Global Security Policy

Telefónica, S.A.

Telefónica, S.A.
Approved by the Board of Directors of Telefónica S.A. at its meeting held on 25/10/2023.

5th Edition - October 2023

Change control

Edition	Date	Prepared by	Approved by	Modifications
1.0	01/04/2001	General Chief Security Officer	Board of Directors Telefónica S.A.	First version
2.0	27/07/2016	Global Chief Security Officer	Board of Directors Telefónica S.A.	Complete update of the Policy
3.0	04/11/2019	Global Chief of Security and Intelligence	Board of Directors Telefónica S.A.	Update of documentary template and minor changes
4.0	29/09/2021	Global Chief of Security and Intelligence	Board of Directors Telefónica S.A.	Updating of document template, alignment of common regulatory texts, introduction of digital security concept, reporting on the state of the group security to the Board of Directors by the Global Chief of Security and Intelligence and other minor changes.
5.0	27/09/2023	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.

Table of contents

1. Introduction

1.1. Context

Telefónica reaffirms its leadership ambition in the digital world, in which **new and increasingly sophisticated threats** are continually joining more traditional threats. As a consequence of its digital nature *(both the organisation and the business itself)*, the security effort is more demanding than in other business sectors.

On the other hand, **regulatory requirements and our customers' expectations of privacy and security are rising**, becoming key attributes of the services we offer them. Telefónica also plays an important role in protecting the technological, industrial, and commercial activity of its business customers, the development and operation of critical infrastructures that provide essential services for society, as well as for public organisations and government entities.

In addition, these existing **regulatory challenges** in the telecommunications and Internet industry, linked to national and international legislations, on many occasions unequally affect the organisation, the activity, and the business of the Telefónica Group in the countries where it is present.

1.2. Object of the document

This ***Global Security Policy*** *(hereinafter the "**Policy**")*, inspired by the principles of "integrity, commitment and transparency" set out in the Telefónica Group's ***Responsible Business Principles*** and guided by national and international standards and regulations in this field, establishes and regulates the **general provisions and guiding principles** for the matters of security referred to in this *Policy*, which are applicable to all Telefónica Group companies.

1.3. Scope

Security, one of the fundamental pillars on which the Telefónica Group's global Organisation is built, must be understood as a **comprehensive concept whose purpose is the safeguarding of the Group's assets and the protection of the Group's interests and strategic objectives**, both in its vertical Organisation (*including its business units*) and its horizontal dimension (*applicable to all its platforms*): infrastructure and network 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**, undermine their efficiency, or affect their operability and **availability**. Likewise, security is one of the fundamental principles upon which the ***Global Privacy Policy*** of the Telefónica Group rests [Ref. 1].

Comprehensive security encompasses not only physical and operational security (*of people and assets*) but also digital security, business continuity, supply chain security, commercial fraud prevention, as well as **any** other **relevant** area or **function whose purpose is corporate protection from potential harm**, of any nature whatsoever, and possible losses. In turn, the digital security concept contains aspects related to information security and cybersecurity. These aspects will be applicable to the supports, systems and technologies and elements that make up the Network.

The **security dispositions** applicable to the Telefónica Group assets will also **be extended to its collaborating agencies** (suppliers, subcontractors, etc.), when the activity of these parties affects these assets in carrying out their business, being applicable at all levels of the supply chain and with a special focus on those entities that manage the Telefónica Group's data.

1.4. Scope of application

This **policy** is **global in scope** and **mandatory** for all **Telefónica Group** companies, notwithstanding the particularities derived from the law applicable to each of them. To that end, the Telefónica Group shall be understood to be companies in whose capital **Telefónica S.A.**, holds, directly or indirectly, the majority of shares, participations or voting rights or whose corporate management body it has designated or has the power to appoint the majority of its members, in such a way that it effectively controls the company (hereinafter, Telefónica or individually any of the companies, or the "Company").

In its capacity as parent company of the group of which it is an integral part, **Telefónica, S.A.** is responsible for establishing the basic rules, determining the instruments, and designing the mechanisms necessary for appropriate and efficient coordination in security-related matters among all the companies in the group; all the foregoing notwithstanding the autonomous decisions that they may need to take, not only in accordance with the corporate interest of each of them, but also with their respective legal and fiduciary duties.

