

**OPERATIONAL AND LIQUIDITY RISK**  
**MANAGEMENT POLICY**

**BEETELLER GROUP**

Date 11.11.2022  
Version [2.0]

---

---

|                            |  |
|----------------------------|--|
| <b>Title</b>               | Operational and liquidity risk management policy |
| <b>Reference</b>           | PGROL  |
| <b>Classification</b>      | Internal   |
| <b>Version</b>             | 2.0  |
| <b>Status</b>              | Review   |
| <b>Approver</b>            | Partners and directors                           |
| <b>Approval date</b>       | 11/11/2022                                       |
| <b>Date of next review</b> | 1 (one) year after the date of the last approval |
| <b>Policy owner area</b>   | Operational                                      |

## SUMMARY

|    |   |    |
|----|---|----|
| A. | SCOPE OF THIS POLICY .....  | 4  |
| 1. | Goal .....  | 4  |
| 2. | Scope.....  | 4  |
| 3. | Applicable Standards.....   | 4  |
| 4. | Definitions.....  | 5  |
| B. | RISK MANAGEMENT .....   | 6  |
| 1. | Risk Management Structure.....                                      | 6  |
| 2. | Responsibilities.....   | 7  |
| 3. | Strategies .....  | 7  |
| C. | OPERATIONAL RISK .....  | 8  |
| 1. | Scope.....  | 8  |
| 2. | Prevention, identification and treatment of Operational Risks ..... | 9  |
| D. | LIQUIDITY RISK .....  | 10 |
| 1. | Scope.....  | 10 |
| 2. | Prevention, identification and treatment of Liquidity Risks .....   | 10 |
| E. | RISK TRANSACTION RATING MATRIX .....                                | 11 |
| F. | RISK MONITORING .....   | 11 |
| G. | CONTINGENCY AND BUSINESS CONTINUITY MANAGEMENT .....                | 11 |
| H. | TROUBLESHOOTING PROCEDURES .....                                    | 12 |
| I. | THE PARTICIPATION IN OPEN FINANCE .....                             | 11 |
| J. | APPLICATION OF FUNDS HELD IN PAYMENT ACCOUNTS                       |    |
|    | 132   |    |
| K. | FINAL TERMS .....   | 15 |
|    | AAPPENDIX I   | 17 |
|    | APPENDIX II   | 18 |

## A. SCOPE OF THIS POLICY

### 1. Goal

The purpose of this Operational and Liquidity Risk Management Policy ("Policy") is to establish the general guidelines, criteria and procedures adopted for the management of operational and liquidity risks, governance, safeguarding of funds held in payment accounts, in order to enable the identification, assessment, monitoring, treatment, communication of operational and liquidity risks of **BEETELLER GROUP** compliance with Bacen regulations and best practices.

### 2. Scope

The Policy applies to all directors (collectively "Senior Management"), employees and contractors<sup>1</sup> of BEETELLER (collectively, including Senior Management, referred to simply as, "Employees").

Risk management is inherent to BEETELLER's activity and, therefore, it is everyone's duty to comply with this Policy. It is up to the Top Management, or the area determined by it, the disclosure and implementation of its measures and procedures.

### 3. Applicable Standards

- **LAW No. 12,865/2013:** provides for the Payment Arrangements and Payment Institutions integrating the Brazilian Payment System (SPB).
- **BACEN Circular Nº 3,681/2013:** Provides for risk management, minimum equity requirements, governance of payment institutions, preservation of value and liquidity of balances in payment accounts.
- **BCB RESOLUTION Nº 80/2021:** establishes the requirements and procedures for the constitution and operation, and for the application for authorization to operate of Payment Institutions and provides for the rendering of payment services by other institutions authorized to operate by the Bacen.
- **JOINT RESOLUTION No. 01/2020:** provides for the implementation of the Open Finance System.
- **BCB RESOLUTION No. 01/2020:** Creates the PIX payment arrangement and approves its Regulation.
- **BCB RESOLUTION Nº 197/2022:** Classifies the prudential conglomerate composed of at least one institution that provides payment services and establishes the

---

<sup>1</sup> Any third parties acting on behalf of BEETELLER, such as External Audit, Legal Counsel, Information Technology, IT Infrastructure, among others.

