1. Purpose

Establish the general guidelines for the creation and management of passwords in the information systems of Grupo Bimbo.

2. Scope

This policy applies to the administrators of applications and to the Global Information Security Department of Grupo Bimbo S.A.B. de C.V., and/or any of its affiliates ("Grupo Bimbo" or "the company").

3. Definitions

Approved encryption algorithms: Algorithm used in one-way and used to storage access passwords in a secure way.

Authentication: Activity to verify the identity of a user, process or device, to allow access to information technologies.

Multifactor authentication: Activity additional to the traditional user credentials validation (username and password) to verify the identity of a user, through a unique code sent to a mobile device or using a custom token.

Confidentiality: Security principle which requires that the data only should be accessed by the authorized users.

Password: Authentication that uses a character string to grant access for information technology.

Global IT Departments: Global Departments of i) Information and Services, ii) Service Delivery and Digital, iii) Infrastructure.

Integrity: Security principle that guarantees the modification of data and configuration activities only by the owner and authorized personnel. Considering all possible modification causes, including software and hardware flaws, environmental events and human intervention.

Irreversible cryptographic transformation: Procedure that uses an algorithm to encrypt a message in an incomprehensible or difficult way to understand.

Usability: Level in which a product can be used to achieve specific goals.

4. Responsibilities

Applications administrators and Global Information Security Management: Define and guarantee the implementation of established security criteria in the present policy.

5. General guidelines

In order to preserve the confidentiality, integrity, availability and IT usability, as well as to avoid any inappropriate use of the information assets of the company, it is mandatory to comply with the following guidelines:

Passwords management

The application administrators, together with the Global Information Security Department, must ensure:

- The implementation of security parameters to guarantee the creation of secure passwords according to the procedure set forth for this activity.
- The company applications must request the change of passwords every 90 days.
- The existence of rules inside the company applications forbidding the use of previous passwords, considering the last 6.
- The existence of rules inside the company applications warranting the use of passwords between 12 and 14 characters in length
- Automatic block of accounts to access the company applications after 5 failed attempts.
- The request of multifactor authentication to access the applications, through a different network of the company.
- The use of irreversible cryptographic transformations to protect the user´s passwords.
- The implementation of approved encryption algorithms (irreversible) in the company applications which storage and transfer passwords to other applications.

6. Responsibility / Ownership

The Global IT Departments are the assigned owners of this policy and are 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				