1 Table of Contents

Contents

2 Purpose

This regulation establishes the guidelines to ensure the confidentiality, integrity and availability of information and information assets at YPF, managing the associated risks and minimizing the impact in face of the potential materialization of internal or external threats.

3 Main Considerations

It focuses on orienting staff regarding the objectives to implement and the guidelines to comply with in order to manage Cybersecurity at YPF reducing the risks to which IT and information assets are exposed to levels acceptable to the Company.

Guidelines are established in compliance with the national and international legal frameworks, as well as recognized standards to protect the interests of the Company and its investors.

It´s based on the best practices to adequately manage Cybersecurity and includes Information Technology (IT) and Operations Technologies (OT), which must be operated safely in order to ensure business continuity and continued improvement in processes.

This regulation shall be disclosed for internal awareness and compliance by every staff member of the Company and shall be easily accessible.

Failure to comply with this regulation poses legal and disciplinary risks including civil and criminal sanctions as well as the possible termination of the labor or contractual relationship.

4 Content

This document describes the provisions related to all IT resources and systems of the Company.

4.1 Cybersecurity Organization

4.1.1 Cybersecurity Internal Organization

Defining the structure to manage Cybersecurity within the Company and setting a framework to control their implementation.

Ensuring the signing of the confidentiality commitment by all members of staff and third parties related to the Company.

4.1.1.1 Cybersecurity roles and responsibilities

The Cybersecurity Management defines the roles and functions required for the correct and efficient administration, management, operation, control, and monitoring of the implemented mechanisms to protect the Company's IT and industrial assets.

4.1.1.2 Segregation of duties

Privileged or sensitive tasks must be separated from similar ones to minimize the risk of privilege abuse and enhance control capabilities, in accordance with the principle of segregation of duties.

4.1.1.3 Contact with authorities and special interest groups

The chain of communication with authorities is determined by the impact of a cybersecurity incident, according to the classification of the incident. These incidents should be notified immediately to the personnel involved within the organization, and it is recommended to keep updated on the best practices and regulations through membership and subscription to forums or special interest groups.

4.1.2 Mobile Devices and Remote Work

Considering the risks associated with unprotected environments, it is necessary to ensure the secure management of information when using mobile devices and working remotely by applying appropriate protection measures to safeguard the technological platform.

The security measures must be applied according to the Company's policies, rules and procedures. This includes establishing monitoring and control mechanisms and maintaining a specific audit log for these accesses under periodic reviews.

The Company´s information and infrastructure must be protected when using mobile devices, as this increases the risk of incidents due to loss, robbery or theft. Therefore, the staff using them shall be made aware of the risks and procedures must be established to promptly report any incidents, thus mitigating the risks to the information systems.

4.2 Security of Human Resources

All employees, suppliers and contractors from the start until the end of their employment and/or business relationship, are responsible for handling the information used in the performance of their duties. The information is the exclusive property of the Company except in cases where it contains personal data, in accordance with Personal Data Protection Law 25.326.

All employees are subject to the security provisions established by the Cybersecurity Management and must return the assigned assets upon termination of their employment and/or business relationship. During this period, they must comply with the Company´s "Code of Ethics and Conduct" and the "Cybersecurity and Corporate Security Policy" while the cybersecurity Management Provides support in these aspects.

4.2.1 Cybersecurity Training and Awareness

All the Company's staff and, when required, contracted personnel and third parties performing duties in YPF, shall be trained and updated periodically on the Cybersecurity policy and its related rules and regulations. Highlighting the security requirements and legal responsibilities. An strategic plan of Cybersecurity Awareness adapted to the business necessities it´s stablish Cyber Risks Management

4.3 Cyber Risks Management

4.3.1 Managing Cyber Risks

Establishing the management methodology to identify, assess and manage Information Technology (IT) Cyber Risks, taking into account the disclosure of information in face of the threats to which the Company is exposed, in order to ensure the highest possible levels of confidentiality, integrity and availability of the data and information processed and/or stored in the systems and devices involved, for the purpose of minimizing the level of risk, considering the main controls and good practices.

4.3.2 Manage Industrial Cyber Risks (OT)

Define a methodology for Cyber Risk Assessment (CRA) to analyze and protect industrial systems against cyber threats, maximizing availability and safeguarding the confidentiality and integrity of information in Industrial Systems and reducing risks to tolerable levels by YPF S.A.

