Global Security Policy

Telefónica, S.A.

Telefónica, S.A.
Approved by the Board of Directors of Telefónica, S.A. at its meeting of 26/11/2025

6th edition - November 2025

Change control

Edition	Date	Prepared by	Approved by	Modifications
1.0	01/04/2001	General Manager of Security	Board of Directors Telefónica S.A.	First version
2.0	27/07/2016	Global Director of Security	Board of Directors Telefónica S.A.	Complete update of the Policy
3.0	04/11/2019	Global Chief Security and Intelligence Officer	Board of Directors Telefónica S.A.	Update of document template and minor changes
4.0	29/09/2021	Global Chief Security and Intelligence Officer	Board of Directors Telefónica S.A.	Updating of document template, alignment of common texts in regulations, introduction of digital security concept, reporting on the state of the group's security to the Board of Directors by the Global Chief Security and Intelligence Officer and other minor changes.
5.0	25/10/2023	Global Chief Security and Intelligence Officer	Board of Directors Telefónica S.A.	Added reference to Risk Management Policy, mention of "supply chain security" and "commercial fraud", and other minor changes and clarifications.
6.0	26/11/2025	Global Chief Security and Intelligence Officer	Board of Directors Telefónica S.A.	Simplification of texts, updating of the concepts of digital security and co-responsibility, incorporation of the concepts of resilience and security measures, and reorganisation of the Security area.

Table of contents

Introduction **4**

Context 4

Purpose 4

Scope 4

Scope of application 5

Validity and revisions 6

Principles **6**

Security organisation **7**

Security framework **9**

Strategic plans **10**

Internal Audit **10**

References **10**

Introduction

Context

Telefónica is asserting its ambition to be a leader in the digital world, a scenario in which traditional threats are constantly being joined by **new, increasingly sophisticated threats**. As a consequence of the very digital nature of both the organisation and the business, the security effort is becoming more demanding than in other business sectors. Security is a material aspect for Telefónica.

Telefónica plays an important role in protecting the technological, industrial and commercial activity of business customers, the development and operation of critical infrastructures that provide essential services to society, as well as public organisations and government bodies.

Regulatory requirements and our customers' expectations of privacy and security are growing, becoming key attributes of the services we offer them. These **regulatory requirements** in the telecommunications and Internet sector, linked to national and international legislation, often have an unequal impact on the organisation, activity and business of the Telefónica Group in the countries in which it operates.

Purpose

This ***Global Security Policy***, inspired by the ***Telefónica Group's Responsible Business Principles*** [Ref. 3] and guided by national and international standards and regulations in this area, establishes and regulates the **general provisions and guiding principles** on security issues that are applicable to all Telefónica Group companies.

Scope

Security must be understood as an **integral concept that aims to preserve its assets and protect Telefónica's strategic interests and objectives**, both in its vertical organisation (including its business units) and in its transversal dimension (applicable to all its platforms): network infrastructure and assets, information technologies, products and services, and data; **safeguarding**, on the one hand, their **integrity** and protecting them, on the other, from potential threats that could damage their value, affect their **confidentiality**, impair their efficiency or affect their operability and **availability**, contributing to the resilience of the Telefónica Group. Likewise, security is one of the fundamental principles underpinning the ***Global Privacy Policy*** [Ref. 1].

Integral security encompasses physical and operational security (of people and assets), digital security, business continuity and crisis management, security in the supply chain, as well as **any** other **relevant** area or **function whose objective is corporate protection against potential threats that could cause damage**. In turn, the concept of digital security includes all the human resources, procedures, systems and elements necessary in the Organisation to preserve the capacity of the networks and

information systems, and to achieve the appropriate levels of efficiency and resilience to withstand any event that could compromise the availability, integrity or confidentiality of the data stored, transmitted or processed, or of the services offered by or accessible through such networks and information systems.

The **security provisions** applicable to the Telefónica Group's assets **will** also **apply to** its **collaborating entities** (providers, subcontractors, etc.) when their activity has an impact on those assets in the development of their business, at all levels of the supply chain and with a special focus on those entities that manage Telefónica Group or customer data.

Scope of application

This **policy is global in scope** and is **mandatory for** all **Telefónica Group** companies, without prejudice to the particularities deriving from the legislation applicable to each of them. For such purposes, the Telefónica Group shall be understood to be those companies in whose share capital **Telefónica, S.A.** directly or indirectly holds a majority of the shares, holdings or voting rights or in whose governing body it has appointed or has the power to appoint a majority of its members, such that it effectively controls the company (hereinafter, Telefónica, S.A. or any of the companies individually, the "**Company**" and, collectively, the "**Telefónica Group**" or "**Group**").

