1. Purpose

Establish the general guidelines for protection against vulnerabilities, and for ensuring appropriate security measures are implemented to protect the information assets of Grupo Bimbo and its subsidiaries.

2. Scope

This policy applies to the associates of the Global IT Departments, as well as application owners and administrators of Grupo Bimbo, S.A.B. de C.V., and/or any of its affiliates.

3. Definitions

Change: Any modification that could have an effect on IT services. Its scope could include changes in architectures, processes, tools, metrics, and documentation, as well as other configuration elements.

Malicious code: Software designed to infiltrate, damage, or obtain information on the computer system without the owner's consent. It is commonly includes viruses, worms, trojan horses, spyware, and adware.

Vulnerability: Weakness that could provoke a threat to the information assets (i.e., an open port in a firewall, a password that has never changed or an open folder). Also, the lack of control is considered a vulnerability.

4. Responsibilities

Global Infrastructure Department and Global IT Governance Department: Establish and communicate the controls that ensure the configuration and protection of the information assets.

Global IT Risks and Compliance Management: Perform the impact calculation of the vulnerabilities through the risk analysis.

Global Information Security Management: Perform the analysis of development vulnerabilities or relevant application changes and guarantee the compliance of the isolation procedure for information assets infected by malicious code.

Applications owners and administrators: Generate and keep updated the IT assets inventory, as well as comply with the guidelines of the present policy.

5. General guidelines

In order to guarantee the control and protection of information assets, the following guidelines are mandatory:

Technical vulnerabilities

For technical vulnerabilities management, the application owner must:

- Establish the roles and responsibilities for the monitoring, identification and remediation of all active and potential vulnerabilities.
- Inform to the Global Information Security Management of any changes or new developments that could affect the configuration or operation of the application, in order complete the required vulnerability analysis.
- Request from the Global IT Risks and Compliance Management the impact calculation for the vulnerability, in order to estimate the risk to company information assets.
- Based on the risk analysis, define the actions and the provider responsible for implementing appropriate actions, and providing technical support to the application.

- In the event of a security incident, request the support from the Global Information Security Management to provide a solution for the incidents presented and appropriate remediations for the vulnerabilities detected.

At the same time, the administrator of the application must:

- Ensure the information systems (network, servers, databases, and applications) have the appropriate security patches installed. And these patches are acquired from legitimate sources.
- Establish a security patch installation plan, prioritizing the systems identified as critical.
- Test the security patches in a test environment, prior to installation in the production system.
- Implement the additional protection controls when the attention of the technical vulnerabilities exceeds the expected cost-benefit for the information asset.
- Attend the recommendations from the Global Information Security Management, which could be from the execution of risk analysis to the application cancellation.

Application installation

- The Global Infrastructure Department, together with the Global IT Governance Management, must establish a process to manage and control changes to company infrastructure and applications.
- The site support team must install only the software that is tested and approved by the Global IT Governance and the Information Security Management groups.
- The application owner or administrator must:
  - Comply with the installation controls and, in the event of a failure, restore the previous configuration.
  - Keep track of all the updates in the information assets.

Protection

In order to guarantee the protection of the applications against malicious code, the Global Information Security Management group must:

- Define appropriate protection software, for the information assets, against malicious code, and the protection metric to be applied.
- Define the isolation procedure for an information asset that is infected by a malicious code, to prevent its propagation. In case where elimination of the malware is not possible, ensure that the equipment, software or application is removed from the company network.
- Ensure, together with the Global Infrastructure Department, that the information assets have a protection software against malicious code.

6. Responsibility / Ownership

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

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				