EXTRACT OF GENERAL INFORMATION SECURITY AND CYBERSECURITY POLICY

Code: SGSI-PO-01
Version: 2.4
August 2025

COPEC

Contents

01 Objective

01.1. General Objective

- To develop, implement, and maintain an Information Security model that protects the information assets of Copec SA and Copec Renovables SpA, hereinafter referred to as the Company or the Organization, by identifying the risks related to the creation, processing, storage, access, and destruction of said assets, as well as the controls that allow for the definition of roles and responsibilities of those involved in the related Information Security Management System (ISMS).

01.2. Specific Objectives

- To establish guidelines to maintain the confidentiality, integrity, and availability of the Organization's information, so that it is duly protected according to its assessment and classification.

- To ensure the establishment and implementation of controls that preserve the confidentiality, integrity, and availability of information, based on Information Security and Cybersecurity risk management.

- To outline the framework for managing the Information Security Management System (ISMS) appropriate to business requirements and in accordance with the guidelines defined in this policy.

- To define and establish roles and responsibilities in matters of Information Security and Cybersecurity.

02 Scope

The scope of this Policy includes the Board of Directors, Senior Management, Head of Departments, Employees, Contractors, Advisors, and External Collaborators of the Company who, in the exercise of their roles, make use of information and/or technological resources of Copec SA and/or Copec Renovables SpA.

Any other Company policy, rule, and procedure shall be subject to this document, with the General Information Security Policy serving as the basis of the fundamental guidelines for the development of other documents that regulate activities involving Copec SA and/or Copec Renovables SpA information assets.

03 Definitions

- Information asset: All data that is part of an information system, whether or not it enables the Company to make decisions.

- Senior Management: Composed of the CEO and the executive team. It is responsible for designing and implementing the Company's business strategy and ensuring Copec's sustainability.

- Risk appetite: Corresponds to the amount of risk the Company is willing to take on in order to achieve its strategic objectives.

- Risk capacity: This is the maximum risk that the Company can bear in pursuit of its objectives.

- Cyber threat: Potential cause of an unwanted incident that may affect the confidentiality, availability, and/or integrity of a system or cause damage to the organization by becoming a cyberattack.

- Cyberspace: The virtual space implemented between computers and digital information networks.

- Cyber risk: Risk is defined as “the effect of uncertainty on objectives” (ISO 31000). Cyber risk refers to the possible negative outcomes resulting from failures in the security of technological systems or those associated with cyberattacks.

- Cybersecurity: It refers to the development of business capabilities to anticipate and fight cyber threats, in order to protect and ensure the availability, integrity, and confidentiality of data, systems, and applications in the cyberspace associated with Copec.

- Malicious code: Software created to enter a computer system, breaching security controls, in order to perform unauthorized, harmful, and/or illegal tasks. Typically known as malware.

- Confidentiality: Property that ensures that information is accessed only by authorized persons and/or processes.

- Contractors and Advisors: Any person or company who is not a Company employee or director and who provides or offers professional or support services to the Company.

- Control: In the context of Information Security and Cybersecurity, it refers to countermeasures that help to stop threats to the Company's assets.

- Board of Directors: The highest governing body, whose role is to determine the strategic focus of the business.

- Availability: Property that indicates that data, as well as the resources that support it, must be accessible when and how required.

- Risk Assessment: Process that identifies and analyzes risks relevant to the achievement of the Company's objectives and determines how those risks should be managed.

- Risk factor: Any circumstance or situation that increases the likelihood of a risk materializing.

- Head of Department: Consisting of business managers (who report to other managers and not to the CEO) and area directors.

- Impact (magnitude): Loss caused by the materialization of a risk. It can be measured qualitatively or quantitatively.

- Information Security Incident: An unexpected or unwanted event with the significant potential to affect the information's properties (Triad).

- Cybersecurity incident: Materialization of a situation that affects the protection or security of the Company's data, systems, and applications that are essential to the business in cyberspace.