Telefónica, S.A., in its capacity as parent company of the group of which it forms part, is responsible for establishing the bases, setting the instruments and designing the necessary mechanisms for adequate and efficient coordination in matters of security among all the companies of its group, without prejudice to the autonomous decisions that may correspond to them, in accordance not only with the corporate interest of each of them, but also with the legal and fiduciary duties that are incumbent upon them.

It is the responsibility of the *Global Chief Security and Intelligence Officer* (GCSIO) to adopt the guidelines and measures necessary for their application, implementation, control and supervision.

Telefónica Group companies must disseminate and promote knowledge of and compliance with this policy, as well as provide the human, material, technological, organisational and budgetary resources necessary for its fulfilment.

Validity and revisions

This policy **came into force** on the date of its approval by the Board of Directors of Telefónica, S.A., on which date the policy previously in force was repealed.

It is the responsibility of the **Global Chief Security and Intelligence Officer** to perform the necessary powers of **interpretation**.

This document must be **reviewed** periodically, when deficiencies are detected in the text itself or in its application, and when organisational or process changes have led to its obsolescence, as defined in the ***Policy for the preparation and organisation of Internal Rules and other Organisational Documents of the Telefónica Group*** [Ref. 2]. In such cases, once approved by the Board of Directors, the revisions shall be reported to the Global Security Committee and published on the **Telefónica Group's Global Intranet**.

Principles

The **Board of Directors of Telefónica S.A.** considers people, information, technologies and the material resources that support them to be fundamental assets, which is why **guaranteeing their security is considered essential to Telefónica's strategy and an essential enabler of the Organisation's activity**.

By approving this **policy, the Board of Directors expresses its determination and commitment to achieve a level of security appropriate to the needs of the business which ensures the protection of assets in a homogeneous manner in all Telefónica Group companies.**

To achieve this, the Board of Directors relies on the **Security Organisation** as an integral security area committed to the protection of the Group's assets, in the context of the modern and dynamic nature of being a digital telco, and entrusts it with the effective and efficient management of physical security (protection of goods and people), digital security, business continuity and crisis management, as well as any other action that may contribute significantly to this end.

The security activities carried out by the different environments, organisational structures, asset managers and employees shall be governed by the following **principles**:

- **Principle of legality**: the necessary compliance with the Laws and regulations, both national and international, in force at all times in the territories in which the Telefónica Group operates shall be observed.
- **Principle of efficiency**: in order to achieve the required level of security in an efficient manner, the proactive and preventive **nature of** security activities **will be emphasised** over the passive and reactive nature. To this end, knowledge of potential threats will be prioritised, and the resulting risks will be analysed as part of an **intelligence process**. The purpose of this continuous intelligence process is

to **identify** and understand the **most relevant threats** affecting the organisation, with the aim of anticipating their action and evolution, protecting the Telefónica Group from their potential harmful effects, mitigating the damage caused by these risks to a level that is acceptable for the business.
In order to achieve a homogeneous level of security, a **Security Framework** is defined which will bear in mind the analysis of threats and risks, as well as the establishment of preventive, detection and corrective security measures in activities aimed at governing, identifying, protecting, detecting, responding and recovering.
Strategic plans shall be designed and developed to identify and prioritise the projects and budgets required to achieve these appropriate levels of security, minimising the security risks identified in the relevant analyses and maximising the effectiveness of the investment and resources employed.

- **Principle of co-responsibility**: In addition to the responsibility of the **Security Organisation**, **people** must preserve the security of the assets that Telefónica makes available to them, in line with the criteria, requirements, procedures and security technologies defined in the **Security Framework**, as well as the applicable laws and regulations on security. At the same time, they must use the assets strictly for the performance of their job activities and assigned tasks.

  The **Asset Owner** is the employee or position who decides on the purpose, content and use of the asset and is therefore jointly responsible for the security of the asset. He/she is also the Owner of the Risk associated with the asset, and therefore has the ultimate responsibility and authority to manage that risk and select a strategy consistent with the Company's acceptable level of risk, in accordance with the provisions of the ***Telefónica Group Risk Management Policy*** [Ref. 4]. The Security Organisation shall provide support to the Asset Owner in fulfilling its security responsibilities.
- **Principle of cooperation and coordination**: in order to achieve the levels of efficiency and resilience that Telefónica's business project requires, global action and the integral concept of security activities will be preserved together with the aforementioned requirements of anticipation and prevention, and cooperation and coordination between all Business Units and employees will be prioritised, in order to generate the appropriate synergies and strengthen joint capabilities.

  The Security Organisation **will coordinate the security responsibilities of the various structures** of the Telefónica Group, **encouraging cooperation between them**, and establishing global capabilities that will improve the effectiveness and efficiency of the protection of all assets.