The provisions of this policy prevail over the rest of the security regulations existing in the Telefónica Group at regional, country or business line level, and in all cases, it is the **Global Chief Security and Intelligence Officer** (GCSIO) who is responsible for adopting the guidelines and measures necessary for its application, implementation, and control.

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

1.5. Validity and revisions

This policy will be valid on the day of its approval by the Board of Directors of Telefónica, S.A., the date when the previously valid policy shall be repealed.

It is the duty of the **Global Chief Security and Intelligence Officer** to exercise the **interpretative** powers that may be necessary.

This document must be **reviewed** in the light of any organisational, legal, or business changes that may occur from time to time in order to maintain its relevance, sufficiency, and effectiveness and, in the absence thereof, with the periodicity established in the ***Policy for the Preparation and Organisation of the Regulatory Framework*** [Ref. 2]. In such a case, once approved by the Board of Directors, revised versions shall be communicated to the Global Security Committee and published on the **Telefónica Group's Corporate Regulations Web Portal** [Ref. 3].

1.6. References

[1] **Global privacy policy.**

[2] **Policy for the drafting and organisation of the regulatory framework.**

[3] **Telefónica Group Corporate Regulations Portal**. Available on the Global Intranet.

[4] **Telefónica Group Risk Management Policy.**

2. Principles

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

With the approval of this **policy, the Board of Directors expresses its determination and commitment to reaching a level of security that is appropriate to the needs of the business and that consistently guarantees the protection of the assets in all Telefónica Group companies.**

To achieve this, the Board of Directors relies on the **Security Organisation** as an integral security area committed to protecting 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 the group's physical security and protection of assets and people, digital security (information security and cybersecurity), business continuity and

the prevention of commercial fraud, as well as any other action that may significantly contribute to that end.

The security activities performed by the different environments, organisational structures, parties responsible for assets, and employees will be governed by the **principles of legality, efficiency, co-responsibility, cooperation, and coordination**. Any and all appropriate promotion, conduction, control, and improvement measures will be established to this end.

- **Principle of legality**: the necessary compliance with national and international laws and regulations in force at all times in the territories in which the Telefónica Group operates will be observed.
- **Principle of efficiency**: to reach the required level of security efficiently, **the anticipatory and preventive nature of such actions** must be highlighted above a passive and reactive stance towards security activities. To do so, the knowledge of potential threats will be focused on, and the derived risks will be analysed as part of an **intelligence process**. The purpose of an ongoing intelligence process is to **identify** and understand **the most significant threats** that affect the organisation, with the aim of anticipating their activity and evolution, protecting the global organisation of the Telefónica Group from damage resulting therefrom, and to mitigate any possible risks to a degree that is acceptable for the business.

  In order to achieve a homogeneous level of security, a **global regulatory framework for corporate security** is defined. This framework will bear in mind the analysis of threats and risks, and will establish preventive, detective and corrective controls in the activities aimed at identifying, protecting, detecting, responding, and recovering.

  Strategic plans will be conceived and prepared to identify and prioritise the projects and budgets needed to achieve these appropriate levels of security, minimising the security risks identified in the corresponding analyses, and maximising the effectiveness of the investment and resources used.
- **Principle of co-responsibility**: **people** must preserve the security of the assets that Telefónica makes available to them in accordance with the security criteria, requirements, procedures, and technologies defined in the *Security Regulatory Framework*, as well as applicable laws and regulations regarding the matter of security. At the same time, they must use the assets exclusively for carrying out activities that correspond to their job and assigned tasks.

  The **Asset Owner** is the employee or executive that decides on the purpose, content, and use of the asset, and is therefore responsible for the security of the asset. The Asset Owner is also the owner of the risk associated with the asset, and therefore has the ultimate responsibility and authority to manage that risk and accept the residual risk, in accordance with the provisions of the ***Telefónica Group's Risk Management Policy*** [Ref. 4]. The Asset Owner will rely on the Security Organisation to carry out tasks aimed at ensuring the security of the asset.
- **Principle of cooperation and coordination**: in order to achieve the levels of efficiency required by Telefónica’s business project, global action and the comprehensive concept of security activities will be preserved. Thus, together with the aforementioned anticipatory and prevention requirements; 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 to improve the effectiveness and efficiency in the protection of all assets.