- Integrity: Information must be accurate, consistent, and complete throughout its life cycle.

- Information: An organized set of processed data that, regardless of its presentation, medium, or format in which it is created or used, serves as a basis for decision-making and knowledge acquisition.

- Log: A file containing activity records of a user or system.

- Policies and Standards: Reference documents for the proper use of the Company's information assets.

- Probability of occurrence: The possibility that a risk will materialize. It can be determined qualitatively or quantitatively.

- Asset Owner: Individual or entity designated by the Company to be responsible for managing the asset throughout its life cycle, ensuring that the asset under their responsibility is protected and secure.

- Risk Owner: Individual or entity that has the responsibility and authority to manage a risk to an Asset.

- Information Resource: Data storage elements, such as records (in different formats), files, databases, computer equipment, and software.

- Information Custodian: The employee for whom the information was created for the purpose of performing his/her duties and who is responsible for managing and classifying it, as well as assessing the risks that may affect it.

- Risk: The possibility that a specific threat could exploit a vulnerability.
- Inherent risk: Level of risk inherent in the nature of processes, systems, people, and suppliers.
- Residual risk: Remaining level of risk after taking measures to address the inherent risk.
- Sanction: Consequence or effect of committing an infringement associated with non-compliance with a Policy or Standard.
- Information Security: Set of policies, strategies, methodologies, resources, IT solutions, practices, and competencies to preserve Integrity, Availability, and Confidentiality.
- Information Security Management System (ISMS): Methodology that systematically allows to establish, implement, operate, monitor, review, maintain, and improve the information security of an Organization.
- Risk Tolerance: The acceptable level of deviation from risk appetite.
- Employee: Any person who has an employment contract with Copec and is subordinate and dependent on the company.
- Information Security Triad: Integrity, Availability, and Confidentiality.
- Vulnerability: A weakness that has the potential to allow a threat to materialize, affecting the information security of an asset. In general, it is a weakness that can be exploited by a threat.

04 Standards and reference frameworks

The following are standards and reference frameworks for Information Security and Cybersecurity, on which an ISMS is based. Its controls can be complemented to expand their governance capabilities.

- ISO 27001: Standard that defines the requirements for establishing, implementing, maintaining, and continuously improving an information security management system within an organization. It is complemented by the domains and controls outlined in ISO 27002.

- ISO 27005: Standard that provides guidelines for managing information security risk in an organization, particularly supporting the requirements of an information security management system based on ISO 27001.

- ISO 22301: Standard that specifies the structure and requirements for implementing and maintaining a business continuity management system.

- ISO 31000: Standard that provides principles and guidelines for managing the risk faced by organizations, with a common approach for any risk and without specifying an industry or sector.

- NIST CSF: Framework created by the U.S. National Institute of Standards and Technology (NIST). It proposes controls to help organizations manage their cybersecurity risks, respond to and recover from cybersecurity incidents.

- CIS Controls: Best practices for computer security, issued by the Center for Internet Security. It defines 20 controls that prioritize the actions an organization can take to improve its cybersecurity, proposing levels of implementation.

05 Structure for the approval of the Information Security Regulatory Framework

The approval of these documents will be carried out according to their category:

Type of document	Approver
General Information Security and Cybersecurity Policy	Copec's Board of Director
Specific policies	Chief Executive Officer
IT Policies and Standards	Chief Technology Officer
Procedures	Head of the area that manages the procedure

Specific Information Security and Cybersecurity Policies, Standards, and/or Procedures are established as part of this Information Security regulatory framework**,** in accordance with the domains outlined in ISO 27002, namely (and any other domains that may be incorporated into the aforementioned standard in the future):

- Information Security Standard
- Information Security Organization
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- Systems Acquisition, Development, and Maintenance
- Supplier Relations
- Information Security Incident Management
- Information Security Aspects of Business Continuity
- Compliance

06 Information Security and Cybersecurity Policy

Senior management acknowledges the importance of adequately protecting the Company's information assets against threats that could compromise business continuity. Therefore, it establishes the development of activities to protect its information assets, security culture, and behaviors for all those involved in the scope of this document.

