1 Table of Contents

Contents

2 Purpose

To define the categories of classification, protection, correct use and handling of information to ensure compliance with the core pillars of information security, data Integrity, Confidentiality and Availability throughout its lifecycle.

3 Main Considerations

This regulation is mandatory throughout the whole lifecycle of the information asset, i.e., from its generation, storage, distribution, operation to its final disposal and/or destruction.

Failure to comply with this regulation by YPF's own staff, its consultants or external service providers rendering services for YPF might result in the immediate loss of access permissions to information assets and sanctions consistent with the damage that may or might have been caused.

Failure to comply with any of the provisions of this regulation may expose the Company to:

- The loss, theft, manipulation, modificación, elimination, destruction or unathorized copy of sensitive information assets.
- The public disclosure of sensitive information assets of YPF.
- Severe financial and economic losses.
- Loss of prestige for YPF.

By default, unclassified assets will be considered as YPF-Confidential[1].

In line with the "General Standard on Industrial Cybersecurity" and in relation to industrial system Cyber Assets, all Support Files will be classified in the same category as the industrial Cyber Asset they belong to.

[1] *Establishing a term of 18 months from its publication to confirm or adjust the classification.*
If a classification adjustment were required, it shall be scheduled within this term and performed by December 31, 2023.

3.1 General Considerations on the Use of the Company's Information

- Employees are not recommended to open a message from the Corporate Electronic Messaging Service when the sender is unknown, except in cases of force majeure, where given their role in the Company, they would not be allowed to do so.
- It is not allowed to forward or redirect emails automatically to personal email addresses or any other email address not belonging to YPF. Where this is required due to a business need, the specific procedure for exception management must be followed.
- An information asset classified as YPF–Secret or YPF-Confidential may not be read, discussed or disclosed in any manner in public places where it may be compromised to third parties. This includes conversations on the telephone, social media or in presence of devices / applications compiling voice information.
- Information may only be shared with staff with functional competence on the subject, avoiding its transmission to anyone who does not need it due either to their role or their authorization level to access such information.
- Any information of a non-public nature shall be considered as restricted access information (YPF-Secret, YPF-Confidential or YPF-Private).
- With the aim of preventing information leakage, ensuring protection against possible attack vectors and safeguarding information, access to storage devices through USB, Airdrop and Bluetooth ports allowing to remove information from the organization will be restricted on information assets. In the exceptional case of transporting information on USB storage devices, please refer to the requirements established by the Cybersecurity Management.
- Passwords shall not be stored in plain text files.
- The information shall be protected throughout its lifecycle in accordance with its classification category, i.e., from its generation, storage and distribution to its final disposal. The classification assigned to information assets need not remain unchanged over time. Circumstances such as information no longer being sensitive or critical after a certain time, changes in the organization, changes in the economic or legal context, changes in the technological infrastructure or changes in existing threats demand a regular revision of the classification.
- An information classification category may only be reduced or increased with the authorization of the Owner of the classified information asset or the highest-ranking executive of the employee's business line.

3.2 Improper Access to Employees' Data

Employees should manage information ensuring its proper classification and processing to guarantee its confidentiality and integrity, and preventing, among other risks, its disclosure. Supplementarily, the "*Cyber and Corporate Security Policy*" establishes the commitment and responsibility to use assets in a reasonable and secure manner, and to preserve and warn about any threat or improper use of those assets.

If an employee identifies that he/she is authorized to access other employees' data (employees' personal data, financial data and performance and goal-based assessments) in an improper manner, he/she shall avoid such access, ensure such data are not disclosed and that the identified vulnerability will not be disseminated, immediately reporting the incident to the "CRMC@ypf.com" email address for the activation of the Protocol for Improper Access to Employees' Data of the VP of People and Culture, and acting in compliance with the "*Cyber and Corporate Security Policy*" and the "*Code of Ethics and Conduct*" of YPF.

4 Contents

This edition formalizes the classification of information as “Personal” and existing categories are divided into two groups to facilitate their interpretation.

This classification is grouped as follows:

- **YPF Group Internal / External Use** : YPF-Private, YPF-Confidential and YPF-Secret.
- **YPF Group Public Use**: YPF-Public.
- **Personal**[2]

4.1 Cyber Risks and Compliance

Information assets shall be classified in order to indicate their need, priorities and risks associated with their exposure, their unavailability and therefore, the level of protection that should be provided in accordance with the regulatory framework, or the lack and/or loss of data and the level of protection in terms of confidentiality, integrity and availability.

The Company’s information assets are grouped into:

4.1.1 Structured: Information associated with applications and/or specific business processes[3]

Information contained in the information systems approved by the Company or electronic or printed documents supporting specific processes of the different business units.

4.1.2 Unstructured: Information managed by YPF employees in electronic or printed documents that are not included in the previous definition

Information directly or indirectly managed by the user or a group of users with a business interest. It may be processed from their computer, mobile device or any another processing method, such as the Corporate Electronic Messaging Service and, Teams, among others, and which is typically stored or shared in the form of a file and needs to be preserved or shared with other organization members or third parties. This information may be found in formats such as Power Point, Word, Excel, Autocad, PDF, LAS, LIS, DLIS, SEGY, SHP, among others.

