**QIWI Wallet Payment System**

**Operating Rules**

**(v.2, dated 01/06/2014)**

**CONTENTS**

[1. General Provisions 3](#_Toc438331396)

[2. Use of E-money 4](#_Toc438331397)

[2.1. General Issues Pertaining to the Issue of E-money 4](#_Toc438331398)

[2.2. General Issues Pertaining to the Sale of E-money 4](#_Toc438331399)

[2.3. General Issues Pertaining to the Redemption of E-money 4](#_Toc438331400)

[3. Payments with E-money 6](#_Toc438331401)

[3.1. General Issues Pertaining to Making Payments with E-money 6](#_Toc438331402)

[3.2. Payments for Goods or Services and Loan Repayments. 6](#_Toc438331403)

[3.2.1. General Issues Pertaining to Payments for Goods or Services and Loan Repayments 6](#_Toc438331404)

[3.2.2. Requirements for Making Payments for Goods or Services and Loan Repayments to Merchants 6](#_Toc438331405)

[4. Risk Management 7](#_Toc438331406)

[4.1. General Provisions Pertaining to Risk Management 7](#_Toc438331407)

[4.2. Threat and Vulnerability Identification 7](#_Toc438331408)

[4.3. Assessing Information Security Risks 7](#_Toc438331409)

[4.4. Processing Information Security Risks 8](#_Toc438331410)

[5. Dispute Resolution 9](#_Toc438331411)

[5.1. Claims by System Participants 9](#_Toc438331412)

[5.2. Claim Consideration 9](#_Toc438331413)

[5.3. Conciliation Committee 9](#_Toc438331414)

[5.4. Arbitration 10](#_Toc438331415)

[6. Appendices to Operating Rules 11](#_Toc438331416)

[6.1. Appendix 1: Procedure for Assessing Information Security Risks in Automated Information Systems 11](#_Toc438331417)

[6.2. Appendix 2: Procedure for, and Rules of Conciliation Committee 14](#_Toc438331418)

# General Provisions

The Operating Rules of the QIWI Wallet Payment System (“Operating Rules”) are regulations for the System, which set forth the rules governing the System Participants’ activities in the QIWI Wallet Payment System.

The Operating Rules set forth:

* the procedure for the use of e-money;
* the procedure for making payments with e-money;
* the risk management process for the System; and
* the procedure for dispute resolution between the System Participants and between the System Participants and persons, which are not members of the System.

# Use of E-money

The “use of e-money” in the QIWI Wallet Payment System means the activities of the Issuing Bank associated with the issue, sale and redemption of, and making payments with, e-money.

The Issuing Bank prepares an agreement to be entered into between the Issuing Bank and an individual, which is the potential e-money holder, subject to the general Rules of the System. The Issuing Bank prepares an agreement to be entered into between the Issuing Bank and a legal entity, which is the potential Agent of the Issuing Bank, subject to the general Rules of the System.

## General Issues Pertaining to the Issue of E-money

The Issuing Bank has the right to issue e-money in the QIWI Wallet Payment System.

The Issuing Bank issues e-money within the amount paid by the Issuing Bank’s Agent or an individual to the Issuing Bank in accordance with the agreement entered into by the Issuing Bank and such Issuing Bank’s Agent or individual.

By issuing e-money, the Issuing Bank assumes payment obligations, which substitute claims for e-money from Merchants and/or E-money Holder as payment for goods or services, as well as claims from the System Participants and/or E-money Holders for the repayment of the E-money Holders’ loan obligations to a System Participant (“Loan Repayment”), including payment obligations in an electronic form.

E-money is issued in the currency of the country, of which the Issuer is a resident and where it issues e-money.

## General Issues Pertaining to the Sale of E-money

In the QIWI Wallet Payment System, the Issuing Banks have the right to sell e-money on their own, or with the involvement of agents under respective agreements between the Issuing Bank and the Issuing Bank’s Agent (unless this is contrary to the Applicable Laws). E-money is sold by means of the Issuing Bank (or its Agent) receiving cash from an individual, or by means of transferring money by an individual to the respective account of the Issuing Bank.

