1. Purpose

Establish general guidelines for the management of user accounts whose privileges are used to configure, administer or support Grupo Bimbo's information systems.

2. Scope

This applies to users of applications that support business functions at the different Grupo Bimbo Departments, areas, Business Units and subsidiaries that have direct or indirect responsibilities for managing privileged accounts in any of Grupo Bimbo's information systems.

3. Definitions

Help Desk: The entity responsible for providing the services of attention to incidents and requirements of end users.

Privileged accounts: The application or system accounts that have advanced or elevated permissions, compared to the permissions that a regular user account has.

Privileges: The system permissions associated with a user account, including, but not limited to, the permissions to access or change data, process transactions, create or change configurations, etc.

User: Associates, consultants, personnel with temporary assignments and anyone who has any type of direct or indirect employment relationship with Grupo Bimbo and who access the company's information systems.

4. Responsibilities

Roles and access manager: Maintain an updated and custodian inventory of the privileged accounts of all Grupo Bimbo information systems. Manage and authorize the creation, modification and deactivation of privileged accounts in cooperation with the administrator of the application. This role belongs to the Global Systems Department.

Application administrator: Maintain the registry of privileged accounts for the system for which they are responsible. Keep the registry updated and communicate to the roles and access manager all changes to privileged accounts, at the moment they occur.

User: Solely responsible for the appropriate use of the privileged account where access was granted for the performance of their job functions. Immediately notify the security group when something indicates an information system has been compromised, especially through the use of the privileged account.

5. General Guidelines

All personnel with privileged access to Grupo Bimbo (or Grupo Bimbo subsidiary) systems and applications are expected to follow and comply with these guidelines.

Access

- Any request for access to information systems through a privileged account must be requested through the help desk. Any such request must be accompanied by a business justification and approved by the role and access manager.
- The Functional Director, together with Global Systems Director, may authorize the use of privileged accounts in the information systems.
- No assignment of a privileged account may be valid for more than six months. If an extension is

required, the user must request again the authorizations indicated in this policy.

Administration

- Requests to create, deactivate and update privileged accounts must be submitted through the Grupo Bimbo help desk. A valid business justification and approval by the access and role manager is required before the privileged access will be granted.
- Only the Functional Director, together with the Global Systems Director, can authorize privileged account changes (creation, deactivation and updating of attributes and permissions).
- The role and access manager must ensure that privileged accounts are not personalized or associated with an identity from the global identity directory, however there should be a record about the assignment.
- The application administrator must update the passwords of the privileged accounts when the use of these accounts ends, or when their last access has exceeded 30 calendar days. Passwords of the privileged accounts must also be changed when people who have access to these accounts leave the company or change jobs within the company.

6. Responsibility / Ownership

The Global Internal Control and Risk Management 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 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				