---

segmentation for prudential conglomerates classified as Type 3 for the purposes of proportional application of prudential regulation.

- **BCB RESOLUTION No. 198/2022:** Provides for the minimum Payment Institution Reference Equity (PRIP) requirement for Type 2 conglomerates, pursuant to Resolution BCB No. 197/2022, and for payment institutions that are not part of a prudential conglomerate, and on the methodology for calculating these requirements and the respective continuous risk management structure.
- **CMN Resolution Nº 3,919/2010:** Changes and consolidates the rules on the collection of fees for the provision of payment services to end users, including for the purposes of remuneration.

#### 4. Definitions

- **Top Management:** Formed by BEETELLER's Partners and Administrators.
- **Payment Arrangement:** set of rules and procedures that disciplines the provision of a certain payment service to the public by Law No. 12,865/2013.
- **Bacen:** Central Bank of Brazil.
- **Payment Account:** account owned by the User, intended for the loading, transfer and redemption of funds, whose values, converted into electronic currency, will be managed and held in custody by BEETELLER.
- **Payment Institution:** for the purposes of this Policy, is BEETELLER as the issuer of electronic currency, whose activity consists of managing the Payment Account of Users, used for the payment of prepaid transactions.
- **Open Finance:** standardized sharing of data and services through openness and systems integration.
- **Pix:** Payment arrangement set up by Bacen that disciplines the provision of payment services related to Instant Payment Transactions under the arrangement.
- **Risk:** possibility of the materialization of an event that results in negative impacts to the operation of BEETELLER's business.
- **Operational Risk:** possibility of losses resulting from failures, deficiencies or inadequacy of internal processes, people and systems, or from external events. The scope of this definition also includes the legal risk associated with inadequacy or deficiency in signed contracts, in addition to sanctions that may be imposed due to noncompliance with legal provisions and compensation for damages to third parties.

- 
- **Liquidity Risk:** the potential for a mismatch of financial flows of assets and liabilities, as well as its effects on BEETELLER's financial capacity to obtain funds and honor its obligations.
  - **Payment System:** services related to the opening of a Payment Account and the carrying out of fund loading, transfer and redemption Transactions by the User, including the provision of information on fund transfers and statements.
  - **Transaction:** operation in which the User performs the operation of his/her Payment Account, loading funds, transferring funds to the Payment Account held by other Users, or redeeming funds to the User's bank account or that of a third party indicated by him/her.
  - **User:** an individual or legal entity, holder of a Payment Account, who, by adhering to the Payment Account opening term, is qualified to make Transactions through the Payment System.
  - **Risk Matrix:** guideline for the qualitative and/or quantitative assessment of the effect of risks on BEETELLER's strategic objectives.
  - **Risk Appetite Statements ("RAS"):** this is the Risk Tolerance Appetite, defined as the acceptable level of variation in achieving a given objective.
  - **Risk Response Plan:** set of measures adopted to reduce the inherent risk to a level that is in line with BEETELLER's Risk Tolerance.
  - **Incident:** this is the materialization of the risk.

## B. RISK MANAGEMENT

### 1. Risk Management Structure

To ensure the effectiveness of this Policy, the Risk Management Structure ("Risk Structure") provides for a shared performance for the management of each risk. All Collaborators who perform activities related to the risks that are the subject matter of this Policy have the duty to ensure the compliance of the risk management processes.

The Risk Management Framework shall provide policies and strategies approved and reviewed, annually, by the board of directors and/or senior management, to determine its compatibility with BEETELLER's objectives and with market conditions; and shall keep this documentation on the policies, risk management strategies and governance at the disposal of the BACEN, with criteria for deciding on the outsourcing of services and for selecting their providers, including the minimum contractual conditions necessary to mitigate the operational risk, and the continuity of the payment services provided.

---

The Risk Framework has three main lines of defense:

- **FIRST LINE OF DEFENSE:** composed of managers with business functions or activities that generate exposure to risks, in accordance with policies, limits and procedures defined by the Risk Department and approved by Senior Management, and who manage and implement the actions for monitoring and mitigating the risks associated with the processes under their responsibility.
- **SECOND LINE OF DEFENSE:** composed of the areas or people responsible for Compliance, Controls, and Risk Management, as the case may be, responsible for defining the methods for identifying, assessing, and monitoring the degree of exposure to operational risks.
- **THIRD LINE OF DEFENSE:** composed of the internal audit areas, or persons responsible for the activities that provide independent and periodic verification and evaluation of the efficacy of the processes and procedures established for risk control and management, including the degree of exposure and adequacy of the structure of BEETELLER's internal systems.

