1. Purpose

Establish the general guidelines for security and protection of Grupo Bimbo information, according to its importance and life cycle.

2. Scope

This policy applies to associates and temporary staff, performing functions from Business Technology Department (BT), Local Personnel or Legal areas, as well as to any person, including third parties, who maintains any type of relationship with Grupo Bimbo S.A.B. de C.V. and/or any of its affiliates.

3. Definitions

Confidentiality agreement: Unilateral or mutual contract, through which, one or both parts are compromised to not share with third parties' information listed as confidential.

Confidentiality: A security principle that requires that the data must be only accessed by authorized people.

4. Responsibilities

Global Information Security Management: Implement and maintain an information security program with all associates and third parties, that guards and protects the information of the company, as well as the confidentiality, integrity, and availability of data. Establish the categories to classify the information. Oversee that all systems ensure compliance with company access requirements.

The administrator of IT systems: Implement the access controls to the IT systems, according to the security and classification of information requirements that the Global Information Security Management group defines.

Global key approver: Identify the risks and define the necessary control to guarantee the segregation of functions within its scope of responsibility. Comply with the segregation of functions model at a global level and approve the changes to that model.

IT Committee: Determine the existence of and evaluate any violation of information security policy or inappropriate access. In this case, communicate and apply established company disciplinary actions to associates or third parties that have violated the policy.

Global Direction and local IT Personnel Departments: Establish the procedures to ensure that the associates know and sign the established policies of the company for the information security. Recollect and manage the candidate information according to the existing laws in the corresponding jurisdiction.

Local legal areas and Compliance champions: Comply with the guidelines of this policy.

5. General guidelines

In order to ensure the confidentiality, integrity, and availability of Grupo Bimbo information, it all GB, and subsidiary and affiliate personnel must comply with the following guidelines:

Relationship with associates and third parties

- Personnel functions (HR) of all Business Units must ensure that all Grupo Bimbo associates, at the time of starting work for the company, comply with the following:
  - Agree to and Sign off the ***GGB-001 Grupo Bimbo Code of Ethics*** and global general policies.

- Agree to and Sign off the policies about information security, before having access to confidential information or information systems.

- Compliance champions for each GB subsidiary and affiliate must complete background checks of company associates and IT service providers, in accordance with the ***FGB-IT-12 Global Policy of IT Business Partners Management***, in order to identify alerting behavior or signaling about corruption topics and/or lack of integrity that could lead to risks for the company.
- All associates must adhere to the information retention and destruction protocols established in the ***FGB-CP-03 Global Retention and Destruction of Information Policy.***

IT security awareness

The Global Information Security Department must:

- Give training regarding the policies and procedures governing Grupo Bimbo information, to all associates and third parties, at least once a year.
- Define, together with the Global Personnel Department, the methods of participating in Security awareness campaigns, such as classroom, distance learning, website, GB Talent, etc.
- Execute the awareness program regarding information security at least once a year. And ensure that the new entry associates and third-party personnel, complete the required training within 3 months after their company start date.

Job termination or job change

- The local legal areas must ensure that the contracts with associates and third parties have the responsibilities and duties after the termination of the contractual relationship, including nondisclosure of the information, which they had access to.
- The administrator of IT systems must activate or deactivate the access of the associates, according to the request received through the IT Works and in adherence to the ***FGB-IT-22 Access Management Global Policy.***

6. Responsibility / Ownership

The GB Global IT Governance 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 Global 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	Apr 2020	Maria Fernanda Cruz	Alejandro Cuevas Gallegos	N/A
2	**Jul 2023**	**Miguel Ángel López Cortez**	**Alejandro Cuevas Gallegos**	• **"Scope" Updated** • **Changes in the General Guidelines section, responsibility is added in "Relationship with associates and third parties"**