1. Purpose

Establish the general guidelines for the firewall administration installed in the company network.

2. Scope

The present policy applies to the associates that are part of the Architecture Committee and the Global Infrastructure Department of Grupo Bimbo, S.A.B. de C.V.

3. Definitions

Firewall: Security device that monitors the network traffic and allows or blocks the data traffic based on a set of rules.

Leader of IT Project: Associate responsible for managing the IT project tasks execution.

Risk: Fact, action or omissions that could affect in a negative way the company capacity to achieve its business goals and execute success strategies.

4. Responsibilities

Architecture Committee: Evaluate and according to the results, approve or reject prior to its execution, the requirements and security controls of the Information Technologies (IT) projects.

Functional Department: Authorize and define the maintenance time for system changes.

Global Telecommunications Management: Authorize the firewalls installations within the company network.

Global Information Security Management: Ensure the compliance policies authorized by Architecture Committee.

5. General guidelines

In order to maintain the information security, transmitted through the company network is Grupo Bimbo policy to comply with the following guidelines:

Firewall configuration

- The IT Project leader must request through *Service Now,* the enable traffic authorization between firewalls, sites and/or required applications, prior to the project execution.
- Only the Global Telecommunications Management can authorize or install firewalls in the company IT infrastructure.
- The Global Information Security Management must ensure the production environment firewalls located in the company IT infrastructure contain the configurations approved by the Architecture Committee.
- Any required change in the firewalls configuration, located in the company facilities, must be according to the service now change management procedure and this change must be applied out of working hours and with Functional Department authorization.

Recertification

For the apply configurations recertification firewalls, the Global Information Security Management must:

- Validate the “super users” and “users with privileges” access control assignments in order to recertify the granted permissions.
- Monitoring that the firewall management service provider has installed the latest patches issued by the manufacturer

Physical access

The Global IT Field Services Management must ensure the physical access to the Data Centers, located in the company facilities, must be according to ***FGB-IT-18 Global Policy for the Information Technology Security for Data Centers Physical and Environmental.***

6. Responsibility / Ownership

The Global IT 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				