



## **INFORMATION SECURITY POLICY**

### **FRONTERA ENERGY CORPORATION AND SUBSIDIARIES ("FRONTERA" or the "CORPORATION")**

#### **1. INTRODUCTION**

The information security policy (the "**Policy**") is an action framework whose purpose is to protect strategic information as well as the assets related to its creation, processing, storage, transmission, elimination or destruction for the entire Corporation and its subsidiaries.

The scope of this policy is protection of the mission critical infrastructure at Frontera's different production fields to guarantee that cybersecurity risks are managed in a structured and adaptable manner according to the changes of the technological and business environment.

Information assets include but are not limited to: processes, information (electronic, physical and any other type of information that originates from non-conventional means), persons, hardware, software, intellectual property, databases, services, unstructured information and control systems.

#### **2. DECLARATION OF THE INFORMATION SECURITY POLICY**

Frontera recognizes information as an asset that is of the utmost importance for the business, that allows it to achieve its objectives and maintain its competitive advantage, as such, we must generate the mechanisms necessary to protect it guaranteeing its integrity throughout time.

Information, throughout its life cycle, must be available, be unambiguous and catalogued in a manner that is consistent with its value, importance and the privacy required by its nature.

The Security policy and the Guidelines that support it define the following basic principles:

- We generate a culture aimed towards the secure use of information and the means that support it by employees, contractors and third parties, through the strengthening of knowledge and the development of competencies that allow mitigation of cybersecurity risks; as well as strengthening of the necessary technical capacity.
- From the Senior ITS Office and the Information Security Office we developed together with all areas in the Corporation processes to manage risks to allow us to identify and assess the different threats and vulnerabilities which information may be exposed to, including the technological platform and the industrial control systems. As a result, control and treatment measures that support the achievement of the Corporation's objectives are defined and implemented.

- We promote the adequate use of the technological resources provided by Frontera, which must be used only to carry out the purpose for which they were assigned; said resources must be used in a way that protects copyright and intellectual property and in no case may be used for any illegal activity or use that is not aligned with our corporate values. In addition, Frontera reserves the right to access the corporate assets and the technological services provided by the Corporation.
- We comply with all laws, regulations, and contractual requirements, as well as with the internal guidelines provided to manage confidential information and/or personal information guaranteeing its integrity, confidentiality, and access only by authorized personnel.
- All directors, officers, employees (temporary, fixed term or permanent), consultants, contractors, subcontractors, interns, seconded staff, remote-workers, apprentices, or any other person that works for (hereinafter “**Frontera Personnel**”), regardless of location, must be discrete when speaking about their work at Frontera, especially when meeting at public places or when surrounded by others who should not have access to this type of information.
- For execution of services, Frontera Energy contractors, subcontractors or third parties, must comply with **A-SCM-CC-007 INFORMATION SECURITY ANNEX** and the confidentiality clauses defined in the contracts.
- Projects developed by the Corporation that affect information security or the technological or mission critical platforms, must include, from their initial stages, the assessment of aspects related to the information security architecture in accordance with the defined guidelines.
- Frontera has defined monitoring and control mechanisms to minimize impact generated by information security incidents. All Frontera Personnel must report information security or cybersecurity incidents, suspicious events, breach of regulations and improper use of assets they identify which may affect the Corporation.
- Define, implement, operate and continuously improve an Information Security Management System, fostered by the Corporation's senior management.

### 3. SCOPE AND MONITORING

Compliance of this policy is mandatory for all Frontera Personnel, regardless of location.

The board of directors of the Corporation (the “**Board**”) is the body responsible for the approval hereof and this policy shall be reviewed by the Information Security Office according to a programmed schedule to identify opportunities for improvement. Unscheduled reviews shall occur as a consequence of material changes to the business practices, changes to the technological infrastructure or due to new legal or regulatory requirements that impact information security.

### 4. COMPLIANCE

In case of breach, Frontera Energy Corporation reserves the right to apply the disciplinary measures and sanctions defined by Labour Laws, the Internal Work Rules, the Code of Business Conduct and Ethics or as defined by the terms and conditions of contracts entered into with Frontera Personnel.

All Vice presidents, Directors and Senior Managers are responsible for guaranteeing compliance of the Information Security Policy in their teams.

## **5. VALIDITY**

This Policy was updated effective October 10, 2022.

## **SCHEDULE A: Key Rules for Information Security Compliance**

Taking into account the evolution of technology, the ease with which information can be managed and the advance of collaborative work, the confidentiality and integrity of information becomes more relevant and each collaborator at Frontera is responsible for avoiding risks that may impact the organization's reputation or the loss of information.

We remind you that as users of the information and technological platforms provided by Frontera you must consider, at least, the following rules:

1. Do not use technological solutions that require licensing without prior authorization of ITS. All licenses must be authorized by the company and managed by ITS.
2. Do not deliver or publish, under any circumstance, confidential internal use information to third parties without proper approval. For example, databases with personal information, ongoing projects, reserved financial information, corporate images, among others.
3. Inadequate use of external devices that may risk the security of information, such as USB, external hard drives.
4. Loaning passwords to access the network or corporate information systems is not allowed.
5. Do not share virtual workspaces with unauthorized personnel. In addition, storing and sharing information on personal clouds, such as personal Dropbox, OneDrive and Google Drive accounts, is prohibited.
6. Be careful with external emails, webpages, messages or networks that may expose the company to cyberattacks.
7. Permissions assigned over corporate information are the responsibility of each user, who must guarantee proper access and use of this information.

For compliance of the above rules all collaborators have the support of the Senior ITS Office and the Information Security Office, who will provide guidance on management thereof.

Notwithstanding the foregoing, we remind you that compliance of these rules is mandatory, and breach thereof may cause the application of disciplinary measures and sanctions, as per Labour Laws, the Internal Work Rules and the Code of Business Conduct and Ethics.