1. Purpose

Establish the general guidelines for the implementation and use of wireless connection technologies in any Grupo Bimbo facility.

2. Scope

This policy applies to the management of all wireless networks at all Grupo Bimbo, S.A.B. de C.V., (GB) and GB affiliate locations. This policy also applies to all GB associates responsible for supporting and maintaining company wireless networks.

3. Definitions

Encryption: Data conversion process, from a readable format to a coded format, to protect the information confidentiality.

Active directory: Tool included in operative systems and designed for the users and network resources management.

Routing device: Technological device used for the creation and management of networks to unite them and route them between them.

Personal devices: Any technological device that is not owned by the company (i.e. tablets, smartphones, personal computers, etc.).

Domain: Name given to the set of technological devices connected between them, which, may or may not, have access to the internet.

Firewall: Security device implemented in networks for internet traffic monitoring, which allows website blocking through the implementation of configuration rules.

Guest: Person outside the company or associates that visit other Business Units and require internet access through personal devices.

Captive portal: A designed tool to give internet access, through an information exchange that allows the identification of the person that requires it.

Network segment: Subdivision that is made to a network, to increase the number of connected devices to it, boost its performance, and facilitate its management.

SSID: Name given to the wireless network, commonly known as Wi-Fi, for its identification.

4. Responsibilities

Network administrator / designee: Generate and maintain an updated inventory of wireless access points. Comply with and enforce the established guidelines in the present policy for the wireless networks management

Global Telecommunications Management: Administer the access of the identified wireless network devices.

5. General guidelines

In order to reinforce the security of the Grupo Bimbo wireless networks access, IT must comply with the following requirement:

Network controls

The network administrator or their designee must:

- Ensure that the company owned devices are connected to the internal (company) network. I.e., are NOT connected to the guest network *(GB Guest).*
- Ensure that non-company owned devices are NOT connected to the internal network.
- Define the structure of the password, for all the wireless SSID, according to ***FGB-IT-03 Global Password Management Policy.***
- Change the passwords of all wireless SSID at least once a year
- Restrict access to the wireless network devices only to all associates and/or third parties. Any exceptions to this requirement must be authorized by Global Telecommunications Management.
- Ensure company wireless networks have two network segments (external (Guest) and internal (Employee) network).
- Ensure that the wireless SSID is divided for the next groups:
  - Laptop and desktop computers.
  - Smartphones, tablets, hand-helds, wireless printers, televisions, and non-smart devices.
- Provide to the third parties and/or guests, who visit the company facilities and require internet network access, with an appropriate username and temporary password, ensuring that:
  - The username and password are created in a captive portal, through which, the guests could access to the internet.
  - The validity of the guest account is valid for a maximum of 5 days.
  - The guest account only has access to internet browsing.

Security in network services

For security in network services, the Global Infrastructure Department must:

- Ensure that all the information assets belong to the domain of the specific company´s active directory.
- Avoid the existence of wireless access points or routing devices that are NOT administrated by the Global Infrastructure Department.
- Ensure that the firewall rules and web content filtering, established by the Global Information Security Management, restrict unauthorized access to the internet.
- Define and guarantee the use appropriate of security protocols and encryption in wireless devices.
- Ensure that the wireless transmissions (WIFI) used to access the networks and devices of the company are encrypted. In case a public network is used, the protocol used must guarantee that the authentication data and its content are encrypted.
- Ensure that all wireless information transmissions are done using appropriate wireless transmission security protocols and approved encryption technics.

At the same time, the network administrator or their designee must:

- Encrypt the confidential information using the most secure and appropriate configuration available according to requirements defined by the Global Infrastructure Department.
- Ensure that company wireless networks that transmit information or are connected to confidential information environments, comply with the industry encryption practices for security, authentication and information transmission.
- Perform semi-annual scans to detect all Wireless access points, both authorized and un-authorized.
- Ensure the existence of an inventory of authorized wireless access points by the Global Telecommunications Management.
- Ensure appropriate response procedures are in place and operating effectively, in case un-authorized wireless access points are detected.

6. Responsibility / Ownership

The Global GB 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				