Security organisation

The **Global Chief Security and Intelligence Officer** is the highest representative of the Security Organisation in the Telefónica Group. Its mission is the effective and efficient protection of the group's assets and will be oriented towards ensuring the viability of the

business. Her duties include leading the development and monitoring the implementation of the Regulatory Framework and global security initiatives, as well as promoting the Security Organisation defined in this policy. He/she must report to the Board of Directors or, where appropriate, to its Audit and Control Committee, as well as to a restricted Committee of the Executive Committee (Excom), with the frequency agreed by the Board of Directors or the Audit and Control Committee, to report on the state of the Telefónica Group's security and set out the *global strategic security plan* and the corresponding derived actions, in order to ensure an efficient level of security.

In the Security Organisation there are **local Security Officers**, whose duties and responsibilities will be defined and coordinated by the **Global Chief Security and Intelligence Officer**. Each Telefónica Group company will have one of these Security Officers assigned to it, depending on which is the most efficient and effective solution in each case. They will be proposed by the **Global Chief Security and Intelligence Officer,** and their appointment will be subject to the decision of the corresponding administrative or management bodies of the companies.

There shall be a **Global Security Committee** chaired by the **Global Chief Security and Intelligence Officer,** in which **local heads of security** and other areas may participate when deemed necessary.

Similarly, there will be local and functional **Security Subcommittees** chaired by the corresponding Heads of Security, which must follow the guidelines set at the global level.

These management bodies materialise the principle of cooperation that must prevail in the Telefónica Group's Security Organisation.

Notwithstanding the above, and bearing in mind the principle of co-responsibility, **all Telefónica Group employees are responsible for security** within their functional and organic scope of performance, in such a way that there is **co-responsibility between all employees and the Security Organisation**.

Security framework

In line with the classification established in the ***Telefónica Group's Policy for the preparation and organisation of Internal Rules and other Organisational Documents*** [Ref. 2], and bearing in mind the principles of hierarchy and minimums, internal rules and organisational documents will be issued at a global (corporate) or local level (either at company level or territory level), bearing in mind that global rules establish a set of minimum requirements that prevail over local rules.

The **Security Framework** regulates the following matters:

- the functional organisation of the Telefónica Group's security areas, their areas of responsibility and the general provisions, principles of action and postulates that regulate their operation.
- The security measures that must be implemented, supervised, reviewed and improved. The **principle of proportionality** between the resources required by the security measures and the possible damages that may arise from their absence or insufficiency will be one of the fundamental principles of the **Security Framework**.
- the security criteria, requirements, procedures and technologies to be taken into consideration and to be applied in each of the Telefónica Group's environments and platforms, in order to ensure that processes and technology can be used in an environment of "trust".
- the objectives to be pursued and the targets to be achieved.

The **Security Framework** will be aligned with the main international security standards and **will observe the necessary compliance with the Telefónica Group's internal regulations and the security requirements derived from the laws and regulations**, both national and international, that may be in force at any given time in any of the territories in which the Telefónica Group operates.

Contractual clauses with customers, business partners, contractors and providers of services and products must be in line with Telefónica's security regulatory framework.

It is the responsibility of the **Global Chief Security and Intelligence Officer** to perform any development and/or interpretation duties that may be necessary at a global level under the **Security Framework**, and of the **Responsible Security Officers** to perform the same duties with respect to local regulations.

The Security Framework shall be **published and reported** to all employees through awareness campaigns and training, as well as to relevant third parties (subcontractors, service providers or similar). The Security Officers will work with the relevant areas to promote awareness and practice of this policy and its implementing regulations.

Strategic plans

The **Global Chief Security and Intelligence Officer** will define, and periodically review, the Telefónica Group's ***global strategic plan for security.*** This will bear in mind security risks, business needs and the Group's strategic plans.

Any other **strategic plans** shall be conceived, designed and implemented by the various **Security Officers** in accordance with the guidelines of the Global Chief Security and Intelligence Officer. The strategic plans shall identify and prioritise projects and budgets to improve the level of security, minimising any identified risks to a level acceptable to the organisation, and to achieve the objectives set out in the security ratings or metrics.

The **Heads of Security** shall submit the strategic plans to the relevant local bodies, identifying the resources necessary to carry them out and requesting budgetary approval.

Internal Audit

The Telefónica Group's Internal Audit Department may carry out as many analyses and verifications as it deems appropriate to verify the correct application of the aspects contained in the **Security Framework**. Such audits shall include any recommendations for improvement that may arise from the results of the audit.

References

[1] Global Privacy Policy.

[2] Policy for the preparation and organisation of the Telefónica Group's Internal Regulations and other Organisational Documents.

[3] Telefónica Group Principles of Responsible Business.

[4] Telefónica Group Risk Management Policy.

www.telefonica.com