1. Purpose

Establish general guidelines for the administration of the roles assigned to users who operate Grupo Bimbo's information systems, and for the management of the global model for segregation of duties.

2. Scope

This policy applies to users of the different Grupo Bimbo Departments, areas, Business Units and subsidiaries that have direct or indirect responsibility for managing roles and the segregation of duties model in any of Grupo Bimbo's (and subsidiary) information systems.

3. Definitions

Access assignment rule: A set of attributes of an identity that determines the associates' access to information systems.

Application: Program or system that provides functionality or information technology (IT) service to users.

Global Key Approver: Functional expert of the business process implemented in one of the specific application systems and appointed by the Global Functional Director.

Minimum privilege: Minimum required permissions granted to a user account or process for that user to perform the functions of their position.

Permission recertification: Annual evaluation of privileges granted to a user (e.g. existence and validity) or at the time of registration, cancellation or change of functions, whichever occurs first.

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

Segregation of Duties Model (SoD): The framework that regulates the requirement for adequate separation of activities and privileges in order to reduce the risk of fraud and errors. Segregation of Duties controls implement an appropriate level for supervision and workload upon the activities of individuals.

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

4. Responsibilities

Global People Department: Ensure the integrity of the information in the source systems. Notify to the roles and access administrator when any update occurs in the catalogs associated with the rules for assigning access.

Global Internal Control Department: Approve all changes to the segregation of duties model and promote its compliance at a global level. Generate and monitor the user access recertification campaigns of users and roles within the Organization and report the result.

Functional Vice Presidents: Responsible for the segregation of duties that guarantees the separation of duties and privileges in order to reduce the risk, measured in impact and probability, that intentional or unintentional errors may affect the assets and / or image of the Company, in information systems and / or applications used for its operation.

Global Key Approver: Identify the risks and define the necessary controls that guarantee an adequate segregation of duties within their area of responsibility; approve all changes in the segregation of duties model in its area of competence and fully comply with the model worldwide.

Organization and / or Business Unit Functional Directors: Authorize the privileges granted in the application systems taking into consideration the segregation of duties and applying the principle of the minimum privilege required for user.

Direct and/or Functional manager: Authorize the privileges granted in the application systems and request the deactivation of these in a timely manner in the event of the resignation or change of functions of an associate, as well as supervising the execution of compensatory controls related to the segregation of duties.

User: Only person responsible for the use of the application accesses and privileges they have been granted to perform their assigned job function, as well as for executing and monitoring any established compensatory controls to ensure the segregation of duties.

Global identity directory administrator for role management: Configure and update business and application roles, as well as their respective access assignment rules, in the global identity directory system. Ensure consistency of permissions / privileges between information systems and the global identity directory.

Application administrator: Create, update and revoke access permissions and roles in the application under their responsibility.

5. General Guidelines

To ensure adequate control of the role administration model and segregation of duties functions, it is Grupo Bimbo's policy that all personnel comply with the following guidelines:

Role management

- Global IT Department must ensure that all information systems consider the application of roles as part of their release to production.
- The role owner (functional departments) must:
  - When generating the roles, an access assignment rule must be defined that ensures the correct segregation of duties.
  - Validate and authorize requests for modification or elimination of a role, derived from business needs, company policies or regulatory compliance.
- Functional Vice Presidents and the functional Directors of the Organization and / or Business Unit must authorize the generation and / or updating of roles, ensuring the principle of minimum required privilege and ensuring the correct segregation of duties in the information systems related to the business processes under their responsibility.
- The role and access administrator must ensure that access to information systems is granted in accordance with the role assignment rules as defined by the role owner.

Assignment of privileges

- Any request for privileges in the company's application systems must be supported by the approval of the associate's Direct Manager and by what is stated in the ***FGB-IT-22 Access Management Global Policy***. Additionally, privileged accounts require authorizations from a global key approver and from the Global IT Department.
- The user's Direct Manager must promptly request the deactivation of the previously assigned

privileges for access terminations or changes to functional access within the application.
- The user's Direct Manager must also supervise the execution of appropriate compensatory controls related to the segregation of duties.
- The privileges granted due to: a) emergency access to resolve highly critical incidents; b) insufficient head counting to support a process; c) absenteeism (e.g. vacation, illness, etc.), must be authorized by the functional Director of the Organization and / or Business Unit, with a maximum validity of 6 months.

Segregation of Duties (SoD)

- Global key approvers must:
  - Create and update the role and responsibilities matrices that form part of the governance model and submit them for authorization to the Grupo Bimbo Internal Control Global Department.
  - Identify, record and update the segregation of duties matrix with the risks and the definition of mitigating controls in order to ensure associates and third-party personnel responsibilities have the adequate segregation of duties.
- Functional Departments are responsible for the remediation of the detected segregation of duties conflicts.
- In case of exceptions where it is not possible to guarantee an adequate segregation of duties, the role and access administrator may authorize accesses that contain conflicts, it is mandatory that the role owner implements compensatory controls that mitigate the risks to Grupo Bimbo's information.
- Compensating controls must be documented in such a way that the Global Internal Control Department can verify its validity and execution regarding access Grupo Bimbo's information.
- Exceptions to these requirements must be justified by a Grupo Bimbo relevant business need and requires authorization by a Global Functional Vice President.

Role certification

In order to ensure the validity of the permissions assigned to specific roles, the following must be done:
- Execute annual recertification campaigns for privileges assigned to a role, ensuring compliance with policies, regulations and mitigating controls.
- As a result of the recertification process, changes should be implemented as required. If the creation, modification or elimination of roles is needed; these changes should be implemented through the role and access control area.

User certification

In order to evaluate the privileges granted to users at the time of their registration, cancellation or change of functions, the Direct Manager must:
- Perform yearly user recertification campaigns. The review must be performed to ensure:
  - The validity of user's access to functions within the application
  - That associates or third-party personnel have no access conflicts within the application.
- Required changes or remediation of user access that are indicated by the recertification process should be processed through the Global IT Department to ensure the changes do not adversely impact the operation, performance of the application, or business function.

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 Global Internal Control Department, 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				
2	March 3, 2021	Ricardo C Chávez Cruz	Gabriela López Juarez	Segregation of duties controls were included