## **2. Responsibilities**

It is up to the Top Management:

- Approve and review, annually, the Risk Management Policy;
- Approve the strategic risk planning, the Risk Matrix, Risk Tolerance limits, Risk Response Plan, and business continuity policies;
- Ensure compliance with this policy;
- Appoint the Chief Risk Officer (CRO).

It is up to the Chief Risk Officer (CRO):

- Define objectives and develop policies and procedures related to strategic risk planning, Risk Matrix, Risk Tolerance limits, Risk Response Plan, and business continuity policies;
- Monitors the degree of adherence of the risk management framework's processes to policies;
- Periodically inform the Senior Management about the policies, procedures and events that are the object of this Policy;
- To ensure compliance with this Policy by managers with business functions or activities that generate exposure to risks, and by those responsible for defining the methods for identifying, assessing and monitoring the degree of exposure to operational risks.

## **3. Strategies**

The Risk Framework will perform its activities with the purpose of ensuring the realization of the following responsibilities:

- 
- **Identification of Events:** the internal and external events that influence the Operational Risk are identified and classified between risks and opportunities. These opportunities are channeled into management's strategy or objective setting processes;
  - **Risk Assessment:** Risks are analyzed considering probability and consequence to determine the way in which they should be managed;
  - **Control Activities Evaluation:** these are the existing control activities in the processes, bearing in mind that an effective internal control system reduces the probability of human errors and irregularities in processes and systems, resulting in the reduction of operational losses;
  - **Risk Response and Mitigation:** in the face of risk, BEETELLER establishes the response to it, which includes avoiding, reducing, sharing or accepting risk according to the assessment of the effect, costs and benefits. Actions are developed to maintain the alignment of the RAS;
  - **Monitoring and Communication:** Monitoring is carried out through continuous management activities and/or independent evaluations. All the results of this management are reported to Senior Management by means of reports that signal the qualitative and quantitative aspects of BEETELLER's exposure to operational risk.
  - **Adequate application of resources:** BEETELLER shall ensure the human and technical resources to implement the objectives and responsibilities of the Risk Framework. The application of these resources includes qualified staff and security, control and data monitoring systems.

## C. OPERATIONAL RISK

### 1. Scope

The following are considered Operational Risk events:

- Failures to protect and secure sensitive data related to both end-user credentials and other information exchanged for the purpose of making payment transactions;
- Failures in end-user identification and authentication;
- Payment transaction authorization failures;
- Internal fraud;
- External fraud;
- Labor claims and poor workplace safety;
- Inappropriate practices regarding end users, payment products and services;
- Damage to physical assets owned or in use by BEETELLER;
- Occurrences leading to interruption of BEETELLER's payment activities or discontinuation of the payment services provided.
- Failures in systems, processes, or information technology infrastructure;
- Failure to execute, meet deadlines, and manage the activities involved in payment arrangements;
- Failed payment transaction initiation.



## 2. Prevention, identification and treatment of Operational Risks

For the prevention, identification and treatment of Operational Risks, BEETELLER will adopt:

- Contingency plan and other mechanisms to ensure the continuity of the payment services provided;
- Mechanisms for the protection and security of stored, processed or transmitted data;
- Mechanisms to protect and secure networks, electronic sites, servers, and communication channels in order to reduce vulnerability to attack;
- Procedures for monitoring, tracking, and restricting access to sensitive data, networks, systems, databases, and security modules;
- Procedures for monitoring data security breaches and end-user complaints about them;
- Procedures for reviewing security and data secrecy measures, especially after failures occur and prior to changes in infrastructure or procedures;
- Preparation of reports that indicate procedures to correct identified failures;
- Performing tests to ensure the robustness and effectiveness of the data security measures adopted;
- Segregation of functions in the information technology environments for development, testing, and production;
- Proper identification of the end user;
- Mechanisms for authenticating end users and authorizing payment transactions;
- Processes to ensure that all payment transactions can be properly tracked;
- Mechanisms for monitoring and authorizing payment transactions, in order to prevent fraud and detect and block suspicious transactions in a timely manner;
- Specific evaluations and filters to identify transactions considered high risk;
- Notification to the end user about possible non-execution of a transaction;
- Mechanisms that allow the end user to verify that the transaction was executed correctly;
- Criteria for deciding to outsource services and for selecting service providers;
- Mechanisms for monitoring and controlling payment transaction initiation failures, segregating at least the following events: i) unauthorized payment transaction initiation; ii) non-execution of payment transaction initiation; iii) incorrect payment transaction initiation execution; and iv) delay in payment transaction initiation.