When e-money is sold, the holder of such e-money is provided with a receipt or another confirmation of their purchase of e-money. The form and means of issuing receipts for the sale of e-money are set forth in the respective agreement to be entered into between the Issuing Bank and an individual, who is the potential e-money holder. The content of the receipt must comply fully with the requirements of the Applicable Law.

The Issuing Bank’s Agent may sell e-money via electronic terminals, which accept cash, or cash offices, or by other means, which do not contradict the Applicable Law, under an agreement entered into between the Issuing Bank and the Issuing Bank’s Agents.

E-money is considered sold to the E-money Holder when information on the available balance of e-money in the E-money Holder’s e-wallet is displayed.

## General Issues Pertaining to the Redemption of E-money

In the QIWI Wallet Payment System, the Issuing Banks may redeem e-money if this does not contradict the Applicable Law.

The Issuing Bank redeems e-money when an E-money Holder provides it for redemption. The Issuing Banks redeems e-money by providing cash to the person who has presented it for redemption, or by means of a transfer to the bank account specified by the E-money Holder.

When e-money is redeemed, the amount of cash/money provided/transferred to the E-money Holder, who has presented e-money for redemption, must be equal to the amount of e-money presented for redemption. E-money is considered to be redeemed by the Issuing Bank when the E-money Holder who has presented e-money for redemption is provided with the respective amount of cash or when the respective amount is credited to the bank account specified by the E-money Holder.

# Payments with E-money

## General Issues Pertaining to Making Payments with E-money

The Issuing Bank shall effect transactions with e-money in accordance with these Operating Rules, the agreements entered into between the Issuing Banks and the Issuing Bank’s Agents or Merchants, and the Applicable Law.

A transaction with e-money is effected based on an instruction from the E-money Holder submitted with the use of equipment and methods determined by the Issuing Bank. To ensure the safety of transactions with e-money, the Issuing Bank must only use such equipment and methods, which it is entitled to use by the System Operator when the Issuing Bank joins the QIWI Wallet Payment System.

An instruction from the E-money Holder to effect a transaction with e-money must indicate the transaction amount, the recipient of e-money, and other details specified by the Issuing Bank in the agreement entered into with the E-money Holder. A transaction with e-money is effected by means of debiting e-money from the e-wallet of the E-money Holder who has sent the respective instruction and their transfer to the recipient indicated by such E-money Holder.

A transaction with e-money is accompanied with the issue to the E-money Holder who has sent an instruction to effect the respective transaction of a document, which confirms the respective transaction. The form and means of the issue of such confirmation are set forth in the respective agreement entered into between the Issuing Bank and the E-money Holder. The content of the document, which confirms the transaction with e-money, must be fully compliant with the requirements of the Applicable Law.

As and when requested by the E-money Holder, the Bank must provide them with a report on all transactions effected by the E-money Holder in their e-wallet. The format and the timeframes for the provision of such report are set forth in the agreement entered into between the Issuer and the E-money Holder.

## Payments for Goods or Services and Loan Repayments.

### General Issues Pertaining to Payments for Goods or Services and Loan Repayments

Payments for goods or services and loan repayments with e-money may be effected with Merchants, which sell such goods or services. Payments for goods or services are made within the limits established by the Issuing Bank.

### Requirements for Making Payments for Goods or Services and Loan Repayments to Merchants

When making payments for goods or services to Merchants, the System Participants must comply with the following requirements:

* checking the transaction for compliance with limitations set by the Issuing Bank;
* ensuring that the transaction with e-money, which is planned to be effected, is authorised;
* producing a primary confirmation of the transaction in an electronic form; and
* providing the E-money Holder with a hard copy of the transaction confirmation in a format compliant with the requirements of the Applicable Law.

# Risk Management

## General Provisions Pertaining to Risk Management

The main functions of the System Operator associated with the ensuring of safety of transactions effected by the System Participants in connection with the issue, sale and redemption of e-money are as follows:

* identifying threats and vulnerabilities in automated information systems;
* assessing information security risks in automated information systems; and
* processing information security risks in automated information systems.

This section of the Operating Rules sets forth the procedure for assessing information security risks in automated information systems and the methods for processing the risks identified.

The procedure extends to, and is binding on, all the System Participants and their automated information systems.

