1. Purpose

Establish the general guidelines regarding retention, management and destruction of tangible and intangible relevant information of Grupo Bimbo.

2. Scope

This policy applies to the associates of all of Grupo Bimbo's companies in their various locations and functions, who produce or obtain, keep or destroy relevant information.

3. Definitions

Accessory information: Information that supports the documents that are subject to a retention period (e.g. supporting or background materials of transactions, correspondence, minutes, memos, proposals and analyses used to make a decision etc.). This type of information must follow the same rules of retention and destruction, as the document they support.

Destruction of information: Properly dispose of and discard information that, according to legal, fiscal, financial or operational regulations, is no longer useful or has any obligation to safeguard it.

Information: Set of ordered and processed data with the goal of providing knowledge or understanding of a process, decision or transaction in Grupo Bimbo.

Information for litigation, revisions or audits: Any information referring to contracts, purchase orders, lawsuits, and others related to litigation, as well as any other physical or electronic document that may establish the commercial relationship, agreements, invoices or tax documents or any other public or private document, or relevant working papers that may support the materiality of the transactions, and which may be used as evidence of the decisions or actions of Grupo Bimbo in reviews carried out by authorities, or in case of audits or trials.

Information retention: Technique to organize, track and secure internal tangible or intangible information. The retention must have security levels of access and protection, the greater the sensitivity, confidentiality or relevance, the more restrictive the access and the greater the level of protection in its safekeeping and destruction.

Intangible information: That which is presented digitally, such as emails, databases, registries, files, information in ERPs, digital platforms, digital receipts, etc.

Mandatory destruction of information: There are laws that require the destruction or return to the owners of any document or medium containing personal data, once the service covered by the contract between the company and the client, collaborator or any other third party has been completed.

Method of securely erasing intangible information: Data deletion algorithms (e.g. complete disk overwrite) or physical destruction that ensures that digital information on company-owned storage units (e.g., hard drives, optical drives, USB sticks) cannot be recovered for later use.

Relevant information: Information that allows Grupo Bimbo to secure and defend its rights and/or to inform decisions made in the past or planned for the future. In addition, information that it is obligated to retain and/or control due to legal, fiscal, regulatory, legislative, financial or local requirements. Any information that does not meet the criteria may be destroyed for reasons of cost of storage.

Responsible in the Business Units: For the purposes of this policy, it refers to those who are responsible for the items and/or types of registration listed in Annex I.

Safe destruction of tangible information: Method of destruction of documents that guarantees the impossibility of reconstructing them and their subsequent use, as well as the recovery of any information contained in them (e.g. shredding, pulverization, incineration).

Tangible information: That which has a physical presentation (e.g. contracts, invoices, quotes), evidence and materiality of transactions of services and/or purchases of goods, etc.

4. Responsibilities

Global Functional Departments and associates responsible in the Business Units: Comply with the guidelines set in this policy. Define the protocols for retention and destruction of information, specifying its relevance and expiration period for disposal, according to the standards and operational or legal needs. Ensure that those responsible for each Department and Business Unit adopt the appropriate procedures for the handling and conservation of documents and physical and electronic information, in order to maintain safekeeping, in accordance with their sensitivity, confidentiality and relevance. Interrupt the destruction of information, by virtue of reviews, audits, investigations, foreseeable litigation or requests from an authority. Ensure the secure and confidential destruction of documents, with the same level of security they have had throughout their life cycle. If regional conditions require it, Business Units should create local guidelines to comply with operational and legal standards.

Global Legal and Compliance Department: Advise, at the request of the Functional Global Departments and those responsible in the Business Units, on the legal aspects of retention and destruction periods and situations in which the destruction of information must be interrupted. Establish the sanctions in case of violation of this policy.

Global Controlling Department and Global Tax Department: Advise, at the request of the Functional Global Departments and Business Units, on the financial and fiscal aspects of retention periods, destruction and situations in which the destruction of information must be interrupted.