- 
- Assessment, management and monitoring of the operational risk arising from outsourced services relevant to the regular operation of the payment institution. Where outsourced services are provided, BEETELLER shall stipulate in a contract that the contractor shall: (a) comply with the provisions of this Policy; and (b) allow BEETELLER access to data and information about the services provided.

## D. LIQUIDITY RISK

### 1. Scope

The following are considered Liquidity Risk events:

- The inability to efficiently honor expected and unexpected current and future obligations without affecting the daily operations of BEETELLER and without incurring significant losses;
- The inability to convert electronic currency into physical or scriptural currency at the time of the user's request.

Liquidity Risk can be classified as:

- **Mismatch Risk:** the possibility that differences between the maturity structures of assets and liabilities generate a cash mismatch. This would lead to an inability to honor its payments and, by the nature of the business, this risk is mainly related to the inability to honor the resources used by clients.
- **Financing Risk:** the possibility that BEETELLER may be unable to meet its obligations arising from an inability to sell assets or to finance itself;
- **Contingency Risk:** the possibility of not having adequate options for obtaining liquidity as a consequence of an external event that implies greater financing needs.

### 2. Prevention, identification and treatment of Liquidity Risks

For the prevention, identification and treatment of Operational Risks, BEETELLER:

- It will define the guidelines to be observed in the design and maintenance of the activities under the management of the Risk area;
- It will define criteria and instructions for the effective liquidity management of the payment arrangements set up by BEETELLER;
- It will define liquidity model with criticality parameters.
- It will disclose its liquidity risk management structure in a report with public access, at least annually. The Senior Management must state in the public access report its responsibility for the information disclosed, also indicating the address for public access to the liquidity risk management structure report.

The Risk Management Structure must also foresee for Liquidity Risks: (a) processes to identify, evaluate, monitor and control exposure to liquidity risk in different time horizons, including intraday; and (b) a liquidity contingency plan that establishes responsibilities and procedures to deal with liquidity stress situations.

BEETELLER undertakes, to maintain the value of the reference equity in accordance with the regulatory requirements defined by the Central Bank of Brazil.

## E. RISK TRANSACTION RATING MATRIX

Every problem identified through the instruments described in the previous steps requires analysis and definition of action plans, aiming at improving the processes and maintaining the risk levels within acceptable exposure levels according to the RAS defined by BEETELLER.

- **Definition of the RAS:** the RAS will be defined and approved according to the responsibilities of the Risk Framework. BEETELLER's internal procedure will describe the process regarding the construction and monitoring of the operational risk boundary.
- **Mapping of the activities' risks and controls:** BEETELLER will determine its Risk Matrix, with the purpose of identifying the risks associated to the processes/activities, classifying them as to probability and impact, their consequences and used controls. Its application has the objective of providing an integral vision of the process flow, its dependencies and interactions.

## F. RISK MONITORING

The *Compliance*, Risk, and Internal Audit Officers, if applicable, are responsible for monitoring the processes and informing top management of risks and occurrences of failures in internal processes.

Part of the monitoring process is to conduct verification and review tests for compliance with policies, procedures, and compliances. All systems, processes, operations, functions and activities within BEETELLER are subject to future review.