4.1.3 Preventing information leakage

In the event of a presumed information leakage, each employee of the Company, consultant or external service providers rendering services for YPF is obliged to immediately report the event to the CRMC area 24/7 through the Corporate Electronic Messaging Service at CRMC@ypf.com.

4.1.4 Classification Categories

4.1.4.1 YPF Group Internal/External Use

The classifications and labels contained in this group are described below.

a) YPF-Secret

Information that provides a competitive advantage to the organization, or which is essential for the technical or financial success of a specific product, service or project. The unauthorized dissemination of this

[2] *The classification of information as Personal shall be applied to purely personal information that is not used for business purposes (as set out in section 5.2.4).*

[3] *If the information is not categorized according to the criteria set out in section 5.1.1, either because it does not fall under such criteria or the classification process has not yet been completed, it shall be classified as established in section 5.1.2.*

information may have a high impact on the continuity of the business value chain and might severely damage to the Company's interests. Its access is only for authorized staff in compliance with the rules and regulations in force.

- **Label**: Document: **YPF-Secret.**

b) YPF-Confidential

Information which, if disclosed, could cause adversely affect global business objectives or some of YPF's activities.

- It may also be used for information classified as "YPF – Confidential Habeas Data".
- **Label**: Document: **YPF-Confidential.**

c) YPF-Private

Information available to Company employees and third parties (e.g., contractors) as part of the regular course of business. It is disclosed when the information needs to be known for the Company to operate. Its unathorized disclosure might affect the accomplishment of particular objectives of certain areas of the Company.

- **Label**: Document: **YPF-Private**

4.1.4.2 YPF Group Public Use

The following are the types of classifications and labels contained in this group.

a) YPF-Public

Information that freely flows inside and outside the Company.

Examples of YPF-Public information include:

- Marketing brochures approved for dissemination.
- Press releases.
- External job searches.

- **Label:** Document: **YPF-Public.**

4.1.4.3 Personal

The types of classifications and labels contained in this group are indicated below.

a) Personal

Information created or used by whom classifies the information, for non-professional purposes, which is subject to the following conditions:

- On creating or using the information for the purpose mentioned above, the user shall not breach their confidentiality duty (both towards the Company and third parties) or generate incompatibilities with their functions in the Company.
- The information shall not fall under the following classifications: "YPF–Secret", "YPF–Confidential", "YPF–Private" o "YPF-Public".

The person classifying the information may decide not to apply the "YPF Categories – Personal Data" section and, instead classify the information as "Personal" when, given the conditions mentioned in the previous paragraph, the information only contains Personal Data which:

- Exclusively refers to the person responsible for classifying the information (for example, personal procedures, pay slip, medical studies, photographs, etc.);
- Exclusively refers to their immediate family members or dependents (for example: procedures related to them, etc.);
- Exclusively refers to any other person who has granted an express or implied consent for the specific purpose (for example, communications with other users with a non-professional specific purpose, etc.);
- Is publicly available by the law or the will of third parties' (for example, news reports, bibliographies, laws, national and provincial regulations, etc.).

  For the use of this classification, the user shall take specifically contemplate the provisions of Regulation called "*Acceptable Use of IT and Information Assets".* Therefore, they may make personal use of the IT assets *made* available to them in a moderate and exceptional manner and may not classify any information whose storage in such files is prohibited as "Personal".

- **Label**: Document: **Personal.**

4.1.4.4 YPF – Personal Data Categories

In compliance with the Data Protection Law No. 25,326, this regulation establishes an identification scheme to be used within the Company that defines three security levels for the classification of the information subject to the aforementioned Law, which extends to the 5 YPF-Generic Categories already established.

Thus, information assets containing personal data should also be classified under any of the following categories:

a) YPF – Sensitive Personal Data

Assets containing personal data revealing racial or ethnic origin, public opinions, religious beliefs, philosophical or moral convictions, union membership or information related to health or sex life. Biometric data will only fall under this category when they allow to reveal any of the information types previously described.

This type of information will be handled as YPF-Secret Information.

b) YPF – Confidential Personal Data

Information assets containing any personal data falling under the two categories previously described. They include, among others, the following data: records of building entries and exits, records of incoming and outgoing calls, GPS location or similar information, certain banking and tax data, consumption preferences, etc.

This type of information shall be handled in compliance with the specifications provided for PF-Private information.

c) YPF – Public Personal Data

Information assets containing, exclusively, Personal data which YPF is authorized or empowered to disclose to the general public.

This information will be handled in compliance with the specifications provided for YPF-Public information.

When the information only refers to the Company, these data will not be considered "personal" for the purposes of this regulation, should not be classified under any of the three categories of YPF-Personal Data categories, and will only be governed by the YPF-Generic Categories.

If the information in any of the "Generic" classifications overlaps with any of the "YPF – Personal Data" categories, it shall be processed applying the more restrictive provisions.

Besides, under the "*Personal Data Security"* regulation, several security measures have been established, taking into account the higher or lower need to ensure the confidentiality and integrity of the information contained in the respective database, the nature of the data and the correct management of the risks to which they are exposed, as well as the higher or lower impact that file-recorded information failing to meet the appropriate integrity and reliability conditions would have on peolpe.