## Threat and Vulnerability Identification

The identification of threats and vulnerabilities in automated information systems is done collectively, with the involvement of representatives of the System Operator, the Issuing Bank, the automated information systems of which are subject to assessment, and other System Participants, which interact with the automated information systems of the assessed Issuing Bank.

The identification of threats and vulnerabilities in automated information systems is performed each time when new threats and vulnerabilities are revealed, however not less than once a year.

The following must be taken into account when identifying threats and vulnerabilities:

* data on information security incidents in the automated information systems of the Issuing Bank;
* the results of checks approved in the System (scanning for vulnerabilities, penetration tests, monitoring of information security events, etc.);
* opinions of the involved System Participants; and
* information from external special knowledge databases (news feeds, etc.).

The assessed Issuing Bank maintains a register of threats and vulnerabilities identified.

## Assessing Information Security Risks

Information security risks are assessed by a risk assessment committee (“Risk Assessment Committee”) at least once a year, or when material changes, which affect the results of previous assessments, occur.

The Risk Assessment Committee comprises representatives of the System Operator, the Issuing Bank, and other System Participants, which use and/or interact with the assessed automated information systems, and is formed of specialists, which have sufficient knowledge of the key automated information systems used, main processes, and risks.

An authorised representative of the System Operator (“Chair of the Risk Assessment Committee”) arranges the work of, prepares initial information for, moderates and chairs the Risk Assessment Committee.

Information security risks in automated information systems are assessed as set forth in Appendix 1 hereto.

The Risk Assessment Committee prepares a Risk Assessment Report, which is approved by the Chair of the Risk Assessment Committee and includes recommendations by the Risk Assessment Committee on improvements in the automated information systems of the Issuing Banks necessary to prevent information security threats and eliminate vulnerabilities in such systems.

## Processing Information Security Risks

The System Operator determines an acceptable level of information security risks in the automated information systems of the System Participants.

The possible actions with the assessed risks include:

* selecting and applying protective measures to reduce risks to the acceptable level;
* preventing risks by means of excluding risky actions and/or optimising the operation of automated information systems;
* transferring risks to third persons, which are not System Participants (for example, arranging insurance against information security risks);
* accepting the risks, which do not exceed the acceptable levels; or
* accepting risks if the cost of protective measures exceeds the possible damage from the respective threat.

When considering Risk Assessment Reports, the Risk Assessment Committee passes risk processing decisions: the risks, which do not exceed acceptable levels, are accepted while other risks are mitigated, prevented or transferred.

Based on the decision of the Risk Assessment Committee, the System Operator devises the Information Security Risk Processing Plan for risks, which require measures to be taken.

The devised and approved Information Security Risk Processing Plan must be performed by the System Participants during the period advised by the System Operator. After the Risk Processing Plan is fulfilled, a follow-up identification of threats and vulnerabilities in the automated information systems of the respective System Participant is undertaken.

# Dispute Resolution

## Claims by System Participants

If a System Participant has any claims to the System Operator and/or other System Participants with respect to any controversies relating to the System Participant’s activities in the QIWI Wallet Payment System, the System Participant may send a respective written claim to the System Operator.

If a System Participant disputes transactions with e-money effected in the System, they may submit the respective claim in one of the following instances only:

* a transaction with e-money has not been effected through the fault of one of the System Participants; or
* a transaction with e-money has been blocked by the System Operator as allegedly illegal.

The claim submitted by the System Participant must be accompanied with the evidence of facts or circumstances, because of which it is submitted.

System Participants may submit claims by any of the following means:

* electronically, by means of the electronic exchange of documents; or
* by registered post, return receipt requested and a description of the contents included; or
* via a courier, with confirmation of receipt from a representative of the System Operator.

## Claim Consideration

The System Operator considers claims from System Participants within ten (10) business days of receiving them.

After considering a claim, the System Operator takes one of the following actions:

* if the claim from a System Participant is validated in full or in part, the System Operator takes action to satisfy it;
* if the claim from a System Participant is not validated, the System Operator sends explanations on the disputed transaction to the claiming System Participant.

## Conciliation Committee

If the claiming System Participant disagrees with the System Operator’s explanations, such System Participant may require that the dispute be referred to the Conciliation Committee. The claiming System Participant may require that the dispute be referred to the Conciliation Committee within five (5) business days of receiving the System Operator’s explanations on their claim.