4.4 Asset Management

Assets shall be managed and protected effectively and classified as per their criticality for the business, taking into account its functions and the rules and regulations applicable.

4.4.1 Ownership of Information Assets

IT asset must have an assigned owner who ensures compliance with their identified, defined, and recorded responsibilities. The owner must ensure that assets are correctly classified, inventoried, and protected to prevent their exposure, loss, or corruption during the established lifecycle.

4.4.2 Information Asset Classification

Control and ensure confidentiality, integrity and availability of the information and data processed and stored in IT assets through their correct identification and classification to avoid their exposure, loss, or corruption.

4.4.3 Handling Information in Removable Media:

Establishing guidelines to manage the media according to the Company's classification scheme, in order to avoid the alteration, transfer, disclosure, elimination or destruction of the information stored in these physical or digital devices, used by employees and third parties.

4.5 Access Control

4.5.1 User Administration in Technological Platforms

Establishing general guidelines to ensure the appropriate administration of user access to YPF information technology resources and Cloud Computing platforms.

4.5.2 Managing Service Accounts

Establishing the activities for the correct management of the Service Accounts used in YPF information systems, considering the main control and good practices, highlighting the following, among others:

- Password safeguard.
- Use limitations.
- Nomenclature.

4.5.3 Managing Users with Broad and Emergency Privileges

Establishing the required actions for managing users with broad and emergency privileges implemented in the systems of Password Management, including all environments (Production, Development and Testing).

4.5.4 Password Security

Establishing and standardizing the security password settings for operating systems, databases, communication equipment, base software, and applications.

4.6 Cryptographic Control

Establish the necessary regulatory and technical controls to manage cryptographic keys throughout their lifecycle, as well as encryption mechanisms to protect data at rest and in transit. The objective is to ensure the integrity, confidentiality, non-repudiation, and authentication of the Company’s information assets.

4.7 Physical and Environmental Protection:

4.7.1 Secure Areas

The data processing centers (DPCs) shall be located in secure areas, protected by the security perimeters defined and with strict access controls in compliance with the Company´s regulations.

The physical spaces intended to contain the Company’s information assets and IT infrastructure shall be protected and classified as restricted access areas based on the value, classification of the information and level of criticality of the services they provide to ensure business continuity.

Any third party's access to restricted areas with IT assets shall be strictly controlled by the staff in charge of the area security and the asset owner requiring the third party's access.

The areas where information assets are located shall be protected against natural and/or environmental risks and threats.

4.7.2 Equipment in DPCs

It is important to control environmental parameters associated to the equipment in DPCs, thus ensuring the correct operation of processing equipment minimizing any potential interruption of related services.

The equipment shall have a periodical maintenance plan, which may involve transportation and location outside secure areas, therefore, these processes shall be performed under strict security rules and considering the classification of the information stored therein and assessing transportation risks and final disposal.

4.8 Operation Security

4.8.1 Environment Separation

Establishing the general guidelines that allow ensuring implementation of new software developments or updates of the ones used in a controlled environment with an appropriate separation of duties, and minimizing associated risks (unauthorized changes, development errors, implementations that have not been tested, accidental updates, operating interruptions, etc.), considering the main controls and good practices.

4.8.2 Antimalware Security

Establishing that requirements in relation to antimalware must be met for all the client's equipment and servers connected, either logically or physically, to the Company's IT systems or networks, in order to prevent and effectively detect malicious intrusions, avoiding their propagation and replication.

4.8.3 Log Reviews

Systems and network components should be monitored to record all user activities such as exceptions, failures and information security events.

4.8.4 Data Network Scanning

Establish the general guidelines for the execution of vulnerability scanning activities on technological assets of the Company and third parties.

4.8.5 Managing Vulnerabilities

Establishing step-to-step processes to identify, analyze, remedy and validate proactively the vulnerabilities to maintain the Company's security levels.

4.8.6 Managing Changes

In order to minimize the risks associated to alteration of information systems, strict controls shall be run during change implementation enforcing the application of formal procedures. Thus, ensuring compliance of the security and control procedures and respecting the segregation of duties.

4.9 Security in Communications

4.9.1 Security in Internal and External Communications

Establishing general guidelines to ensure appropriate information protection in data transfer processes in internal and external networks of IT systems, considering the main controls and good practices.

4.10 Acquisition, Development and Maintenance of Information Systems

4.10.1 Security for Software Acquisition or Development

Establishing security guidelines and controls to be executed at the time of acquiring or developing software in order to reduce all internal and external risks due to unauthorized access and data losses to an acceptable level.

