1 Table of Contents

Content

2 Purpose

This policy establishes the guidelines to ensure security of YPF operations[1], persons and assets against any type of internal or external threats, in every area, minimizing their impact on the Company's goals, strategy, operations and performance, or its image, persons and communities, the market, the environment and other stakeholders.

3 Main Considerations

In compliance with the Code of Ethics and Conduct and other corporate policies associated , we seek to uphold corporate values, specially the value "We prioritize security: we protect people and their environment, we protect the company's information, assets and reputation".

In line with the values we defend, in YPF we are committed to protecting our assets in full compliance with the highest industry standards and the best internationally recognized practices, the various contractual agreements to which the Company is subject, provincial, national and international legal and regulatory requirements, and in particular, the UN Declaration of Human Rights, the Guiding Principles on Business and Human Rights and the Voluntary Principles on Security and Human Rights.

In order to comply with the legal requirements and the Company's business objectives, the following criteria have been defined as the Company's core principles:

- Compliance.
- Availability.
- Confidentiality.
- Integrity.

All persons having access to YPF information are responsible for understanding, monitoring and complying with this policy and its regulatory framework. Besides, YPF ensures it applies this policy and its regulatory framework to third parties' information.

[1] *This document establishes the security guidelines to protect operations, in terms of Physical Security and Cybersecurity , together with the current rules and regulations*

This Policy will be revised and updated on an annual basis and shall be approved by the CEO.

As an integral part of this Policy, the Glossary of Corporate Security Terms will establish the terms and definitions used in this document.

4 Policy

YPF's operations are based on core or essential values that govern all corporate and business decisions.

Under this Policy, subject persons are committed to:

- Ensuring compliance with the Regulatory Framework (regulations, procedures, security standards, specifications, manuals and/or instructions) arising from this Policy, by everyone in the organization.
- Complying with the training and awareness plan.
- Defining and implementing efficient Cybersecurity and Corporate Security management processes, aligned with Corporate Risk Management, adopting accepted industry standards and best practices.
- Acting jointly with organizations and/or external entities required to develop risk control alternatives.
- Conducting the necessary internal investigations to clarify security events or incidents and/or possible deviations from the Code of Ethics and Conduct and other pertinent regulations, under the principles of objectivity, completeness, relevance, accuracy and timeliness, and reporting the findings to the pertinent parties.

Failure to comply with this Policy, as well as Cyber and Corporate Security regulations, procedures and standards arising therefrom, poses risks to the Company's assets, and may also result in the respective disciplinary sanctions, pursuant to section *Measures to be applied in case of breach of the policy of the "Code of Ethics and Conduct".*

Negligence in the protection of information that may result in theft or disclosure of such information, due to an act or omission, resembles an economic fraud and will be referred to the Ethics Committee for it to assess the responsibilities and fiduciary impact.

4.1 Responsibility Statement

Through this Responsibility Statement, YPF employees and other subject persons undertake to comply with the civil responsibilities defined under Cybercrime Law No. 26,388, acting in a professional and responsible manner.

All subject persons bound by this Policy undertake their respective duties and commit to the following:

1. To sign this Policy annually.
2. To be informed and responsible for cybersecurity and corporate security at YPF and to be aware of the importance of this aspect .
3. To ensure the proper use, treatment and protection of the Company's assets, including information assets and the systems that transport, store or process such information.

4. Understanding and accepting that access credentials to assets and Systems are personal and non-transferable, and that this also applies to any profile created for a third party to act on behalf of the Company.
5. Applying Cyber and Corporate Security regulations arising from this Policy, particularly the Classification of Information Assets, to any information we generate, transport, store, print or distribute whether digital written or through voice communications
6. Accepting, complying with and enforcing the confidentiality agreements defined by YPF, ensuring us that they are also respected when access to company information is allowed to third parties.
7. Using, in a reasonable and secure manner, the information assets necessary to perform the work designated by the Company, and warning of any threat or improper use.
8. Properly defining segregation of duties in all business processes so that nobody can individually control several key aspects of a process.

4.2 Company's Commitment

The Company, through its designated employees, is bound and responsible for:

1. Implementing the Cyber and Corporate Security policy and its regulatory framework.
   All members of the Board of Directors, the CEO, Vice Presidents, Executive Managers and General Managers of the YPF Group companies are directly responsible for implementing the Cyber and Corporate Security policy and its regulatory framework, ensuring compliance by their employees.
2. Assessing cyber security events and corporate security /cyber security risks, and ensuring that the risks and events associated with asset security are identified, communicated, accepted, mitigated or remediated.
3. Maintaining the inventory of Technological Assets (IT/OT) associated with the company's processes.
4. Protecting the company's assets, ensuring compliance with the legislation in force and commitments with third parties.