## CHANGES RECORD

<table>
<thead>
<tr>
<th>Version</th>
<th>Prepared by</th>
<th>Changes made</th>
<th>Approved by</th>
<th>Validity Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>General Security Manager</td>
<td>First version</td>
<td>Board of Directors Telefónica, S.A.</td>
<td>01/04/2001</td>
</tr>
<tr>
<td>2.0</td>
<td>Global Chief Security Officer</td>
<td>Complete update of the Policy</td>
<td>Board of Directors Telefónica, S.A.</td>
<td>27/07/2016</td>
</tr>
<tr>
<td>3.0</td>
<td>Global Chief Security and Intelligence Officer</td>
<td>Update of documentary template and minor changes</td>
<td>Board of Directors Telefónica, S.A.</td>
<td>04/11/2019</td>
</tr>
</tbody>
</table>
## Contents

1. INTRODUCTION .................................................................................................................. 4
   1.1. Context .......................................................................................................................... 4
   1.2. Purpose of the document .............................................................................................. 4
   1.3. Scope ............................................................................................................................ 4
   1.4. Scope of application ....................................................................................................... 5
   1.5. Validity and revisions ................................................................................................... 5
   1.6. References .................................................................................................................... 5
2. PRINCIPLES .......................................................................................................................... 6
3. SECURITY ORGANISATION ................................................................................................. 7
4. SECURITY REGULATIONS FRAMEWORK ......................................................................... 8
5. STRATEGIC PLANS ........................................................................................................... 9
6. AUDIT ................................................................................................................................... 9
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 both the Organisation’s and business’ inherent digital natures, the security effort is much more demanding than in other business sectors.

Moreover, regulatory requirements and our customer's expectations regarding privacy and security are constantly increasing, becoming key attributes of the services we offer them. Furthermore, Telefónica plays a key role in the protection of the technological, industrial, and commercial activities of business customers, of the development and operation of the critical infrastructures that provide essential digital and other services to society, such as organisations, and public governmental agencies.

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. Purpose of the document

The present Global Security Policy (henceforth the "Policy"), inspired by the principles of “integrity, commitment and transparency” included in the Action Principles of the Telefónica Group and guided by the national and international standards and regulations on the matter, establishes and regulates the general dispositions and governing principles of the security issues to which this Policy refers to, and are applicable to all companies that are part of the Telefónica Group.

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 its four platforms): (1) infrastructure and network assets, (2) information technologies, (3) products and services and (4) data; guaranteeing, on the one hand, their integrity and on the other hand, eliminating potential threats that could damage their confidentiality, undermine their efficiency, or affect their operability and availability. Likewise, security is one of the fundamental principles upon which the Privacy Policy of the Telefónica Group depends, Ref. [3].

Moreover, comprehensive security encompasses not only the physical and operational security (of people and assets), but also information security, cybersecurity, security of technologies, network security, business continuity, fraud prevention, as well as any other relevant scope or function whose purpose is corporate protection from potential damages, of any nature whatsoever, and possible losses.
The security dispositions applicable to Telefónica Group assets will also be extended to its collaborating agencies (suppliers, subcontractors, etc.), when the activity of these parties affects the Group in carrying on its business, with special focus on those that manage the Telefónica Group’s data.

1.4. Scope of application

This Policy has a global scope and its application is mandatory in all Telefónica Group companies. To that end, the Telefónica Group shall be understood to be companies in whose share capital Telefónica S.A. holds, directly or indirectly, of the majority of shares, interests, or voting rights, or whose governance or management body has been designated or has the power to appoint the majority of its members, in such a way that it effectively controls the company.

In its capacity as parent company of the Group, Telefónica, S.A. is in charge of establishing the basic rules, instruments, and mechanisms necessary for an appropriate and efficient coordination in matters of security among all the other companies in the Group; all of the aforementioned without prejudice to, and without impairing, the autonomous decision-making capacity of each of said companies, in accordance with their own corporate interests and fiduciary duties.

The dispositions of this Policy overrule the security regulations that exist at a regional, country, or business line level. In every case, it is the Global Chief Security and Intelligence Officer (GCSIO) who must monitor this Policy and adopt the guidelines and measures necessary for its application and implementation.

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

1.5. Validity and revisions

This Policy came into effect on the day of its approval by the Board of Directors of Telefónica, S.A., the date when the previously valid policy was 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 according to any organisational, legal, or business change that may occur at any given time in order to maintain its level of pertinence, sufficiency, and effectiveness. In such a case, the reviews shall be communicated and published in the Telefónica Group’s Corporate Regulations Portal, available through the Telefónica Group’s Global Intranet. Ref. [1].

1.6. References

2. PRINCIPLES

The Board of Directors of Telefónica S.A. considers people, information, technologies, and material resources that support them, to be fundamental assets. For this reason, guaranteeing their security is considered to be an essential asset within the Telefónica 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.

The Board of Directors entrusts this task to the Security Organisation in its capacity as comprehensive security unit committed to the protection of the Group's assets, considering the modern and dynamic situation that being a digital telco entails, and tasks it with the efficient and effective management of the physical security and the protection of assets and people, with the Group's information security and cybersecurity, with the business continuity and the prevention of fraud, as well as any other action that could significantly contribute towards this 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 all national and international laws and regulations regarding the matter of security that may be valid at any given time in any of the territories where the Telefónica Group operates, shall be ensured.

