

## 1. Purpose

Establish general guidelines for the hiring, use, and access to banking platforms.

## 2. Scope

This policy applies to those responsible for the Administration and Finance Areas of Grupo Bimbo who either perform treasury operations or consult information within banking platforms.

## 3. Definitions

**Banking platform:** Online and mobile bank access

**Administrator or master user:** Person responsible of ensuring the correct segregation of duties and limiting the operational users, as well as assuring the correct allocation of products and services; such position will be granted to the highest-ranking associate in the Administration and Finance Area of the Subsidiary.

**Authorizing user:** Person who has the joint capacity to validate, approve or reject payment, which was previously entered by the operating user. Must ensure correct delivery process to release payment according to the instructions received.

**Operating user:** Person responsible to capture, within bank platforms, generate payment, either massive or individual, according to the information received in the payment request. Validate all data to submit for approval.

**Consulting user:** Person with query online access only to generate reports and consult online the information available in the banking platform. Normally all the types of users have assigned for default the consulting modules. **The consulting users do not have access to edit or make operations within the banking platforms.**

**Payment disbursement:** Monitor cash outflow in bank platform, either in local or foreign currency, to suppliers, payroll, government tax payments, bank fees, among others.

## 4. Responsibilities

**Global Treasury Department:** regulate the hiring, administration, and use of the banking platforms. Perform the treasury services explicitly defined in the service contracts between the Global Cash Management Department and the applicable subsidiaries of Grupo Bimbo.

**Administration and Finance Areas of the subsidiaries:** Ensures compliance with this policy, as well as the procedures deriving from it, in its management area.

**Banking platform users:** Guarantee the adequate use of their assigned responsibilities according to the capacities assigned by this policy.

## 5. General guidelines



In order to guarantee the provisions of the ***FGB-TR-01 Global Treasury Policy*** regarding the proper contracting and use of the bank platforms, to carry out treasury operations, it is essential to comply with the following guidelines:

### Generalities

Any approval through the bank platform, either as an administrator or authorizing user, must be done in a jointly manner; this includes but not limited to:

- Creation, modification and user inactivation
- Third party account registration
- Grant access to user based on responsibilities
- Assign limit amount per operation
- Any type of payment issued to a third party

### Administration and Finance Areas of the Subsidiaries:

- The highest-ranking associate in this area must:
  - Design an optimal authorized user structure that guarantees business continuity and the adequate segregation of duties
  - Assign access to the different banking platforms, exclusively to associates hired by the firm, for an indefinite period and based on their position
  - Keep the user log updated as changes in responsibilities occur
  - Keep, for at least 5 years, all monthly activities carried out by the users in all different bank platforms
  - In conjunction with the Treasury responsible, create a contingency plan that allows to continue all treasury operations with the highest risk, as well as an action plan that guarantees the safety and continuity of the business from any fraud attempt
  - Prioritize electronic payments over paper check
  - Hire the check protection service in case checks are utilized
  - Preserve personally or through the Treasury responsible, all banking device delivery formats and key assignments ( **FGB-TR-08 Appendix I.pdf**) signed by the users
  - Generate and keep a catalogue of all users with the capacity to request registration of third accounts and payments; a limit amount per operation must be established as a function of the associate's position. The catalogue must be authorized by the highest-ranking associate in the Subsidiary
  - Monitor that:
    - Every user, regardless of the assigned profile, physically signs the banking device delivery format and key assignments ( **FGB-TR-08 Appendix I.pdf**).
    - Under no circumstances the users have more than one profile (administrator, authorizer, operator) within the banking platforms.
    - The requests of third-party bank account registrations are confirmed via callback.
    - The update (modification or elimination) of the third-party accounts is done at least annually.
- Prior to hiring banking products and services, this area must:
  - Provide a detailed analysis that considers the security, costs, and functionality between the financial entities.
  - Validate the contract with the person responsible from the Legal Department, even when addressing a framework or standard contract.
  - Request the IT responsible to value the product so that, in case it is considered safe, the use of the different banking platforms can be facilitated.

### Administrator or master user

The associate that has this capacity must:

- Generate and hand in, to the highest-ranking associate of the Administration and Finance Area of the Subsidiary, a monthly record keeping of the activities carried out by the users in the different banking platforms.
- Require, in the case of registering third party bank accounts, the jointly authorized request and the appropriate documentation validating the authenticity of the accounts (bank statement, certification or letter issued by the banking institution).

- Confirm, via callback, any request to register third party bank accounts, discarding any contact's phone number within an email.
- Keep a record log, per bank, of all the registrations in the banking platform, which must be sent to the highest-ranking associate of the Administration and Finance Area of the Subsidiary on a monthly basis.
- Update (modification or elimination) the third-party accounts, at least annually.

## Users

The guarding and protection of the access keys (passwords) are sole responsibility of the user which they were given to and must not be shared under any circumstance.

## Disclaimer

Anything not provided for in this policy must be consulted and, where appropriate, approved by the Global Treasury Department.

## Non-compliance and Sanctions

The Global Administration & Finance Department shall be responsible for dictating, in conjunction with any other relevant authority, the disciplinary measures (as established in Grupo Bimbo's regulatory framework) that will correspond to any infringement to the scope of this policy. These measures must be applied by management and shall be executed without prejudice to the corresponding legal, administrative or civil procedures.

## 6. Responsibility / Ownership

The Global Treasury Department is the assigned owner of this policy and is primarily responsible for its contents, updating, and presentation for approval to the Global Internal Control and Risk Management Department, Steering Committee and CEO.

## 7. Updates

The changes implemented in between versions are described below:

Revision / History of the revision				
Version	Revision Date	Update by:	Approved for:	Main Changes
1	June, 2020	Juan Guillermo Gonzalez Alanis	Maria José Porrero	
2	December, 2022	Sonia Perez Pineda	Maria José Porrero	The "Non-compliance and Sanctions" section was added.