1. Purpose

Establish general guidelines for the management of all Information assets of the company, the actions required in case of damage, theft and/or loss of company information assets, and to regulate the access to information, the integrity of company data, and the availability of data for company operations.

2. Scope

This policy applies to all associates, consultants, personnel with temporary assignments and to anyone maintaining any sort of working relationship with Grupo Bimbo, S.A. de C.V.B. and/or any of its affiliates ("Grupo Bimbo or the company") in contact with information assets of the company.

3. Definitions

End user: Grupo Bimbo associate who has been assigned an information asset for the performance of his daily activities.

Information asset: It is the information and/or related components valuable to the organization and therefore in need of protection. Information assets may include: intangible information assets (information contained in servers and data bases, electronic documentation, etc.), tangible information (physical documentation), software assets (business applications, commercial programs), fixed IT assets (computers and telecommunication assets, magnetic media, other technical equipment), IT services (computational services and communication, applications and services that support IT equipment).

IT Works: Computer system to register and follow the requirements or incidents of the end user from different apps.

On-site Support: Initial contact to attend the end user requirements or incidents, through IT responsibles in the Business Units and localities.

Third parties: People outside the company that work in the facilities and/or have access to the information assets of Grupo Bimbo.

4. Responsibilities

Associate: Is the primary responsible of appropriately using the assets and information technology according to what is established in this policy.

Global People Department: Manage high, low and changes of associates and inform these to the IT management and financial control.

Global Security and Protection Department: Consolidate acts of theft of information assets.

Business Unit Presidents and Functional VPs: To promote and ensure the adoption of this policy.

Global IT Management and Financial Control Area: Consolidate information of the information assets inventory, for the financial control, budget and supplier's payment.

Global IT Governance Area: Issue, communicate and update the present policy, as well as any other normativity from the Global Information and Digital Transformation Department.

Global IT Security Area: Guarantee the security of the information located in the information assets of the company, through design, implementation, management, operation and replace the security controls, as well as establish standards and operative procedures to limit the access of removable devices.

Local IT Area: Validate the service suppliers manage through the on-site support, the information assets inventory, delivery and seizure, as well as generating and safekeeping the responsive letters about those assets. Establish, together with on-site support, the execution procedures in case of damage, theft and/or loss, as well as the information asset replacement.

Direct manager: In case of low or change from any of his associates, recover the information assets that were assigned and deliver for safekeeping to the on-site support area.

5. General guidelines

Management

- The direct manager and each local IT management must comply with the following guidelines:
  - The acquisition of information assets will be subject to the ***FGB-IT-02 Global Policy of Development and Acquisition of Information Technology (IT) Goods & Services.***
  - Ensure the information assets are assigned to associates from the Business Unit or legal entity that acquired them and that these remain in the same, until the functional life cycle ends.
  - Refrain from assigning information assets to third parties, company property.
- The direct manager must:
  - Ensure the assignation of the information assets is done according to the functions, responsibilities and activities assigned to the associates.
  - Deliver the information asset to the on-site support area in case the associate changes Business Unit and/or legal entity.
  - Refrain, in case of termination of labor relationship of any associate, to safekeeping the information assets of associates that leave their positions vacant.
- Each local IT area must:
  - Ensure the assignation of the information assets is done through IT Works.
  - Ensure that the associate, upon receiving the information asset, sign the correspondent responsive letter.

Theft

In case of theft of an information asset, the associate must:

- Deliver to the on-site support and security and protection areas, in a period of no more than 5 labor days, the theft report indicating serial number, model, brand and owning legal entity, issued by the competent authority for the crime investigation of the locality; in case of theft with violence this period could be more, without exceeding one year.
- Request through IT Works blocking the access to the information systems to recover the access according to the correspondent local procedure.

Loss and/or physical damage

- In case of losing an information asset, the associate must pay the equipment cost at current market value.
- In case of physical damage to the information asset, the associate will assume the reparation cost and must present to the on-site support area for the execution. Its forbidden that the associate repairs and/or buy pieces by himself.

Availability

To guarantee the availability of the information:

- The associates will be able to access or use Grupo Bimbo's information solely and exclusively to fulfill their assigned responsibilities.

- All the information stored in Grupo Bimbo's devices must be considered as property of the same and as such, accessible for the means that the company deems necessary.
- Personal use is permissible provided that it does not interfere with professional duties.

Confidentiality

In order to maintain the confidentiality of the information and to give it an appropriate use, it is Grupo Bimbo's policy that the associates:

- Will have to access the information assets only through company resources that have been previously assigned to them.
- Use of the application accesses and privileges they have been granted only to perform their assigned job functions.
- Must not to share their passwords, assigned for the use of company's systems.
- The consequences of what associates do with their user accounts are shared in co-responsibility with their operational and/or functional manager.
- Are to make use of the information assets in complete compliance to what is established in section "f) Confidentiality" of the ***GGB-001 Grupo Bimbo Code of Ethics*** and in the ***GGB-005 Global Policy on Confidential Information.***
- Must comply with what is established in reference to the handling of the information's privacy according to local regulations (e.g., laws of personal information protection in possession of third parties).
- Will not be allowed to perform activities, with computing equipment property of Grupo Bimbo, outside those related to the business, such as, activities of political character or affinity, fraudulent activities or dissemination of false or defamatory information.
- Will not attribute personal blog or social networks entries to Grupo Bimbo.
- Refrain to use connection ports for external storage devices (e.g., USB, memory cards or any other storage medium of present or future technologies).
- Share information through official company tools and only for purposes of interest to Grupo Bimbo, adhering at all times to this Policy, the ***GGB-001 Grupo Bimbo Code of Ethics,*** the ***GGB-004 Global Integrity Policy*** and the ***GGB-005 Global Policy on Confidential Information.***

Integrity

With the purpose of not compromising the integrity of information assets, Grupo Bimbo associates:

- Shall not use Grupo Bimbo's information assets for activities that are deemed illegal by local, state, federal or international laws or that endanger the information of the Company.
- Are forbidden to execute network monitoring activities without the consent of the Global Systems Department.
- Must take all prudent steps to maintain the consistency, accuracy and trustworthiness of Grupo Bimbo data over its entire life cycle.
- Must use institutional photographs that promote a professional image for the company, as part of their identity information.

6. Responsibility / Ownership

The Global Information and Digital Transformation Department is the assigned owner of this policy and main responsible for its content, update and monitoring of its compliance and the submission for approval to 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				
2	May 21, 2019	Global IT Department	Global IT Department	• Management of external storage devices.
3	Jan 28, 2020	Global IT Governance Management	Global IT Department	• Adjustment to purpose by including damage, theft and loss. • Adjustment to the definition of third parties and including IT Works, On-site support and end user. • Inclusion of Global HR Department, Global Security and Protection Department, Global IT Management and Financial Control, Global IT Governance Management, Global IT Security Management, Local IT Management and direct manager. • Sections “Administration”, “Theft”, “Loss or physical damage” are added. • In section “Availability”, the guideline about personal information storage is added. • In section “Confidentiality”, the guidelines about connection ports and sharing information are added.
4	Dec 20, 2021	Global IT Governance Management	Global IT Department	• Corporate image guidelines are added.