Information Security Policy

Adopted by the Governing Council at its meeting on 28 October 2025

Contents Index

1 INTRODUCTION

At present, information technologies are facing an increasing number of threats, which requires a constant effort to adapt and manage the risks introduced by them.

The purpose of the Information Security Policy (hereinafter "Policy") is to adopt a set of measures to preserve the confidentiality, integrity and availability of information, and to establish the high-level requirements necessary to protect information, equipment and technological services, which support the business processes of the companies that make up the Amper Group (hereinafter "Amper Group").

This Information Security Policy is the cornerstone of the Amper Group's Safety Standards Corps. The Safety Standards Corps (CNS) is a set of documents at different levels that make up the security requirements, guidelines and protocols to be followed by the Amper Group. The CNS should be developed by each Amper Group society through a set of documents (use standards, regulatory standards, procedures, manuals, guides, good practices, etc.) in such a way that they cover all the aspects presented in the Policy, reaching the operational process level.

1.1 OBJECTIVE

The main objective of this Policy is to define the basic principles and rules for the management of information security. The ultimate aim is to ensure that Amper Group companies ensure information security and minimize non-financial risks arising from an impact caused by ineffective management of information.

1.2 SCOPE

The Policy applies to the entire Amper Group, which will have to meet this minimum requirement without prejudice to being able to implement more restrictive policies. In addition, the subsidiaries will have to adapt and develop this Policy in their companies and will have to report to the parent of the Amper Group their compliance with this Policy. The scope of this Policy covers all information from Amper Group companies regardless of how it is processed, who accesses it, the medium containing it or where it is located, whether it is printed or stored electronically.

The Policy will be available on the corporate website of Amper www.grupoamper.com and in a common Amper repository, so that it is accessible to all people in the Amper Group.

1.3 ADAPTATION AND DEVELOPMENT BY THE PHILIALS OF POLICY

This Information Security Policy should be adapted and developed by each Amper Group society. Each society shall decide how the Policy adapts to its operations by means of specific documentation (its Safety Standards Body, CNS), which shall always be aligned with the guidelines set out in this document.

2 PRINCIPLES OF INFORMATION POLICY

This Policy responds to the recommendations of the best information security practices contained in the International Standard ISO/IEC 27001 and National Security Scheme, as well as to compliance with existing legislation on the protection of personal data and regulations that may affect the Amper Group in the field of information security.

In addition, the Amper Group establishes the following basic principles as fundamental guidelines for information security that must always be taken into account in any activity related to the processing of information:

- Strategic scope: Information security must be committed and supported by the management levels of Amper Group societies to coordinate and integrate with the rest of the strategic initiatives in order to form a coherent and effective framework of work.
- Comprehensive security: Information security shall be understood as an integral process consisting of technical, human, material and organizational elements, avoiding, except in cases of urgency or necessity, any specific action or cyclical treatment. Information security shall be considered as part of the usual operation, being present and applied throughout the process of design, development and maintenance of information systems.
- Risk management: Risk analysis and management will be an essential part of the information security process. Risk management will allow the maintenance of a controlled environment, minimizing risks to acceptable levels. The reduction of these levels will be achieved through the deployment of security measures, which will strike a balance between the nature of the data and the processing, the impact and probability of the risks to which they are exposed and the effectiveness and cost of the security measures.
- Proportionality: The establishment of protective, detection and recovery measures should be proportionate to the potential risks and to the criticality and value of the information and services concerned.
- Continuous improvement: Safety measures will be re-evaluated and updated on a regular basis to adapt their effectiveness to the constant evolution of risks and protection systems. Information security will be serviced, reviewed and audited by qualified personnel.

- Default security: Systems must be designed and configured in such a way that ensure a sufficient degree of default security.

The Amper Group considers that the information security functions should remain integrated at all hierarchical levels of their staff.

Since Information Security is the responsibility of all Amper Group personnel, this Policy must be known, understood and assumed by all its employees.

In order to achieve the objectives of this Policy, the Amper Group will have to establish a preventive strategy for analysing the risks that may affect it, identifying them, introducing controls for their mitigation and establishing regular procedures for their reassessment. In the course of this continuous improvement cycle, the Amper Group will maintain the definition of both the accepted residual risk level and its tolerance thresholds.

3 COMMITMENTS OF THE DIRECTION

The Directorate of the Amper Group, aware of the importance of information security in successfully carrying out its business objectives, undertakes to:

- Promoting security roles and responsibilities in organization information.
- Provide adequate resources to achieve information security objectives.
- Promoting the dissemination and awareness-raising of the Information Security Policy among the employees of the Amper Group.
- Require compliance with the policy, existing legislation and the requirements of the regulators in the field of information security.
- Consider information security risks in decision-making.

4 ROLES AND RESPONSIBILITIES

The Amper Group undertakes to ensure the safety of all assets under its responsibility through the necessary measures, always ensuring compliance with the various applicable regulations and laws.

In the companies of the Amper Group, a figure responsible for defining, implementing and monitoring cybersecurity and information security measures should be designated.

It will be your responsibility to develop and maintain the Policy, ensuring that it is appropriate and timely as both the Amper Group society for which you are responsible and the current regulation evolve.

5 HUMAN RESOURCES SECURITY MANAGEMENT

The Department of Human Resources will be responsible for its management taking into account the security criteria set out in the Information Security Policy, which is a key point for ensuring compliance.