## G. CONTINGENCY AND BUSINESS CONTINUITY MANAGEMENT

In order to ensure the objectives of this Policy, BEETELLER shall develop specific policies and procedures for the treatment of contingencies and business continuity management, observing the following guidelines:

- The effectiveness of the implementation of the plan, policies, and procedures for contingency management and business continuity, following the roles and responsibilities of the Risk Framework;

- The proper handling of crisis management, operational continuity, and disaster recovery;
- The assurance of resources, human and material, for the implementation of the business continuity management plan, policies and procedures;
- Organizational stability at an adequate level during recovery after the unavailability of critical processes and services;
- The appropriate, coordinated and timely response in crisis situations;
- Ensure the validation of contingency environments and procedures through periodic testing.
- Procedures to be followed in case of relevant incidents related to the cyber environment and the interruption of the relevant contracted data processing and storage and cloud computing services will be elaborated, covering hypotheses that consider the replacement of the contracted company and the reestablishment of the institution's normal operation;
- Incident scenarios will be developed to be considered in the continuity testing of payment services provided;
- Deadlines will be stipulated for resumption or normalization of the interrupted relevant activities or services;
- Procedures will be developed for risk management with regard to business continuity, timely communication to the Bacen of the occurrences of relevant incidents and interruptions of relevant services, which constitute a crisis situation by the payment institution, as well as the arrangements for resuming activities;
- Internal audit processes of the monitoring and control mechanisms of the cyber security policy will be developed.

## H. TROUBLESHOOTING PROCEDURES

Fault correction procedures should address:

- **Identification of Operational Losses:** the determination of the loss arising from Incidents is an important factor for compliance with the requirements of regulatory agencies, besides providing BEETELLER with consistent, standardized and updated information, decisive for a quantitative analysis of risk management at BEETELLER.
- **Evaluation of the Quality of Controls:** the evaluation of controls has the objective of evaluating the effectiveness/efficiency of controls, in order to verify if they are being executed as described in the risk matrices and internal policies.
- **Training Plan:** the training plan aims, by means of simulations of Incidents and evaluation of Incidents that have occurred, to ensure that the Collaborators are prepared to deal with Incidents and able to identify situations of risks and vulnerabilities.

## I. THE PARTICIPATION IN THE OPEN FINANCE.

BEETELLER, participating in Open Banking, will meet the requirements for sharing of payment transaction initiation, when requested by customers, observing the rules imposed for the proper sharing of data from the consent, authentication and confirmation stages.

The entire process will occur with security, agility, precision, and convenience to be performed through the dedicated interface, carried out exclusively through electronic channels, in a successive and uninterrupted manner, and with a duration compatible with its objectives and level of complexity.

BEETELLER shall ensure that its policies for risk management, as well as this Operational Risk Policy, provide for business continuity:

- the procedures to be followed in case of unavailability of the interfaces used for sharing;
- the deadline for restarting or normalizing the availability of the interface;
- the handling of incidents related to data security breach related to sharing and the measures taken for their prevention and resolution; and
- the execution of business continuity tests, considering the unavailability scenarios of the interfaces and the evaluation of their results.

BEETELLER is responsible for the reliability, integrity, availability, security and confidentiality in relation to the sharing of data and services in which it is involved, as well as for compliance with the laws and regulations in force.

BEETELLER, prior to data sharing by Open Banking, shall:

- identify the client and obtain his or her consent through clear, objective and appropriate language;
- inform the determined purposes;
- have a validity period compatible with the determined purposes, limited to twelve months;
- discriminate the data transmitting institution or account holder, as the case may be;
- discriminate the data or services that will be the object of sharing, observing the option of grouping the data;
- include the customer's identification.

It is forbidden for BEETELLER to obtain the customer's consent by means of an adhesion contract, a form with an option for acceptance previously filled out, or in a presumed way, without active manifestation by the customer. In the case of successive payment transactions, the

client, at its discretion, may set a longer term than that established, and may condition the validity of the consent to the closing of said transactions.

BEETELLER is forbidden in ITP activities:

- store the set of data related to its Customers' credentials to authenticate the payment transaction before the institution holding the account, except when the services are provided to institutions authorized to operate by the Central Bank of Brazil, based on a contractual relationship, related to:
  - (i) Money Laundering and Terrorist Financing Prevention Policy;
  - (ii) the Cybersecurity Policy; (iii) and the Open Banking System;
- require from its Customers any data other than that necessary to provide the payment transaction initiation service;
- use, store or access the data for a purpose other than the provision of the payment transaction initiation service expressly requested by clients, except when the services are provided to institutions authorized to operate by the Central Bank of Brazil, based on a contractual relationship, relating to: (i) the Money Laundering and Terrorist Financing Prevention Policy; (ii) the Cybersecurity Policy; (iii) and the Open Financial System (Open Banking);
- change the amount or any other element of the payment transaction authorized by Customers; and
- initiate a payment transaction involving a payment account held by an institution that is not a member of the Brazilian Payment System.