The Conciliation Committee comprises representatives of the System Operator, the claiming System Participant, and other System Participants, which took part in the disputed transaction/transactions. The Conciliation Committee is formed by the System Operator within ten (10) business days of receiving the respective request from the claiming System Participant.

The Conciliation Committee considers the dispute as set forth in Appendix 2 hereto.

Within five (5) business days of the Conciliation Committee’s completion of dispute consideration, the System Operator must send the resolution of the Conciliation Committee, including respective explanations and instructions (if the System Participant’s claim is validated in full or in part), to all involved System Participants.

## Arbitration

If any System Participant, the interests of which are affected by a resolution of the Conciliation Committee, disagrees with such resolution, such System Participant may, within thirty (30) calendar days of receiving the resolution, notify the System Operator of their disagreement. The notice of disagreement must state the disputed issues and the reasons for disagreement.

Neither party to the dispute may bring it to a court unless it provides a notice of disagreement with the resolution of the Conciliation Committee as stated above.

If neither party to the dispute provides a notice of disagreement with the resolution of the Conciliation Committee within thirty (30) calendar days of receiving such resolution, the resolution is deemed final and binding on all the involved System Participants.

If the System Operator receives a notice of disagreement from any party to the dispute, the involved System Participants must try to resolve the dispute by negotiations before initiating proceedings. However, unless the parties agree otherwise, proceedings may be initiated on expiry of forty-five (45) calendar days of sending the notice of disagreement, even if no attempts were made to resolve the dispute in an amicable manner.

Any dispute, in which the resolution of the Conciliation Committee is not final and binding on all the involved System Participants and which is not resolved in an amicable manner, must be referred for final resolution in accordance with the Applicable Laws to the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry, in accordance with its current Rules.

In such proceedings, neither of the System Participants may be limited by the provision of evidence or arguments, which were provided earlier to the Conciliation Committee for it to pass its resolution, or the reasons for disagreement stated in the notice of disagreement. Any resolution of the Conciliation Committee may be submitted to a court as confirmation or evidence.

# Appendices to Operating Rules

## Appendix 1: Procedure for Assessing Information Security Risks in Automated Information Systems

The initial data for risk assessment is as follows:

* the list of information systems, processes and other assets subject to risk assessment;
* the most recent Register of Threats and Vulnerabilities; and
* the results of previous information security risk assessments.

In assessing information security risks, the Risk Assessment Committee determines threats and vulnerabilities associated with each asset and assesses their likelihood and impact, proceeding from their knowledge of the protective measures in place and the value of the respective asset. The Information Security Risk Assessment Report is the document to be produced as a result of the process.

The likelihood of an information security incident is assessed using the values provided below and is a measure of how likely it is that a threat may occur with respect to a given asset, given the protective measures in place.

To assess the likelihood of the occurrence of an information security threat, information assets are analysed for the possible loss of each of their information security properties as a result of the influence of the identified threat-sources.

The main factors in assessing the likelihood of the occurrence of information security threats are as follows:

* information on the respective threat models, in particular:
* data on the location of a threat-source in relation to the respective types of environmental objects;
* information about threat-source motivation (for man-made threats);
* assumptions as to the qualification and/or resources of a threat-source;
* statistics on the frequency of threat exercise by its source in the past;
* information on the ways of information security threat exercise by its source;
* information on how difficult it is to identify the exercise of a threat by its source; and
* information on the organisational, technical and other prior protective measures in place in the given types of environmental objects.

The following qualitative scale is used to assess the likelihood of the occurrence of an information security threat:

* very unlikely - 1;
* unlikely - 2;
* likely - 3;
* very likely - 4;
* exercisable - 5.

If several experts are involved in assessing the likelihood of the occurrence of information security threats and different expert opinions are obtained, the final, summarised assessment of the likelihood should be the expert assessment, which determines the highest likelihood of the occurrence.

For man-made threats, the likelihood of the occurrence of a threat through exercising a vulnerability is directly proportional to the qualification of the violator necessary for its exercise.

