SGSI-P-5.1.1
Information Security Policy

CONTENTS

1. DEFINITION OF INFORMATION SECURITY

For Andorra Telecom (hereinafter, AT or the Company) information is a very valuable and critical asset. Without it the Company would not be able to carry out its activity. To achieve the proper management of this asset, AT uses the information in a precise and comprehensive way, and guarantees its availability.

Information security is defined as the protection of information against a wide range of threats to ensure business continuity, minimise risks, and maximise return on investment and opportunities.

Therefore, the Company recognises the importance of security measures to ensure that information is not affected by either internal or external threats, such as: human error, malicious actions (fraud, embezzlement, sabotage, privacy breaches, etc.), technical errors and threats caused by force majeure such as natural disasters.

AT's Management is responsible for implementing the security directives. The adoption of these directives by the Company will minimise the potential risks which it is exposed to in the performance of its business activities.

2. SCOPE OF THE INFORMATION SECURITY POLICY

The Information Security Policy is applicable to anyone who, during the performance of their duties, has or may have access to AT's information, either directly or through any information system.

Therefore, the areas of application of the Information Security Policy are:

- All AT employees, regardless of whether they are permanent or otherwise, including anyone outside AT who has access to or owns the managed information.
- All information and information systems owned or managed by AT.

3. OBJECTIVES

The Information Security Policy sets forth the guidelines for establishing the security regulations with the aim of safeguarding and guaranteeing the basic principles of information security: confidentiality, integrity, availability and traceability.

For the preparation of this document and the achievement of the set objectives, the following key aspects have been adopted:

- The Company's information and information systems are critical assets, and therefore they must be protected, and their availability must be ensured.
- AT's information must be protected according to its legal requirements, value, criticality and sensitivity.

- The responsibility for protecting these assets rests with all employees and external collaborators who have access to the information.
- The security measures applied to the information must be established taking into account its classification; this will determine its level of confidentiality, integrity, availability and traceability. The measures will be determined in accordance with an ongoing risk assessment.

4. DECLARATION OF PRINCIPLES

The information security principles which form the basis for drawing up the information security regulations are as follows:

- Information must be protected throughout its life cycle, from its creation or receipt to its processing, communication, transport, storage, dissemination to third parties and its eventual destruction.
- AT protects the information against unauthorised access, improper dissemination and against its loss.
- Each employee has the obligation and duty to adequately protect information in accordance with security regulations.
- All personnel, including external personnel or third parties with access to AT's information, must comply with AT's security regulations.

5. CONSIDERATIONS INCLUDED IN THE INFORMATION SECURITY POLICY

- The Information Security Policy has been approved by AT's General Management.
- Its content, together with information security regulations, is of mandatory compliance for all AT personnel as well as for external contracts.
- The Information Security Policy must be complied with in order to protect AT's legal rights. Anyone who fails to comply with it will be subject to the disciplinary and legal measures deemed appropriate by AT's Management.
- The Information Security Policy is a live document which must be updated and modified whenever necessary.
- AT's Management will take the necessary steps so that all AT personnel, external personnel and relevant third parties have knowledge of and apply all the aspects included in this policy.

6. IT'S EVERYONE'S BUSINESS TO ENSURE SECURITY

AT's Management has created a Risk Committee, consisting of a number of appointed members, who will meet periodically to address relevant security issues.

The Risk Committee will be responsible for reviewing and approving information security regulations and ensuring they are kept up to date when faced with significant changes. At the same time, it will be the Risk Committee's responsibility to approve the necessary initiatives to improve information security, as well as to raise awareness and encourage the involvement of all employees. This ensures that any action taken in the field of security is implemented by the entire organisation.

7. INFORMATION SECURITY REGULATIONS

To achieve the objectives and principles included in this policy, a series of regulations has been developed, which sets forth the general rules of information security and which are grouped according to established domains.