## **J. APPLICATION OF FUNDS HELD IN PAYMENT ACCOUNTS**

BEETELLER shall maintain liquid funds corresponding to the balances of e-currencies held in payment accounts, plus the balances of e-currencies in transit between payment accounts at the same institution; and amounts received by the institution for credit to a payment account, as long as they are not made available for free handling by the end user of the receiving payment account.

When BEETELLER has access to the Reserve Transfer System (STR) of the Bacen, by the end of the hours established for the STR to operate, the funds calculated must be allocated in cash, by credit transfer to a specific account at the Bacen; or federal government bonds, registered in the Special System for Settlement and Custody (Selic), including by means of repo operations.

When BEETELLER does not have access to the Reserve Transfer System (STR) of the Bacen, the calculated funds must be held in custody in a current account, in the name of BEETELLER, in a first line bank, segregated from its own funds; or federal government bonds, registered in the Special System for Settlement and Custody (Selic), including by means of repo operations.

BEETELLER shall follow the Bacen rules that provide for the custody and investment of funds held in a payment account.

## **K. FINAL TERMS**

Compliance with this Policy is the duty of all Collaborators. In addition, this Policy contains the model of the Adhesion Term to the Risk Management Policy and Adhesion Term to the Changes in the Risk Management Policy, which must be signed by all Employees whose activities are somehow linked to the practices and procedures established in this Policy.

This Policy will be approved by BEETELLER's Board of Directors and Senior Management, and properly documented and submitted to periodic reviews, with the documentation kept at the disposal of the Bacen.

This Policy is available in a place accessible to all Employees, in clear and accessible language. It can be accessed at <https://beeteller.bitrix24.com.br/docs/path/>.

|   |  |
|---|--|
| <b>Author</b>   | Barcellos & Tucunduva Advogados  |
| <b>Approved by:</b><br>Lauriney Leite dos Santos<br>Financial Director              | <i>Lauriney L. Santos</i><br><a href="#">Lauriney L. Santos (15 de Dezembro de 2022 13:07 GMT-3)</a>         |
| <b>Approved by:</b><br>Kelly Viviane da Silva<br>Compliance & Risk Director         | <i>Kelly Viviane da Silva</i><br><a href="#">Kelly Viviane da Silva (15 de Dezembro de 2022 13:13 GMT-3)</a> |
| <b>Approved by:</b><br>Caio Souza Vidal de<br>Negreiros<br>Chief Technology Officer | <i>Caio S. Vidal</i><br><a href="#">Caio S. Vidal (15 de Dezembro de 2022 15:26 GMT-3)</a>                   |



---

**ANNEX I****TERM OF ADHESION TO THE RISK MANAGEMENT POLICY**

I, \_\_\_\_\_ registered in the CPF under n. \_\_\_\_\_ declare that I am aware of this Risk Management Policy, as well as of the guidelines contained in the other policies, norms and internal procedures of BEETELLER.

I also declare that I am aware that, in case of a risk mentioned in this Policy, I must immediately communicate it to the responsible area by means of the e-mail [tesouraria@beeteller.com](mailto:tesouraria@beeteller.com)

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_

Date

\_\_\_\_\_

Signature

## ANNEX II

**TERM OF ADHESION TO THE ALTERATIONS OF THE POLICY OF  
MANAGEMENT OF  
RISKS**

I, \_\_\_\_\_ registered in the CPF under n. \_\_\_\_\_ declare that I am aware of the changes in the Risk Management Policy, as well as of the guidelines contained in the other policies, rules and internal procedures of BEETELLER.

I also declare that I am aware that, in case of a risk mentioned in this Policy, I must immediately communicate it to the responsible area by means of the e-mail [tesouraria@beeteller.com](mailto:tesouraria@beeteller.com)

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_

Date

\_\_\_\_\_

Signature