GENERAL INFORMATION SECURITY POLICY

Change Control

Version	Observation	Date	Created/Modified by
2.0	Update of Information Security Policy	06/01/20	Angélica Trujillo, Head of Information Security
2.1	Update section 1.5	06/07/21	Angélica Trujillo, Head of Information Security

Approval History

Version	Approval	Date	Publication Date
2.0	Laura Grimau, IT Deputy Manager	27/03/20	
2.1	Laura Grimau, IT Deputy Manager	08/07/21	19/07/21

1. Generalities

1.1 Objective

Grupo CAP, composed of the corporate entity and its Operating Companies, recognizing the importance of proper information management, is committed to implementing a policy that establishes the main guidelines for Information Security, safeguarding critical information assets against internal or external threats, whether deliberate or accidental, based on the security attributes of confidentiality, integrity, and availability.

1.2 Scope

This policy applies to all Grupo CAP employees and extends to suppliers and any service providers who access, process, transfer, store, or have any contact with our information assets.

1.3 Adherence

Failure to comply with or violation of the Information Security regulatory framework empowers Grupo CAP to take appropriate measures to sanction improper acts.

1.4 Definitions

- Information Asset: Any information or element related to its processing (systems, documents, media, buildings, people, etc.) that has value for the organization.
- Confidentiality: Ensuring that information is accessed only by authorized persons, entities, or processes.
- Integrity: Safeguarding the accuracy and precision of information accessed by authorized personnel, entities, or processes.
- Availability: Ensuring that information is accessible and usable when required by authorized personnel, entities, or processes.
- Information Security Event: Any occurrence related to assets or the environment indicating a possible security breach, control failure, or a situation relevant to security.
- Information Security Incident: One or more security events that negatively impact business operations and damage one or more information security attributes.

1.5 Roles and Responsibilities

- General Management: Responsible for strategic direction and promoting Information Security in the company, providing resources, assigning responsibilities, ensuring compliance, and raising awareness of the criticality of information assets.
- Head of Information Security: Defines security criteria, ensures compliance with this policy and related programs, advises staff, promotes security culture through training, manages risk analysis and incidents, and oversees policy development and monitoring.
- IT Department: Ensures the physical and logical security of information assets and system integrity, participates in incident management.
- Asset Owner: Classifies information assets based on criticality and sensitivity, maintains classification, and defines user access.
- Asset Custodian: Trusted individuals delegated by owners to safeguard assets according to established guidelines.
- End Users: Must comply with security regulations, protect company-provided information and resources, and report any security event or incident immediately.

2. Policy

Grupo CAP protects information assets to reduce potential impacts, identifying risks and maintaining an exposure level that ensures confidentiality, integrity, and availability. Key directives include:
- Comply with security attributes.
- Protect critical information assets.
- Minimize risk in critical functions.
- Establish a regulatory framework (policies, standards, procedures).
- Promote a security culture.
- Support technological innovation.
- Ensure business continuity during incidents.
- Align security strategy with ISO/IEC 27001.

Best practices are based on international standards such as ISO/IEC 27001, NERC-CIP, among others.

2.1 Information Security Principles

- Define and share security responsibilities across Grupo CAP and third parties.
- Protect information throughout its lifecycle.

- Apply controls for proper classification and access based on:
  - Need-to-know.
  - Least privilege.
- Protect processing facilities and critical infrastructure.
- Implement access controls for systems and networks.
- Protect stored and transmitted information.
- Ensure security is integral to the information lifecycle.
- Guarantee business continuity and operational resilience.
- Manage security incidents effectively.
- Stay updated on security trends.
- Periodically review the security program.

2.2 General Responsibilities for Employees

- Comply with security regulations.
- Protect assigned assets (passwords, laptops, email).
- Do not disclose sensitive information.
- Do not access unauthorized assets.
- Use assets responsibly.
- Cooperate in investigations and maintain discretion.
- Avoid exposing confidential information in unsupervised areas.
- Do not manipulate hardware/software without authorization.
- Do not install illegal or unlicensed software.
- Restart devices after security patches.
- All documents created or stored on company systems may be audited.
- Report any security event or incident immediately.

3. Final Provisions

3.1 Implementation and Compliance

The policy must be implemented within one year of approval. Compliance depends on the implementation process.

3.2 Validity

The policy remains valid annually from approval and will be reviewed by the Security Team or when significant events occur.