1. Purpose

Establish general guidelines for access to Grupo Bimbo's information systems.

2. Scope

This applies to associates of the different Grupo Bimbo Departments, Areas, Business Units and subsidiaries that have direct or indirect responsibilities for managing access to any of Grupo Bimbo's (or GB subsidiary)information systems.

3. Definitions

Access account: Generic way to call all privileged account types specific, within information systems, that support business operations.

Access requirement: Formal request, generated at the service desk, for the attention of high (creation of an access account and assignment of privileges), low (inactivation of an account of access or privileges) and change (assignment or removal of privileges) within a system of information authorized by the Global Systems Directorate.

Assignment by exception: Granting accounts and privileges, to a collaborator, that are not included in the job role assigned by your management.

Authoritative source: Information system, defined by the Global People Directorate, as single source of data for all the information that constitutes the digital identity of the Collaborators. Manage the additions, cancellations, and changes of the life cycle of the collaborator in Grupo Bimbo.

Digital identity: Relevant employment information of an employee that includes the unique identifier global.

Global Key Approver: Functional expert of a business process, implemented in some(s) of Grupo Bimbo's information systems, appointed by the Global Functional Director.

Global Identity Directory: Information system that consolidates, organizes, and maintains updated all the digital identities of the collaborators, as well as their work attributes that come from the authoritative sources of the Directorate of People. It also stores the access and privileges of Grupo Bimbo's information systems.

Global Systems Management: Generic name assigned to encompass the different areas that manage technology and information in Grupo Bimbo.

Generic account: It is the one used by a group of people, to carry out an activity within an information system, but which does not specifically identify a user or person.

Global unique identifier: It is the attribute of the digital identity that uniquely identifies a user in the global identity directory. It is immutable and remains active throughout the cycle of working life of a collaborator and is generated from the authoritative source.

High privileges: Permissions granted to an access account, in information systems, including, but not limited to, those for creating or modifying master data, integrations, business rules, etc.

Immediate Cancellation Event: Disabling, with high-priority, access, and privileges where users' activities that compromise Grupo Bimbo's Information Security, in the event that he terminates his contractual relationship or initiates fraudulent activities against Grupo Bimbo, and its subsidiaries.

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

Least privilege: That designed by the functional areas and that is granted to users to fulfill, exclusively, with the assignments of their position.

Named account: That used, by an automated system or process (e.g. robot), to carry out an activity within an information system.

Privileges: Permissions granted to an access account, in information systems, including, but not limited to, those to access, process business and operate day to day, according to their job functions.

Role: Functions attributed to a user so that, in certain situations or circumstances, operate according to a set of privileges granted to you.

Service desk: Entity in charge of providing, to the end users, service of attention to Incidents and system access requirements.

User: Collaborators, consultants, staff with temporary assignments and any person who maintains any type of direct or indirect employment relationship with Grupo Bimbo (or its subsidiaries) and that access Grupo Bimbo's information systems.

4. Responsibilities

Information System Administrator: Enable or revoke system access privilege requested by an authorized user, where the appropriate approvals required in the access management procedure for Grupo Bimbo's information systems and Subsidiaries.

Global Internal Control and Risk Management Department: Generate and monitor Recertification campaigns, on access, user privileges and their assignment rules of the Organization. Report the results to those involved, via email and at least one once a year.

Global Systems Management: Fulfill and enforce the responsibilities established herein. Manage privilege catalogs used for access requirements. Conserve, in the service desk, records of access requirements and exceptions to this policy. Assure the functionality, continuity, availability, and integrity of information within the global directory of identities. Ensure that information systems, which are part of the portfolio of projects, are evaluated to define whether they should be integrated into the global identity directory. Execute integrations to the Global Identity Directory. Ensure compliance with the information security requirements, in the Global Directory of Identities and all its systems of integrated information. Organizational, Functional and Area Directors: Ensure the implementation of this policy within its scope of responsibility.

Global Key Approver: Design the roles and privileges for each of the activities that are they run within the information systems that support their business functions. Participate in the approval of granting and revocation of access requests, as long as they are valid and appropriate.

Direct Boss: Establish the accesses and privileges, which their collaborators must have within the information systems, to support your business functions. Approve and / or process, according to the in this case, requests for access at the service desk. In each recertification campaign, verify the validity of the accesses and privileges of its collaborators and, in case of detecting any nullity, request cancellations, through an access requirement.