3. Security organisation

The **Global Chief Security and Intelligence Officer** is the highest representative of the Security Organisation in the Telefónica Group.

His mission is to ensure the efficient and effective protection of the Group's assets and be guided under all circumstances by safeguarding the viability of the business. The **Global Chief Security and Intelligence Officer** leads the development and monitors the implementation of the policy framework and global security initiatives.

Within the security organisation there are **Security Officers** at the global and local levels, 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 the most efficient and effective solution in each case.

The **Global Chief Security and Intelligence Officer** is responsible for leading the security organisation as defined in this policy. In this respect, this figure shall propose those to be appointed as Security Officers, who shall be submitted to the decision of the corresponding administrative or management bodies of the companies.

For coordination purposes, there will be a **Global Committee for Security** presided by the **Global Chief Security and Intelligence Officer**. This committee will include the participation of Security Officers of the functions, companies, or territories that are determined, as well as the divisions/departments that are considered necessary at any given time.

Similarly, there will be local and functional **Security Sub-Committees** chaired by the corresponding Security Officers, which shall follow the guidelines set at the global level.

These management bodies are the embodiment of the principle of cooperation that must prevail in the Telefónica Group's security organisation.

The **Global Chief Security and Intelligence Officer** shall report to the Board of Directors or, as the case may be, to its Audit and Control Committee, as well as to a select 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 to set out the strategic plan and the corresponding derived measures to ensure an efficient level of security.

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

4. Security regulatory framework

The ***Security Regulatory Framework*** is aligned with the ***Policy for the drafting and organisation of the regulatory framework*** [Ref. 2]

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

- the territorial and functional organisation of the Telefónica Group's security areas.
- the inherent delimitation of competences.
- the general provisions, operating principles and approaches governing its functioning.
- the objectives pursued and goals to be achieved.
- the security criteria, requirements, procedures, and technologies to be taken into consideration and applied in each of the Telefónica Group's platforms and environments, with the aim in all cases of ensuring that the technology and the processes linked to it can be used in a "trusted" environment.
- the security controls to be implemented, monitored, reviewed, and improved in order to achieve the objectives and goals outlined above; the principle of proportionality between the resources required for security controls and the possible damage that may result from their absence or inadequacy will be one of the fundamental approaches of the aforementioned *Security Regulatory Framework.*

The development of the *Security Regulatory Framework* is **global in scope** regarding the aforementioned issues. Any **regulations, instructions or other provisions of similar significance** may be necessary, which may be of global or local scope (*either at the business or territorial level*), provided that:

- the global standards establish a set of minimum requirements in all cases and in any place; and that
- the requirements set out in the local standards will only prevail if the local level justifies it and the minimum requirements of the global standards are met.

The ***Security Regulatory Framework*** will be aligned with the main international security standards.

The ***Security Regulatory Framework*** **shall observe the necessary compliance with the Telefónica Group's internal regulations and the security requirements derived**

from national and international **laws and regulations** 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 suppliers of services and products shall be aligned with security regulations.

The **Global Chief Security and Intelligence Officer** is responsible for exercising any necessary developmental and/or interpretative powers at the global level under the *security regulatory framework*. Security Officers shall have the same powers with regard to local regulations.

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

5. Strategic plans

The Global Chief Security and Intelligence Officer is responsible for defining and periodically reviewing the Telefónica Group's ***global strategic security plan.*** To do so, the security risks, business needs and strategic plans shall be considered.

It is the duty of the different **Security Officers** to conceive, design, and implement any other **strategic plans**, always in accordance with the guidelines, terms, and conditions that derive from the *Global Strategic Security Plan*. The aforementioned strategic plans, which must be submitted to the **approval of the Global Security Committee**, shall identify and prioritise projects and budgets to improve the level of security, minimising the risks that may have been identified to a level acceptable to the organisation, and enabling the achievement of the objectives set out in the security metrics or table of contents.

The **Security Officers** will submit strategic plans to their corresponding steering committees, identifying the resources required to implement them. Subsequently, the corresponding request for budget approval will be continued.

6. Internal Audit

The Internal Audit Directorate of the Telefónica Group may perform however many audits and checks it deems appropriate to verify the correct application of the aspects contained in the *Security Regulatory Framework.* Such audits shall include any recommendations for improvement that may arise from the results of the audit.

www.telefonica.com