INFORMATION SECURITY ROLES AND RESPONSIBILITIES MANUAL

GRUPO EMPRESARIAL COLOMBINA

OBJECTIVE

To define the roles and responsibilities involved in the management of the information security system of the Grupo Empresarial Colombina.

SCOPE

This manual applies to executives, employees, and suppliers who perform activities within the Grupo Empresarial Colombina.

CONDITIONS

Basic rules, characteristics, validations, and verifications considered for the development of the activities.

STEPS TO FOLLOW

The roles and responsibilities of Information Security within the Grupo Empresarial Colombina define an information security organization, which will be composed of:

a. Information Security Committee.
b. Information Security Officer.
c. Asset Owner.
d. Information Custodian.
e. End User.

a. Information Security Committee

The Information Security Committee, composed of an interdisciplinary group with decision-making power within the organization, serves as the highest authority on information security within the management system. The committee meets once a month as a regular occurrence and can convene extraordinary meetings whenever deemed necessary by the Information Security Officer.

The committee members are as follows:

Additional individuals may attend the security committee meetings as advisors at the discretion of the Information Security Officer.

Responsibilties

- Validate, approve, and authorize the implementation of actions, activities, projects, and policies related to the ISMS (Information Security Management System) in terms of business characteristics, organization, location, assets, and technology.
- Validate and approve a risk assessment methodology that is appropriate within the organization and complies with regulatory, legal, and information security requirements of the business.
- Validate and approve residual risks.
- Validate and approve a statement of applicability proposed by the Information Security Officer.
- Validate and approve a risk treatment plan that identifies appropriate management action, resources, responsibilities, and priorities to address information security risks.
- Validate and approve the allocation of new resources for ISMS activities or projects.
- Be informed about the results of investigations into information security incidents.
- Be aware of the tracking and review procedures for ISMS matters.
- Be aware of regular reviews of information security documentation (including policy and objectives compliance and security control reviews), taking into account the results of ISMS audits, incidents, effectiveness measurements, suggestions, and feedback from all stakeholders.
- Validate and approve developed security plans.
- Facilitate and promote the development of initiatives related to the ISMS.
- Approve and review indicators of the Information Security Management System.
- Issue communications to the organization regarding the importance of meeting information security objectives and compliance with the information security policy, their responsibilities under the law, and the need for continuous improvement.
- Validate and approve criteria for risk acceptance and acceptable risk levels.
- Ensure that internal audits are conducted at planned intervals and be aware of the results.
- Be aware of the responsibility assignment procedure defined in the information security subprocess, ensuring that all personnel are competent to perform the required tasks.
- Approve and review the scope, objectives, and strategies of the Information Security Management System.
- Approve and periodically review ISMS policies and standards.
- Validate the integration of the Information Security Management System with the Integrated Management System.

b. **Information Security Officer:** The Information Security Officer is responsible for coordinating the execution of activities derived from the planning, implementation, review, and maintenance of the ISMS. They coordinate the tactical and operational aspects by implementing the directives of the security committee and leading the ISMS.

Responsibilties

- Defining and proposing to the security leader the scope and boundaries of the ISMS in terms of business characteristics, organization, location, assets, and technology.
- Define and propose to the security leader the ISMS policy in terms of business characteristics, organization, location, assets, and technology.
- Define and propose to the security leader the methodology for identifying, assessing, classifying, and treating information assets.
- Define and propose to the security leader a risk assessment methodology that is suitable for the ISMS and complies with regulatory, legal, and information security requirements identified by the business.
- Coordinate the risk identification management conducted by the respective areas.
- Coordinate the risk management process, including risk analysis and evaluation.
- Identification and evaluation of options for risk treatment.
- Selection of control objectives and controls for risk treatment.
- Receive residual risks from responsible areas and present them to the ISMS leader.
- Validate the implementation and operation of the ISMS.
- Define and present to the ISMS leader a statement of applicability.
- Consolidate information on the risk treatment plan designed by responsible areas and present it to the ISMS leader.
- Coordinate the implementation of the risk treatment plan for each area.
- Coordinate the implementation of selected controls from each area.
- Coordinate the definition of the effectiveness of controls or control groups selected by the areas.
- Coordinate and participate in the design and implementation of training and awareness programs related to the ISMS.
- Validate the need for new resources for the ISMS to establish, implement, operate, monitor, review, maintain, and improve an ISMS and present it to the ISMS leader.
- Participate in the design and definition of procedures and controls to detect and respond promptly to security incidents.
- Coordinate the implementation of the monitoring and review procedures for the ISMS.
- Coordinate the measurement of control effectiveness to verify compliance with security requirements.