Based on the above, the ISMS is founded on:

a) All employees of the Organization, as well as contractors, advisors, and external collaborators, must guarantee and ensure that information is only accessed by authorized personnel; that it is concise, accurate, and precise; that it is available when required; and that it is only legitimately accessed and used for the purpose for which it was authorized.

b) The three defined lines of defense must be proactive in establishing a robust culture of Information Security and Cybersecurity, setting an example of compliance with defined policies, standards, and procedures, carrying out awareness activities, and monitoring compliance with security guidelines.

c) Senior management and the second line of defense must be aligned with the definition and scope of Information Security and Cybersecurity risk management. Risk appetite, tolerance level, and maximum risk capacity must be approved at the highest organizational level.

d) The Company must have a process in place to identify, assess, and manage Information Security and Cybersecurity risks, which must be reviewed periodically and within a reasonable time frame for the organization.

e) The Company must have a process for approving changes to critical processes and systems that assesses information security and cybersecurity risks.

f) The Company must implement and maintain a process to calculate and monitor the degree of maturity of Information Security and Cybersecurity, based on standards and reference frameworks such as ISO 27000 and NIST CSF, which allow for continuous improvement through feedback from awareness activities and diagnosis of the ISMS.

g) The Company must ensure proper compliance with standards and laws associated with the protection of sensitive data, such as the Personal Data Law, establishing appropriate controls for this purpose.

06.1. Information Security

Information owners are responsible for their processes and for ensuring that they have the appropriate protection to maintain Confidentiality, Integrity, and Availability.

The Company must provide the means necessary to preserve and protect information assets.

06.2. Intellectual Property

All Company material considered part of its intellectual property must be specially protected with appropriate controls for this purpose.

06.3. Information Custodian

All information assets of the Organization must have a responsible party.

The person responsible for an information asset must ensure the security and correct use of that asset.

06.4. Compliance

Information Security and Cybersecurity policies, standards, and procedures must always be aligned and comply with applicable laws and regulations regarding privacy and information security.

06.5. Awareness and Training

The Company must establish and maintain a user awareness and training program that allows to maintain a strong culture of information security and cybersecurity.

Suppliers and contractors must be required to ensure that their awareness programs adhere to the Company's guidelines and policies.

06.6. Security in Access to Information

The Company must provide the necessary mechanisms to ensure that its employees and third parties access the information they require to perform their duties, based on the Principle of Least Privilege.

All users who access the Organization's information are responsible for their actions in the use of the resource. Therefore, they must have authentication through a username and individual password, which cannot be shared.

In systems that allow it, additional security must be implemented in authentication through multi-factor authentication. This requirement must be incorporated into the development of new projects that have user authentication for access to resources.

06.7. Control and administration of access to information

Access to Company information must be controlled to prevent unauthorized access.

User access to information must be defined and authorized by the owner of the information and protected in accordance with the classification of the information.

06.8. Classification of Information

The Custodian of an information asset must classify it according to its value, risk of loss or compromise, and/or based on legal or regulatory requirements.

The definition of classification, treatment, retention, and life cycle of the information must be defined in a specific policy or standard that addresses this control in detail.

06.9. Information Recovery and Business Continuity

Information assets and their related processes must have a business continuity plan. Similarly, they must have recovery plans in place in the event of information security incidents.

06.10. Physical Security

All Company departments and areas with physical facilities must have a level of security appropriate to the classification of the information assets they manage or process. The higher the classification, the more restricted physical access to the information assets must be.

The physical areas that support the technological infrastructure must have adequate controls. By way of example, the following controls are identified: doors against tailgating, electronic locks, proximity cards, biometric control, CCTV, among others.

Access to telecommunications cabinets or any Data Center is strictly prohibited except for personnel duly authorized by the Owner of the information assets stored there. For reference, such personnel are normally those responsible for managing this equipment and report to the Technology Management or the area that performs this role.