INFORMATION SECURITY POLICY

SIGNATURE CONTROL

Version	Written by	Reviewed by	Approved by
1.8	Seguridad interna	Marta Garcia Lopez Service Platforms Director	Pedro López Director CTO

CHANGES CONTROL

Version	Date	Modifications	Description of the change
1.0	02/03/2009	N/A	Firts edition of the document
1.1	01/04/2010	1, 2, 3.4	Style improvements Delete of abolished law
1.2	06/10/2011	2, 3.1, 3.4	Style improvements Alignment with corporate Information Security Act
1.3	19/03/2013	3.5, 3.3, 3.8	Update of content (3.5) and name of enterprise
1.4	03/03/2014	3.1	Inclusion of commitment to continuous improvement
1.5	07/10/2014	3.3	Inclusion of a new section focused on the definition of objectives
1.6	29/01/2016	Todo	Change of department name Alignment with Corporate Information Security Act
1.7	20/11/2018	Ap 3.5 Ap 3.8 Ap 3.10 Ap. 3.11 All	Content update
1.8	27/11/2019	All	Change of Telefonica Business Solutions for Telefonica International Wholesale Services
1.9	27/11/2019	All	Review policy

ÍNDICE

1. POLICY OBJECTIVE

The purpose of this document entitled ***Information Security Policy*** is to provide basic guidelines to ensure de security of information (base on criteria of integrity, confidentiality and availability) to get, ultimately, a security improvement for the services offered by the company to its customers, and improving their internal processes.

2. SCOPE

This Policy is of mandatory knowledge and compliance of all areas of Telefonica International Wholesale Services (TIWS II, S.L.), both in its internal relations and with other organizations.

This Policy covers all information used by TIWS II, S.L. for the development of their activities.

This information Security Policy is aligned with the guidelines set by the Corporate Information Security Policy of Telefonica Group.

3. SPECIFICATIONS

3.1. General Principles of Information Security

Telefónica International Wholesale Services (TIWS II, S.L.) grants priority interest and maximum support to the protection of information due to its strategic nature and as a means to ensure business continuity.

This Policy seeks the adoption, implementation and ongoing operation of protocols and procedures to preserve the three basic components of information security:

- **Confidentiality:** ensuring that only authorized people access to data and systems.
- **Integrity:** to ensure the accuracy of the information and systems against unauthorized information alteration, loss or destruction, whether accidental or intentional.
- **Availability:** ensuring that information and systems can be used as and when required

This Policy applies at all stages of the information life cycle: generation, distribution, storage, processing, transportation, consultation and destruction, and systems that process it (analysis, design, development, implementation, operation and maintenance).

The information security affects the entire staff of the organization so this policy should be known, understood and embraced by all levels of the organization.

The Policy should be communicated reliably to the entire Organization and must be available to all interested parties.

Relationships with third party collaborators must always be protected by due guarantees in the use and processing of information.

3.2. Organization and Responsabilities

The information security function rests in the Security Area that is responsible for formulating the basic guidelines and principles of security and ensuring compliance with this document and all the actions derived from it.

Any system user is responsible for appropriate information use made and must comply with established controls and recommendations established in the corresponding protocols aligned with this Policy.

3.3. Information Security Objectives

With the objective of contributing to minimize and control risks within the Organization, TIWS II S.L. define a set of repeatable and measurable objectives.

Those objectives are measured, at least, semi-annually and reviewed annually to be aligned with the strategy of TIWS II S.L.

3.4. Implementation of the Information Security Policy

In order to apply the principles, set forth in this Policy, the definition, preparation, implementation and maintenance of action plans or actions for continuous improvement are required.

The elaboration of these Plans and Actions must be based on formal processes of risk analysis, criteria of evaluation and management of risks or objective business needs, that allow to implement the appropriate solutions.

Operationally, TIWS II S.L. will develop its own procedures, standards and safety guidelines that ensure the integrity, confidentiality and availability of information.

All the necessary security management processes will be implemented according to recognized international standards to ensure effective and efficient monitoring of the actions in security, as well as the processes of continuous review and improvement of security.

3.5. Legal Compliance

Telefónica International Wholesale Services (TIWS II, S.L.) is committed to ensuring compliance with national laws concerning the protection and security of information considering its object, social reason and business objectives, as well as for information technology services provided or that could be provided.

Requirements of applicable laws concerning data processing and information security and mechanisms and proper and reasonable measures are stablished for its compliance.

Telefónica International Wholesale Services (TIWS II, S.L.) will ensure compliance with superior standards (national laws, rules and laws) that will have precedence when they apply by its nature and business objective, been prioritized, when apply, over the guidelines identified in this Policy and even about Customer requirements associated with the provision of contracted services.

Moreover, it will be considered supranational standards which come from official organisms of which Spain is member and the European and extra-community Regulations, due to the areas of service provision by Telefónica International Wholesale Services (TIWS II, S.L.).

Furthermore, normative and conduct policies from Telefónica Group will be considered.

3.6. Classification and Treatment of Information

All information should be classified under its importance to the organization and must be treated according to this classification, according to the provisions of rules specifically developed for this purpose.

3.7. Training and Awareness

The most effective method of improving safety is through continuous training and its incorporation into work activity.

Within the broad training plans of the Company there will be included specific courses on information security according with the target area and target audience as deemed necessary. Also, information security awareness campaigns will be made aimed at all staff through the most effective methods.

Telefónica International Wholesale Services (TIWS II, S.L.), will have the appropriate mechanisms that guarantee the availability of the information so that it can be used when necessary and, in those terms, and conditions considered.

3.8. Business Continuity Management

Telefonica International Wholesale Services (TIWS II S.L.), will provide adequate mechanisms to ensure the availability of information so it can be used when required in activities related to business continuity, in those terms and conditions considered.

3.9. Audit

Information Systems undergo regular internal and external audits in order to verify the correct operation of security plans, determining compliance and recommending corrective action, getting, a continuous improvement.

3.10. Non Compliance

Deviations and exceptions of non-compliance of any guidelines or principles defined in this Policy will be justified by business reasons and must be agreed with Security area.

By the contrary, the total or partial non-compliance of what is collected in this document will end in warnings, according to the magnitude, impact and characteristics of what is breach, apart from the offender profile.

3.11. Continuous Improvement

Telefónica International Wholesale Services (TIWS II, S.L.), considers fundamental to ensure continuous improvement, for this reason, will define actions to improve the organization's performance in terms of the availability, integrity and confidentiality of the information.

3.12. Validity

The Information Security Policy will entry into force since the day of its publication.

Likewise, this Policy must be reviewed, at least, yearly.