GENERAL INFORMATION SECURITY POLICY EMPRESAS COPEC S.A.

November 2015

EMPRESAS COPEC

CONTENTS

PREAMBLE

Information is an asset, exposed to dynamic risks and threats that may come from the inside or outside of the organization, and may be intentional or accidental. These risks may cause property and economic loss, damage to the corporate image and customer trust, legal breaches, regulatory noncompliance, violation of employees or third parties' rights. In lieu the above, it is important to properly secure the information assets of the organization.

For all of the above, Information Security is an ongoing process for Empresas Copec, aimed at protecting its information assets against threats that jeopardize their integrity, availability or confidentiality.

All company information, regardless of the manner in which it is kept or documented (format) must be adequately protected by means of implementing a set of controls, which are defined in policies, standards and procedures on Information Security.

In view of the above, the Board of Empresas Copec supports the strategic objectives of Information Security and ensures that they are aligned with business strategies and objectives.

The Information Security Policies of Empresas Copec are based on the current version of ISO 27002; this document responds to item 5 of said standard: "Information Security Policies".

1. OBJECTIVES

The Information Security Policy aims to:

1. Set the criteria and guidelines on information security management, applicable in Empresas Copec, to serve as basis for other policies, standards and procedures.

2. Provide guidance on actions regarding Information Safety Management that the Management of Empresas Copec may undertake and commit to, so that they are aligned with business objectives.

2. SCOPE

This Information Security Policy applies to all information assets of the Company, in any format whatsoever, as well as the processes and systems that support them.

Therefore, it is the responsibility of all employees, suppliers and customers of Empresas Copec, as appropriate, to know, observe and fully enforce the provisions of this Policy.

3. DEFINITIONS

3.1 Empresas Copec

It refers solely to the parent company; it does not include its affiliates and associates.

3.2 Partner or Employee

Any person who has a contractual relationship with Empresas Copec, whether it is permanent, on a fixed term or a contract worker.

3.3 Information Asset

Each and every thing that holds value and is important for Empresas Copec, whether documents, systems or individuals. All those elements relevant for the production, issuance, storage, disclosure, display and retrieval of information of value to the institution. It has three levels:

- Information itself, in its many formats (paper, digital, text, image, audio, video, etc.).
- Devices / Systems / Infrastructure supporting this information.
- People who use the information, and are aware of business processes.

3.4 Policy

Guideline or general guidance formally expressed by the Management of Empresas Copec.

3.5 Standard

General provision that emerges from the Information Security Policies, establishing obligations, restrictions, prohibitions or other expected behavior.

3.6 Procedure

Chronological sequence of actions linked together, with the purpose of performing a specific activity or task within the scope of Information Security controls.

3.7 Risk

The possibility of an event that may adversely affect the pursuit and achievement of the objectives of Empresas Copec. It is measured by combining the consequences of such event (impact) and its probability of occurrence.

3.8 Threat

Potential source of an unwanted incident, which may result in damage to a system or process.

3.9 Vulnerability

Weakness of an asset or group of assets that may be brought forth by one or more threats.

3.10 Information Security Event

Suspicious activity or series of activities that call for deeper analysis, from the perspective of Information Security.

3.11 Information Security Incident

Information Security Event or series of events, unwanted or unexpected, that compromise Information Security and threaten the business operations.

3.12 Confidentiality

Property of the Information, which determines that it may only be accessed by duly authorized individuals, entities or processes.

3.13 Integrity

Property of the Information, according to which it may only be modified, added or eliminated by persons or systems authorized for each process, so as to safeguard the accuracy and completeness of information assets.

3.14 Availability

Property of the Information that makes it timely available and usable by duly authorized persons or systems, in the format required for its processing.

4. POLICIES

4.1 Employees' Duty

All employees of Empresas Copec have the duty to constantly contribute to Information Security, in a proactive manner, abiding to and complying with the policies, standards and procedures on Information Security, and must be concerned about knowing and understanding the contents thereof.

4.2 Applicability to Third Parties

Security Information Policies will be disclosed, and compliance be required, to third parties with whom Empresas Copec interacts, such as customers or suppliers who perform works for the company, thereby incorporating the appropriate clauses into the respective contracts.

4.3 Information Security Policies

Specific Information Security Policies of Empresas Copec are established and regarded as part of the regulatory framework on Information Security, according to the items defined in ISO 27002, namely:

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operation Security
- Communication Security
- System Acquisition, Development and Maintenance
- Suppliers Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity Management
- Compliance

4.4 Structure of the Regulatory Framework for Information Security

Information Security documentation of Empresas Copec is divided into:

- Policies
- Standards
- Procedures

4.5 Policy Categories

Information Security Policies are grouped into three topics:

a. Policies Related to Information Assets and Technical Requirements

Empresas Copec, with the purpose of defining the criteria applicable to information assets and technical safety requirements appropriate for the Company, has policies on: asset management, physical and environmental security; cryptography; communications and operations management; access control on information systems acquisition, development and maintenance; incident management; and on supplier management.

b. Policies related to Human Resource Management

Empresas Copec, in order to encourage the proper use of information and the systems that support it, has Information Security Information policies related to Human Resource Management. Such policies, to the extent that they relate to obligations or prohibitions affecting employees of Empresas Copec, should be aligned, among other things, with existing labor rules; Employment Contracts; the Internal Rules of Order, Hygiene and Safety; the Code of Ethics; the Crime Prevention Policy and the Information Management Manual, among others.

c. Policies Related to Compliance

Empresas Copec has Information Security policies regarding compliance with legal, regulatory or contractual provisions. Based on these policies, control measures shall be implemented, taking into account legal risks of breach or noncompliance, which are not only corrective, but mostly preventive.

4.6 Security Organizational Structure

Empresas Copec, in order to assign the roles and responsibilities required for the management of Information Security, has organizational policies and standards, essential to ensure a proper Information Security management within Empresas Copec. Furthermore, the main body responsible for monitoring and managing these policies and standards is the Committee for Information Security.

4.7 Approval and Disclosure of Policies

The specific policies of Empresas Copec, as well as any amendments thereto, shall be approved by the relevant parties, as defined in the agreements of the Committee on Information Security.

All Information Security Policies shall be communicated to the partners and employees of Empresas Copec, in a duly, accessible and understandable manner, leaving a record thereof.

4.8 Penalties

Failure to comply with the policies of Empresas Copec shall grant it the right to exercise any civil, criminal and administrative actions as may apply and, if appropriate, to proceed with the termination of the respective contracts.

4.9 Validity

The Information Security Policies and all the contents thereof shall be effective as from its date of approval and implementation, and will have an indefinite validity term, as long as the Board of the Company does not resolve otherwise.

APPROVAL AND AMENDMENTS

This document was approved by the Board of Directors of the Company in its meeting on November 26, 2015. If amendments are made, the date of the Board meeting in which such amendments are approved shall be put on record under this heading.

DISCLOSURE MECHANISMS

The complete and updated text of this policy will be disclosed and remain available to interested parties on the Company's website (www.empresascopec.cl).