4.11 Managing Cybersecurity Incidents

The Company's Cybersecurity Management establishes responsibilities and procedures for responding and managing information security incidents, as well as proactive mechanisms to identify security breaches, develop recovery plans, and enhance organizational resilience. Incidents are documented and preserved to meet legal requirements and potential investigations.

In addition, criticality thresholds for incident response are defined and cyber fraud is managed in accordance with the economical and reputational impact on the Company.

4.11.1 Security Events Monitoring

Establishing the general guidelines to monitor access to resources and critical events in order to identify and follow up any probable security incident or abnormality in information systems, for the purpose of mitigating internal and external risks due to unauthorized access, information loss and damage.

4.12 Security in platforms and applications

4.12.1 Database Security

Establishing general security guidelines for databases setup by limiting the privileges of administrative users. Highlighting the designation of specific roles, installation procedures, account and permissions management, event auditing, limitations and safeguard and updates.

4.12.2 Security in Applications

Establishing the general guidelines that allow guaranteeing confidentiality, integrity and availability of information systems, as well as ensuring their correct control and auditing, in compliance with external policies and lawsHighlighting controls as owner designation, environment separation, infrastructure restrictions, secure design environments, minimum access to resources, cloud platform, security requirements and continuous logging and monitoring.

4.12.3 Security in Operating Systems

Establishing general guidelines for the correct setup of the servers' operating systems, end devices and virtual machines. Highlighting controls as remote access, account management, auditing, event logging, network configuration, threat protection, safeguards and updates, as well as obsolescence management, among others.

4.12.4 Relation with Providers

The relation with the Company's providers shall be managed through service provisions agreements whereby all security aspects and information security requirements shall be established and agreed upon.

The officers responsible for the legal and purchase areas or those who manage agreements with providers shall ensure that the levels of security established by the Company are defined and agreed upon in such agreements.

The mechanisms to be implemented includes information security with providers security management in service agreements risk management requirements, managing delivery of services provided, follow-up and revision of services and managing changes in services provided.

4.13 Information Security in Business Continuity Management

It is required to implement the mechanisms and strategies established to the development, evaluation and activation of contingency plans ensuring restoration of the critical services of the business core processes.

Owners of information assets are responsible for creating a contingency plan and ensuring all the staff participating in its execution are aware of its content so that they may apply it whenever required for business continuity.

The mechanisms to be implemented includes continuity planning, documentation and implementation of processes, procedures and controls, revision and valuation of the continuity and the implementation of redundancy to ensure availability.

4.14 Compliance

4.14.1 Legal Compliance or Conformity

Establishing the general guidelines that allow ensuring that the information and IT assets used in the Company comply with the rules and regulations in force in Argentina, applicable to the obligations assumed by public and/or private instruments by YPF, and with YPF internal policies, regulations and procedures reaching such assets.

In addition, stablishing guidelines for planning audit activities to verify operating systems and minimize business process interruptions.

4.14.2 Digital Signature Security

Establishing the general guidelines for the digital signature use and validation, in order to ensure security of the documents and acts signed using this tool, considering the main controls and good practices.

4.14.3 Personal Data Security

Establishing the security measures to be implemented in files, records and bases containing personal data considered sensitive data, in order to ensure their appropriate protection, in accordance with the Data Protection Law No 25.326 and it´s regulations considering the main controls and good practices.

4.15 Security in Industrial Systems (OT)

4.15.1 General Standard on Industrial Cybersecurity

Establishing general guidelines based on Cybersecurity for the Company's industrial operations, considering:

Establish the necessary guidelines to ensure the availability of Industrial Systems and protect the availability, confidentiality, and integrity of the processed and/or stored data by adopting prevention and control measures.

4.16 Cloud Security

Establishing the cybersecurity governance implementing a standardization and setup model for the security of all the applications and services residing in the Cloud environment, defining the main functions and responsibilities of the following areas:

The Company establishes security and responsibility criteria for managing cloud services, both for IT and OT environments, in collaboration with providers and third parties. Industry standards and applicable legislation are considered to protect the Company's interests.

The security aspects considered include data recovery, protection against data loss, prevention of human error, and reduction of the impact of potential security breaches.

The concepts of the regulations (IaaS, PaaS, or SaaS) are differentiated, and efforts are made to minimize the impact of potential risks on information and industrial (OT) systems.