- Coordinate the planned reviews of risk assessments, residual risk, and acceptable risk levels.
- Coordinate the conduct of internal audits of the ISMS at planned intervals.
- Consolidate information from areas regarding developed security plans and present it to the ISMS leader.
- Facilitate and promote the development of initiatives regarding information security.
- Manage ISMS documentation in coordination with the responsible department (processes).
- Manage the procedure for defining document management actions in coordination with the Processes department.
- Coordinate the establishment and maintenance of records to provide evidence of compliance with requirements and the effective operation of the ISMS in coordination with the Processes department.
- Define and propose to the ISMS leader the criteria for risk acceptance and acceptable risk levels.
- Coordinate and participate in the design of the responsibility assignment procedure defined in the ISMS to ensure that all personnel are competent to perform the required tasks.
- Coordinate the regular reviews of ISMS effectiveness (including compliance with ISMS policy and objectives, and review of security controls), taking into account the results of security audits, incidents, effectiveness measurements, suggestions, and feedback from all stakeholders.
- Lead the analysis and investigation of information security incidents.
- Lead the management of information assets and risks within the organization.
- Propose preventive or corrective actions, communicate them to the responsible area, and validate the actions proposed by the respective areas.
- Ensure the integration of the Information Security Management System with the Integrated Management System.

c. **Information custodian:** The information custodian is any employee or third party who has the responsibility to maintain and support the security controls on the assets that contain Colombina's information.

Responsibilities:

- Provide assistance to the asset owner and the security officer in selecting appropriate technical solutions for implementing or improving controls.
- Operationally ensure the confidentiality, integrity, and availability of information.
- Apply the appropriate level of handling to information classified as "SENSITIVE" according to the information classification procedure.
- Accept, understand, and comply with information security policies and procedures.

- Report any non-compliance with information security policies to the security officer.
- Participate in information security awareness programs.
- Use organizational information in an ethical and responsible manner.
- Report information security events or incidents.

d. Asset Owner: The asset owner is a designated entity, position, process, or workgroup that has the responsibility to ensure that information and assets associated with the process are appropriately classified. They are responsible for defining and regularly reviewing access restrictions and classifications.

Responsibilities:

• Maintain an up-to-date inventory of information assets.
• Determine the classification level of each asset for which they are responsible, as defined in the personal information classification procedure.
• Identify the risks to which the information assets under their responsibility are exposed.
• Identify relevant controls to address the risks for which they are the owner and approve the risk treatment plan.
• Understand and approve the residual risk.
• Validate the operation of defined controls with the support of the asset custodian.
• Define the profiles of the information assets under their responsibility.
• Approve access to the information assets under their responsibility.
• Communicate personnel updates to the human resources department.
• Accept, understand, and comply with information security policies and procedures.
• Report non-compliance with information security policies to the security officer.
• Participate in information security awareness programs.
• Use organizational information in an ethical and responsible manner.
• Report information security events or incidents.

e. End User: An end user is any employee or third party who utilizes Colombina's information for their activities.

Responsibilities:

- Apply the appropriate level of handling to information classified as sensitive, as determined by the personal information classification procedure.
- Accept, understand, and comply with information security policies and procedures.

- Report non-compliance with information security policies to the security officer.
- Participate in information security awareness programs.
- Use organizational information in an ethical and responsible manner.
- Report information security events or incidents.
- Contribute to the effectiveness of the information security management system.
- Accept, understand, and comply with the activities included in the processes they are involved in.
- Report information security events or incidents.

Definitions:

Asset: Any element that has value for the organization. For Information Security Risk Management, the following types are considered: information, business activities and processes, software, hardware, personnel, networks, organization, and location.

Threat: Potential cause of an unwanted incident that can result in harm to the system or the organization. [Source: ISO 27000]

CISO: Chief Information Security Officer.

Confidentiality: Property of information that ensures it is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Measures that modify risk. [Source: ISO 31000]

Availability: Property of being accessible and usable by authorized entities upon demand. [Source: ISO 27000]

Information Security Event: Identified presence of a system, service, or network condition that indicates a possible violation of the information security policy or failure of safeguards, or a previously unknown situation that may be relevant to security. [Source: ISO 27035]

Incident: Unwanted or unexpected event or series of information security events that have a significant probability of compromising business operations and threatening information security. [Source: ISO 27035]

Integrity: Property of accuracy and completeness. [Source: ISO 27000]

Risk Management: Coordinated activities to direct and control an organization regarding risk. [Source: ISO 31000]

Monitoring: Verification, supervision, critical observation, or continuous determination of the status to identify changes in relation to the required or expected level of performance.

OPDP: Officer for Personal Data Protection.

ISMS: Information Security Management System.

Risk: Effect of uncertainty on objectives. An effect is a deviation from what is expected, whether positive, negative, or both. Objectives can have different aspects (economic, image, environmental) and can be applied at different levels (strategic, operational, entire organization). [Source: ISO 31000]

Vulnerability: Identified weakness on an asset that can be exploited by a threat to cause an impact on the confidentiality, integrity, and/or availability of information.