- **Principle of Efficiency**: in order to efficiently reach the required level of security, the anticipatory and preventive nature of security actions shall take precedence over any passive and reactive nature. 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.

A Global Corporate Security Regulations Framework is defined for the purpose of reaching a standardised level of security. This framework will consider the analyses of threats and risks and will also establish the precise preventive or corrective protection measures.

In addition, strategic plans will be conceived and prepared in order to identify and prioritise the projects and budgets necessary for reaching those appropriate levels of security, minimising the security risks identified in the corresponding analyses, and maximising the effectiveness of the investment made and the 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 Regulations Framework, as well as applicable laws and regulations regarding the matter of security. At the same time, users must use the assets exclusively for the performance of activities that are consistent with their position and assigned tasks.
The **party responsible for an asset** is the employee or executive that makes decisions regarding the end purpose, content, and use of said asset, and is therefore responsible for the security of the asset. The party responsible for an asset is also the owner of the risk associated with said asset. Therefore, he/she is responsible for, and has final authority over, the management of the risk and acceptance of the residual risk. The party responsible for an asset shall be supported by the Security Organisation when performing tasks aimed at guaranteeing the security of the aforementioned asset.

- **Principle of Cooperation and Coordination**: in order to reach the levels of efficiency that Telefónica business projects require, the global action and comprehensive concept of security activities shall be preserved together with the aforementioned requirements of anticipation and prevention. Cooperation and coordination between all business units and employees will be prioritised in order to generate the appropriate synergies and to jointly reinforce the capabilities.

The Security Organisation shall coordinate the security responsibilities of the different Telefónica Group structures, encouraging cooperation between them in order to guarantee the efficient and joint protection of the assets.

### 3. SECURITY ORGANISATION

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

The mission of the **Global Chief Security and Intelligence Officer** is the efficient and effective protection of the Group’s assets, and is focused on ensuring, in every case, the viability of the business.

Within the Security Organisation are **Security Officers** both at a global and local levels. Their obligations 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 what is the most efficient and effective solution in each case.

The **Global Chief Security and Intelligence Officer** is responsible for boosting the Security Organisation defined in the present Policy. In this sense, he/she is responsible for proposing those who should be assigned as Security Officers, who will then be submitted to the decision of the corresponding administration or management agencies of the companies.

For coordination purposes, there will be a **Global Security Committee** 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, local and functional **Security Subcommittees** presided by Security Officers will exist following the guidelines established at a global level.

These management agencies materialise the principle of cooperation that must reign within the security Organisation of the Telefónica Group.
Notwithstanding the foregoing, all Telefónica Group employees are responsible for security within their functional and organic performance scopes; in other words, there is a shared co-responsibility between all employees and the Security Organisation.

4. SECURITY REGULATIONS FRAMEWORK

The Security Regulations Framework is adapted to the Preparation and Organisation Framework of the Regulations Framework (Ref. [2]) and regulates, among others, the following matters:

- the territorial and functional Organisation of the Telefónica Group security areas.
- the competence limits inherent to said security areas.
- the general dispositions, principles of action, and tenets that will regulate its functioning.
- the objectives pursued and the goals that should be reached.
- the security criteria, requirements, procedures, and technologies that must be taken into account and that must be applied in each of the Telefónica Group platforms and environments in order to ensure, in each and every case, that the technology can be used in a “reliable” environment.
- the security controls that must be implemented, supervised, reviewed, and improved in order to achieve the reported objectives and goals; the principle of proportionality between the resources required by the security controls and the possible harm that could stem from their absence or insufficiency will be one of the fundamental tenets of the aforementioned Security Regulations Framework.

The development of the Security Regulations Framework is characterised globally regarding, among others, the aforementioned issues as well as the general policy for security of the Telefónica Group. Under the advocacy of said general policy for security, any and all regulations, instructions, or other dispositions of similar or analogous meanings as necessary will be drafted, all of which will have a global or local scope (either at a company level or at a territorial level), considering, however, that:

- global regulations establish a set of minimum requirements in every case and in every location; and that
- the criteria of global regulations will always supersede those local regulations.

The Security Regulations Framework shall ensure the necessary compliance with all national and international laws and regulations regarding the matter of security that may be valid at any given time in any of the territories where the Telefónica Group operates.

All contractual clauses with clients, commercial partners, contractors, and suppliers of services and products must be in accordance with the security regulations.

It is the duty of the Global Chief Security and Intelligence Officer to exercise any and all development and/or interpretation competencies that may be necessary at a global level under the advocacy of the Security Regulations Framework. Identical competencies regarding local scope regulations will be the duty of the Security Officers.
The Security Regulations Framework shall be published and communicated to all employees, as well as to any and all relevant third parties (subcontractors, service providers, or other similar parties), through awareness and training campaigns. Security Officers will work with the corresponding departments to promote the knowledge and practice of this Policy and its development regulations.

5. STRATEGIC PLANS

It is the duty of the Global Chief Security and Intelligence Officer to periodically define and review the Global Strategic Security Plan of the Telefónica Group. To do so, the business needs and strategic plans of the four platforms shall be considered.

It is the duty of the different Security Officers to conceive, design, and implement any other Strategic Plans whatsoever, always in accordance to 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 security projects and budgets for the purpose of reaching the established control objectives. Similarly, they shall minimise the security risks that may have been identified, thus ensuring an acceptable level for the Organisation.

6. 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 Regulations Framework. Said audits shall include proposals for improvement, in so far as it is possible.