User: Use of the application accesses and privileges they have been granted only to perform their assigned job functions.

5. General Guidelines

In order to promote reliable and secure access to the company's information systems, it is the policy of the Grupo Bimbo to comply with the guidelines established in this policy.

User accounts activation

- The access requirements to the information systems of Grupo Bimbo must:
  - Be requested, exclusively, through the help desk, defined by the Global System Directory.
  - Be provided based on legitimate business needs and authorized by the direct boss, under the concept of the least privilege.
  - Be assigned, through the global directory of identities or, manually, always and when the user presents the authorization of his direct manager and the key approver.
  - For external personnel, have a maximum validity of six months or the duration of their service contract, whichever is less.

- The creation of accounts must:
  - Have the globally unique identifier associated, which allows the collaborator to be fully located and make you responsible for the access that has been granted.
  - Be assigned at least one privilege, otherwise Global Systems Management you will need to inactivate the accounts.

- Under no circumstance:
  - Access accounts may be loaned, reused, or duplicated.
  - Generic accounts will be allowed.

- The direct manager can authorize:
  - Access assignments and privileges.
  - Allowances by exception, whose validity must not exceed six months

- For those information systems not integrated into the global identity directory, the information System Administrator must perform the assignment of the access account manually.

- Any collaborator of Grupo Bimbo who requests an access account, for personal external, you will need to provide the name and contact information of the third party and will be Co-responsible for the administration and use of the account.

User accounts deactivation

- The administrator of those information systems not integrated into the global directory of Identities must manually disable access, within 24 hours, to from the occurrence of the termination of work or temporary suspension of functions of the collaborator
- The Global Systems Directory must:
  - Disable the accesses and privileges associated with an account that, for a period of time more than 90 days, have not been used.
  - Backup and safeguard, for a period not exceeding 2 months, the email mailbox and information contained in the computer equipment of a deactivated account, in order to recover that data if necessary.
  - In the event of immediate cancellation, manage the disabling of access and privileges through a requirement prepared by Cybersecurity, Directorate of Patrimonial Security or the direct head of the user, addressed to the Global Systems Management.

Named accounts

- The user responsible for these accounts must make his request, through an access requirement, approved by the predefined responsible.
- The Global Systems Management must ensure that the registration of this type of accounts:
  - It is carried out, as long as it is impossible to assign an access to a collaborator in particular.
  - Are associated with a globally unique identifier of the applicant.
  - Do not contain high privileges.
- Global Functional Directors, through the access certification process and privileges, must validate the use of these accounts, according to the business need.
- For those accounts that are no longer required, the account owner must request, by means of a request for access to the service desk, its disqualification and that of the privileges associated with it.
- In the event that the person responsible for the named account changes departments or terminates his employment relationship with Grupo Bimbo, the Global Systems Management must assign the account to a new active manager within the company.

6. Responsibility / Ownership

The Global Systems 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 Internal Control and Risk Management Department, 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	April 27, 2020	Ricardo Chávez	IAM Committee	Alignment with IAM Governance model.
2	September 23, 2020	Ricardo César Chávez Cruz	Gabriela López Juárez	• Update of "Purpose" • The scope of the policy is modified to the access management of any information system of Grupo Bimbo or its subsidiaries. • The definitions of "Application", "Assignment by exception", • "Information Technology Committee", "Global Identity Directory", "Minimum privilege" and "Role" are added. • The definition of "User accounts" is modified. • The term of "Access privileges" is changed to "Privileges". • The responsibilities of • "Information Technology Committee" and "Global Information and Transformation Department" are added. • The responsibility of "Operational and/or functional manager" is complemented with every six-month reviewing and approving the access of the applications. • In the sections "User accounts activation", "User accounts deactivation", "Access privileges", "Generic accounts activation" and "Generic • accounts deactivation" have new activities.
3	April 29th, 2021	Maria Fernanda Cruz	Ricardo Chavez Cruz	• The responsibility of the support area is modified in the "User accounts deactivation" section.
4	March 2023	Miriam Morales Hernández	Ricardo Chávez Cruz	• Changes in definitions, changes in Responsibilities and updating of General guidelines.
5	June 2023	Miguel Ángel López Cortez	Alejandro Cuevas Gallegos	• Changes in definitions and changes in responsibilities