## 1. Purpose

Establish general guidelines for the Management of Identity and Access for all personnel who have access to Grupo Bimbo information systems. To preserve the confidentiality, integrity and availability of the Information stored and processed by a Grupo Bimbo information system.

## 2. Scope

This policy applies to users of the different Grupo Bimbo Departments, Areas, Business Units and subsidiaries, that have direct or indirect responsibilities for Identity Management in any of Grupo Bimbo's information systems.

## 3. Definitions

**Application:** Computer system that manages or supports a business process that provides functionality or service to users.

**Digital identity:** The information about a person or user, that makes up the description of their digital identity within the organization.

**Generic account:** The account used by a group of people or an automated process to carry out an activity within an application, but that does not specifically identify a person.

**Global Identity Directory:** The information system that stores, organizes and keeps updated digital identities, as well as access and permissions to information systems. It constitutes the only source of digital identities in the company.

**Global Unique Identifier:** The attribute of the digital identity that uniquely identifies a user in the global identity directory. It is immutable and remains active throughout a user's work life cycle. Normally it is generated from source systems.

**Identity and Access Management Committee:** It is integrated with the Board of Directors, has representation from the following Global Departments: Transformation, Comptrollership, Internal Audit, Internal Control, People, Finance and Systems.

**Identity Management:** Set of processes to create, modify and / or deactivate digital identities, with access to company electronic resources and applications.

**Information systems:** Applications, services, information technology assets or any other component that stores and processes company information.

**Source systems:** The Source system is considered the authorized source of data where joiner, mover and leaver data are stored and managed. It is also considered the data source for all information that constitutes the persons digital identity.

**User accounts:** Accounts with associated permissions and privileges to access or change data, process transactions, create or change configurations, etc. within information systems.

**Users:** all associates, consultants, personnel with temporary assignments, and any person who maintains any type of direct or indirect employment relationship with Grupo Bimbo (or any of its subsidiaries), and who has access to the company's information systems.

## 4. Responsibilities

**Roles and Access Manager:** Maintain the consistency of identities and accesses for all joiners, movers and leavers in relation to the operating model of Grupo Bimbo. Ensure that access to information systems is granted in accordance with the role assignment rules defined by the business.

**Application manager:** Apply user registrations, deletions and changes to applications that are not integrated with the global identity directory. Ensure the continuity and availability of an application through support management and monitoring its operation and maintenance. The minimum hierarchical level to be designated for this role is supervisor and must correspond to an internal associate assigned within Information and Business Applications Department.

**Global Identity Directory Administrator:** Ensure the correct operation of the global identity directory, as well as the execution of access provisioning (granting, changing and revoking), and the collection of information on access identities and their accesses.

**Global Systems Department:** Provide the technical elements needed to enable and maintain the information systems required for Identity and Access Management.

**Identity and Access Management Committee:** Review this policy and its annexes annually, or whenever significant changes occur that impact its suitability, adequacy and validity of the requirements and performance indicators of this policy. Ensure the continued effectiveness of the identity management processes and accesses controlled by the identity management processes. This Committee must meet at least once every quarter and will be convened through the Internal Control and Risk Management Global Department.

**Global People (Human Resources – HR) Department:** Ensure the completeness, accuracy and validity of the information stored in the source systems, that sends information to the destination systems.

**Global, Corporate, Business Unit, Functional and Area Vice-Presidents:** Ensure compliance and adoption of this policy within their area of responsibility.

**Process owner:** Ensure the correct functioning of the identity management process in the system or application for which they were designated as the owner. This role must be assigned to an internal associate.

## 5. General Guidelines

In order to preserve the confidentiality, integrity and availability of information, Grupo Bimbo requires those personnel who have direct or indirect responsibilities for identity management in any of Grupo Bimbo's information systems – to comply with the following guidelines:

- Identity and access management functions must be executed through the processes and standards that the global directory of identities has established for management of access identities.
- All Grupo Bimbo applications and information systems require an owner in accordance with the provisions of the Applications and Systems Ownership Standard.
- Given the confidentiality of digital identity information, access to the IAM system must be specifically authorized by the Global People (Human Resources – HR) Department, and access granted by the roles determined by the access manager.

### Creation

- The digital identity must be unique across the entire Grupo Bimbo organization, and be created exclusively for users who:
  - Have a direct or surrogate employment relationship with Grupo Bimbo or one of the GB

subsidiaries.
  - Have a globally unique identifier aligned with the Data Quality Standard established by the identity and access management governance model.
  - Have an operational and / or functional manager assigned within the source systems.
- The creation of a digital identity must comply with the specifications established in the Data Quality Standard defined as part of the governance model.
- Each digital identity may have multiple user accounts in the different systems and applications assigned through a business rule.
- Generic and automated process accounts (e.g., robots) that require a generic description digital identity, but these accounts must have an assigned responsible owner.

### Changes

- The administrator of the corresponding source system must immediately update the information of users' digital identity, when the Global People (Human Resources - HR) Department informs them of any change in the associate's labor or employment data within the organization. This may include; users employment status, assignment to a new legal entity, organization, or business unit, etc.
- The operational and / or functional manager must:
  - Approve or reject the changes to the attributes of the digital identity that correspond to their associate (e.g., change of boss, change of legal entity, organization, business unit, workplace, etc.)
  - In regard with user recertification of access process, the changes made must align with the provisions of the ***FGB-IC-04 Role Management Global Policy***.

### Digital identity deactivation

- It is prohibited for anybody in Grupo Bimbo (or any GB subsidiary), to delete a digital identity.
- The status or a person's digital identity must set to be deactivated when an associate terminates the employment relationship or suspends temporarily employment with Grupo Bimbo (or any GB subsidiary). The user account must be kept as registered in the global identity directory.
- Once the associate has been removed from the personnel source system, the deactivation of the digital identity must be applied through the global Identities directory.
- When the digital identity has associated generic identities, they must be reassigned to a different digital identity before deactivation.

### Protection and privacy of Digital Identity Information

To maintain the confidentiality of the information of the digital identities and give them appropriate protections, all users must comply with the provisions of the ***GGB-010 Global Policy for the Use of Information Assets*** and the ***FGB-CP-01 Global Policy for the Protection of Personal Information***.

## 6. Responsibility / Ownership

The Global Internal Control and Risk Management Department is the assigned owner of this policy and is primarily responsible for its contents, updating, monitoring of its compliance and submission for approval before the Steering Committee and CEO.

## 7. Updates

The changes implemented in between versions are described below:

| Revision / History of the revision | | | | |
|---|---|---|---|---|
| **Version** | **Revision Date** | **Updated by** | **Approved by** | **Main Changes** |

| | | | | |
|---|---|---|---|---|
| **1** | September 2020 | Ricardo César Chávez Cruz **Global Internal Control and Risk Management Department** | Gabriela López Juárez **Global Internal Control and Risk Management Department** | |