These regulations constitute a basis for the development of specific security measures which are specified through the formalisation of procedures.

The regulations have been defined according to the ISO 27001:2013 standard which establishes an internationally recognised security reference framework. The security requirements established by ISO 27001:2013 are defined by control objectives that are grouped according to the following domains:

- **Domain 6. Organisation of information security**. Definition of the roles of AT's directors and employees, as well as organisational aspects and responsibilities to maintain information security.
- **Domain 7. Human resources security.** The security of personnel, in order to define and implement the duties and responsibilities in the workplace.
- **Domain 8. Asset control.** Inventory, maintenance and classification of assets throughout the organisation, including information, in order to maintain an appropriate degree of protection.
- **Domain 9. Access control.** Logical access control to protect AT's information assets, preventing unnecessary or unauthorised access.
- **Domain 10. Cryptography.** Management and control of cryptographic systems.
- **Domain 11. Physical and environmental security.** Physical and environmental security in order to control access to sensitive information.
- **Domain 12. Operations security.** Management and control of operations, in both external networks and AT's internal ones.
- **Domain 13. Communications security.** Management and control of communications, in both external networks and AT's internal ones.
- **Domain 14. System acquisition, development and maintenance.** Definition of the security requirements for the development and maintenance of information systems, with the aim of guaranteeing the correct operation of AT's IT resources at all times. It includes the development of risk prevention plans for possible disasters, as well as procedures for retrieving AT's data and critical information.

- **Domain 15. Supplier relationships.** Management and control of relationships with suppliers as well as services provided by third parties.
- **Domain 16. Information security incident management**. Management, communication and response to security incidents.
- **Domain 17. Business continuity management**. Business continuity to ensure the restoration of critical business processes in the event of any interruptions occurring.
- **Domain 18. Compliance.** Identification of the current applicable law in Andorra to ensure compliance, as well as periodic checks to validate compliance with the organisation's security regulations.

8. EXPECTED RESULTS

The expected results of the implementation of the security policy are as follows:

- To improve security management on a continuous basis. The organisation will have better security resources in the form of knowledge, procedures and tools.
- To consolidate customers and suppliers' trust in the Company, as well as improving in the public image.
- A reduction of costs arising from security incidents, through the progressive implementation of security controls.
- Ensuring compliance with legal and ethical requirements.

GLOSSARY

Asset: anything that may be of value to the Company, such as information, software, physical assets, services, people and intangible assets.

Threat: a potential cause of an undesirable incident, which could have an impact on a system or the organisation.

Confidentiality: a characteristic that ensures that private or confidential information is not disclosed to unauthorised persons, during storage, processing or transit.

Business continuity: the tolerable amount of time that a business process can be interrupted without causing a major impact on the Company.

Criticality: the importance of an asset based on the damage it would cause to the Company in the event that a threat to that asset materialises.

Personal data: any information regarding identified or identifiable individuals.

Availability: a characteristic that ensures that the systems work on time and that services are not denied to authorised users.

Impact: the consequence for an asset should the threat occur.

Security incident: an event identified on a system, service, or network that indicates a possible breach in the security policy or a failure of the safeguards, or a previously unknown situation that may be relevant to security.

Integrity: a characteristic that prevents the unauthorised modification or destruction of domain assets.

ISO: The International Organization for Standardization is an international non-governmental organisation which certifies internationally recognised industrial and commercial regulations.

Security regulations: a set of regulations that support the objectives set forth in the Information Security Policy.

Information Security Policy: a high-level statement of the Company's objectives, guidelines and commitment to achieving security management.

Procedures: operational method sheets that make up the specific tasks and activities of the daily operations.

Risk: the probability that a threat will occur that will have a specific impact on an asset, domain or the entire Company.

Traceability: a characteristic that allows the reconstruction, review and examination of a sequence of events.

Third party: a person or entity recognised as independent from the participating parties, who or which is related to the situation in question.