of Operations (Transactions) and/or Funds, Granting Access to Frozen Funds, and Management of Frozen Funds, approved by Resolution of the Government of the Kyrgyz Republic dated December 25, 2018, No. 606.

Appendix No. 1
to the Rules of the Payment System of PrimeTech LLC

Tariff Policy

The Tariff Policy reflects the general objectives that the Operator seeks to achieve when setting prices for the services provided.

When setting prices for goods, general economic criteria are taken into account that determine price deviations in one direction or another from the use value of payment services.

These criteria can be divided into internal (depending on the management and various services of the enterprise) and external (independent of the enterprise itself and beyond its control).

Internal criteria include:

- Service quality;
- Operator's image.

External criteria are as follows:

- Social significance of the service;
- Presence and expansion of the payment services market;
- Participants and their requirements for the payment services market;
- Regulatory framework;
- Political stability of the state;
- Presence and level of competition;
- Other factors.

The method of price determination based on demand, level of competition, and Participant requirements is used. The Operator uses a combined system of price determination methods simultaneously with solving the task of developing the network of payment services, the network of points and methods of payment acceptance. The structure of tariffs, fees, and commissions must satisfy the goal of achieving the profitability level established by the Operator.

In certain cases dictated by the requirements of goods and services providers, demand, and the price level for tariffs, fees, and commissions in respect of services provided by payment organizations and payment system operators of the Kyrgyz Republic, as well as decisions of the Company — the structure of tariffs, fees, and commissions may differ from the established profitability level.

Before determining tariffs, fees, and commissions, a market analysis of demand and the price level for tariffs, fees, and commissions provided by payment organizations and payment system operators of the Kyrgyz Republic is conducted.

Notification of Participants and users about applied tariffs, fees, and commissions is carried out in accordance with these Rules and the Participant's agreement.

The Payment System Operator, once a year from the date of obtaining the license, submits to the National Bank information on approved and current tariffs. The Payment System Operator must notify the National Bank of all changes to current tariffs within 10 (ten) business days after changing the tariffs.