Global IT Department: Execute the protection and assurance controls for the protection of electronic information, according to the levels of sensitivity, confidentiality and relevance of the information, defined by the areas that own it and the operational processes.

IT Departments in the Business Units: Ensure that, before selling or disposing of a company-owned computer or server, the information contained on the storage units is destroyed by methods of securely deleting intangible information.

5. General guidelines

All the information of operations, transactions, contracts, databases, correspondence, accesses and keys to tools are unique and exclusive property of Grupo Bimbo, including that from mergers, acquisitions and/or joint ventures processes, therefore, in order to define and regulate the periods of retention and destruction of this and to preserve that which is relevant, it is the policy of Grupo Bimbo to comply with the following guidelines.

Retention and destruction

All associates must:

- Adhere to information retention and destruction periods in accordance with local laws.
- Apply the appropriate retention and destruction protocols for those data that are governed by privacy laws and protection of each region, see ***FGB-CP-01 Global Policy on Personal Data Protection***.
- Report any mishandling or improper destruction of information through Speak-up or directly with the local security area, the local legal officer or the local information systems department, in case of digital information.

Retention

For the proper retention of information, collaborators should:

- Take into account the relevance of the information, according to the daily operations of Grupo Bimbo; since there is information that by its nature must be retained for a minimum period.
- Consider that the information loses utility and purpose, and keeping it longer than necessary puts Grupo Bimbo at risk of unauthorized information output and breach of privacy laws.
- Maintain relevant tangible and intangible information of the processes for which they are responsible, in an optimal, organized, traceable and identifiable state within the company and assigned devices, taking care of its confidentiality in accordance with ***GGB-005 Global Policy on Confidential Information.***
- Perform backups of all relevant intangible information in the cloud, instead of on their computers (e.g. fixed or portable computers, smart phones, etc.) to avoid loss due to force majeure.
- Ensure that all documents or files with relevant information contain a control to track the creation date or effective date.
- Apply the retention periods defined in Annex I of this policy, which lists some groups of relevant information that must have a retention period; this list is not limitative, so for a more comprehensive application, the definition of relevant information must be followed.
- Follow the longest period defined between this policy and the applicable legislation.
- Take all necessary measures to safeguard and preserve the information and databases, in a complete and integral manner, when a transfer of information is made between third parties and companies of Grupo Bimbo, as well as between areas and / or subsidiaries thereof, in order to guarantee the rights and obligations of Grupo Bimbo and the full compliance with the guidelines contemplated in this policy.

Destruction

Associates must:

- Keep records of creation and destruction and version control, of the information designated as sensitive, confidential or relevant, according to the guidelines of each Global Functional Department, and use the means of destruction that ensures the information cannot be reconstructed or read by unauthorized people.
- In the case of mandatory destruction of information, adhere to the period indicated by the applicable law, and their destruction must follow the same level of security that they have had throughout their life cycle.
- In those regions that do not have information retention and destruction laws, retain the relevant information for a minimum of twelve years before starting the destruction.
- Before the imminent start or notice of some of the following events: litigation, internal audit, audit by government authorities or internal or external investigation:
  - Suspend the destruction of relevant information.
  - Notify and consult with the local legal area to determine the duration of the suspension of the destruction.
  - The suspension will last at least 6 months, after the closure or conclusion of the litigation, audit or investigation.

Sanctions

The associates of all Grupo Bimbo companies must adhere to the guidelines of this policy. In the event of non-compliance, associates are subject to the disciplinary measures established by the Global Legal and Compliance Department. In case there is any confusion about the retention or destruction of information, a representative of this Department should be consulted for clarification and better understanding.

6. Annexes

Annex I
Retention Periods

7. Responsibility / Ownership

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

8. 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	Feb, 2021	Ignacio Stepancic	Luis Miguel Briola	
2	Sep, 2022	Victor Tapia Quevedo	Ignacio Stepancic	• The retention period for e-mails was changed to two years. • The retention period for personnel documents was changed from fourteen years to twenty years, at the request of the global people department.