To assess the impact of an information security incident, each type of information assets is analysed for the consequences of the loss of each type of information security properties as a result of the identified threat-sources’ influence on the respective types of environmental objects.

The main factors in assessing the impact of information security incidents are as follows:

* the degree of influence on the continuity of operations;
* the degree of influence on goodwill;
* the amount of financial losses;
* the amount of costs necessary to restore information security for the given type of information assets and eliminate the consequences of the information security incident;
* the quantity of human resources necessary to restore information security for the given type of information assets and eliminate the consequences of the information security incident;
* the amount of time necessary to restore information security for the given type of information assets and eliminate the consequences of the information security incident;
* the degree of violation of the statutory requirements and/or contractual obligations;
* the degree of violation of the requirements of regulatory and controlling/supervisory authorities for information security;
* the amount of the stored, transmitted, processed and deleted information relating to the given type of environmental objects; and
* information on the organisational, technical and other prior protective measures in place in the given types of environmental objects.

The following qualitative scale is used to assess the impact of an information security incident occurring as a result of the occurrence of an information security threat:

* insignificant - 1;
* low - 2;
* significant - 3;
* serious - 4;
* critical - 5.

If several experts are involved in assessing the impact of an information security incident and different expert opinions are obtained, the final, summarised assessment of the impact should be the expert assessment, which determines the most serious degree of the impact.

Each member of the Committee provides their subjective assessment of the likelihood and impact of the threats for the scope of risk assessment under consideration.

The resulting assessment is calculated using the formula:

***AR = (A1 + A2 +…+ An) / n,*** where***:***

AR is the resulting assessment;

Ai is the assessment provided by the ith member of the Committee; and

n is the total number of the members of the Committee.

The resulting assessments are recorded by the Chair of the Committee in the Information Security Risk Assessment Report.

The risks for assets are calculated using the formula:

***R = Likelihood x Impact,*** where***:***

R is the risk assessed;

Likelihood is the likelihood of the occurrence of the information security threat;

Impact is the degree of impact of the information security incident.

Risks may be in the range between 1 and 25.

The Risk Assessment Report must be approved by all members of the Committee and the System Operator.

## Appendix 2: Procedure for, and Rules of Conciliation Committee

1. The Conciliation Committee considers disputes within forty-five (45) calendar days of being formed.
2. A resolution on a dispute is deemed to be passed by the Conciliation Committee if it is passed by all arbitrators unanimously.
3. In the course of dispute consideration by the Conciliation Committee, the System Participants must furnish to the Conciliation Committee copies of any documents, which pertain to the dispute, as may be requested by the Conciliation Committee. Copies of all correspondence between the Conciliation Committee and the System Participants must be sent to all System Participants.
4. The Conciliation Committee must act in accordance with these Rules. The Conciliation Committee must:

* act in a fair and unbiased manner when considering disputes between the System Participants and provide each of them with a reasonable opportunity to state their arguments and respond to the arguments stated by other System Participants involved in the dispute; and
* use procedures acceptable for each dispute, without unnecessary delay or expenses.

1. The Conciliation Committee may convene a hearing of the dispute. In such an event the Conciliation Committee determines the date and venue for the hearing and may require that the System Participants provide documents and written arguments before or during the hearing. The Conciliation Committee must notify the System Participants about the hearing via the System Operator not later than ten (10) calendar days before the hearing.
2. The Conciliation Committee is authorised to approve investigation procedures, deny access to the hearing for any persons except representatives of the involved System Participants, and conduct the hearing in the absence of representatives of any of the System Participants, which were notified about the hearing by the System Operator.
3. The Conciliation Committee has the following powers, among others:

* to determine the acceptable dispute resolution procedure;
* to determine on its own the scope of its authority and the extent any dispute relates to it;
* to conduct the hearing as it deems necessary and be guided exclusively by the procedure and rules set forth in the System regulations;
* to take the initiative in investigating the facts and circumstances necessary to pass its resolution; and
* to use its own special knowledge, if available.

1. The Conciliation Committee must not express its opinion as to the weight of any arguments provided by the System Participants involved in the dispute during the hearing.
2. The Conciliation Committee must pass its resolution and notify all involved System Participants via the System Operator accordingly in writing within ten (10) calendar days of passing the resolution.