The requirements set out in this Policy should be safeguarded at all times, including at the pre-contracting stage, the recruitment phase, and the phase of withdrawal of employees' contracts.

5.1 TRAINING AND CONSCIENCE

The Amper Group should ensure that all staff are adequately trained and sensitized in the field of information security, especially in the area of confidentiality and the prevention of information leakage.

Employees will also be informed of updates of security policies and procedures in which they are affected and of existing threats to ensure compliance.

On the other hand, employees have an obligation to act with diligence with respect to the information, ensuring that such information does not fall into the hands of unauthorized employees or third parties.

5.2 LIMITED TABLES POLICY

The following requirements are laid down with the aim of maintaining job security:

- The session of the equipment must be blocked when the employee leaves the position, both by manual means (blocking by the user), and automatically by setting the screen lock.
- The working environment should be left in place at the end of the day. This includes the need for any document or information support to be kept out of sight, keeping under lockdown those classified as confidential or secret (see paragraph 20.1 “Annex: Classification levels”).

6 ASSETS MANAGEMENT

The information assets necessary for the provision of the Amper Group business processes must be identified and inventoryd. In addition, the asset inventory should be kept up to date.

Classification of the information: The classification of the assets according to the type of information to be processed, according to paragraph 7 “Classification of the Information”, shall be carried out.

A person responsible for carrying out the own management of information assets should be assigned throughout the life cycle. The controller shall maintain a formal register of users with authorised access to that asset.

In addition, for each asset or information item there shall be a responsible or owner, who shall be responsible for ensuring that the asset is inventoryed, properly classified and adequately protected.

Asset configurations should be regularly updated to allow for tracking and to facilitate correct updating of the information.

6.1 MANAGEMENT OF BYOD DEVICES OR PERSONAL DEVICES

The Amper Group adopts the policy known as BYOD (Bring Your Own Device), which allows employees to use their personal mobile devices or resources to access Amper Group resources or information.

In addition, users should take into account a number of requirements set out in this Policy:

- The same safety measures and configurations should be applied to devices BYOD that treat information the same as other Amper Group devices.
- The user will be responsible for BYOD equipment. Users should keep the personal BYOD device where they treat information of any type from the Amper Group. Employees must be authorized by their area manager to use BYOD devices.
- Any impact that may affect confidentiality, integrity or availability of these devices must be reported to the security officer.

6.2 MANAGEMENT OF THE LIFE CYCLE OF INFORMATION

The Amper Group should properly manage the life cycle of the information, avoiding incorrect uses during any of the phases.

The life cycle of an information asset consists of the following phases:

1. Creation or collection: this phase deals with records at their point of origin. It could include its creation by a member of the Amper Group or the receipt of information from an external source. Includes correspondence, forms, reports, drawings, computer input/output or other sources.

2. Distribution: is the information management process once it has been created or received. This includes both internal and external distribution, as the information coming out of the Amper Group becomes a record of a transaction with third parties.

3. Use or access: It takes place after the information is distributed internally, and can generate business decisions, generate new information, or serve other purposes. It details the set of users authorised by the Amper Group to access the information.

4. Storage: is the process of organizing information in a predetermined sequence and creating a management system to ensure its usefulness within the Amper Group. Without a storage method for reporting, recovery and use would be almost impossible.

5. Destruction: sets out the practices for the elimination of information that has fulfilled the defined retention periods and information that has ceased to be useful to the Amper Group. The periods of retention of the information must be based on the regulatory, legal and legal requirements affecting the Amper Group. Business needs should also be taken into account. If none of these requirements requires that the information be kept, it must be disposed of by means that ensure its confidentiality during the destruction process.

The Amper Group shall identify security measures in accordance with this Policy to ensure the proper management of the asset life cycle.

6.3 MANAGEMENT OF SAFETY COPIES

The information must be backed up and checked regularly. To this end, backups of applications, files and databases must be made at least weekly, unless no updates have taken place during that period. Where appropriate, a higher backup frequency may be established, if the information to be safeguarded is of high impact to the Amper Group and/or high level of transactionality.

As a general rule, the frequency with which backups will be made shall be determined according to the sensitivity of the applications or data, in accordance with the classification criteria for information declared in the Annex “Classification levels”.

Backups must receive the same security protections as the original data, ensuring their correct preservation, as well as appropriate access controls.

As a general rule and whenever possible, information in backups should be required to be encrypted. This requirement shall be mandatory for certain types of confidential information.

Restoring tests of available backups and defined restoration processes should be carried out to ensure the proper functioning of the processes. These shall be carried out on a regular basis and shall be documented.

A period of retention of backups shall be established until their destruction after the end of the period of existence.

Backups of both master files and applications and information files should be located in secure locations with restricted access. In addition, backup copies will preferably be located in a centre other than the one that generated them or in the cloud.

It should be ensured that there is an additional backup of sensitive information protected against writing, so as to ensure its integrity in the face of the need for recovery from possible security incidents associated, for example, with ransomware.

7 CLASSIFICATION OF INFORMATION

A classification model for information should be defined to make it possible to identify and implement the technical and organisational measures necessary to maintain its availability, confidentiality and integrity. The classification model shall integrate the requirements and conditions set out in this section of the Policy.

The classification model must have a responsible to update it when it is considered appropriate and to make it known to all employees of the Amper Group.

7.1 TYPES OF INFORMATION

The Amper Group shall classify the information according to the medium in which it is being used:

- Software: information being used by office media, mail electronic or customized or acquired information systems from a third party.
- Physical media: information that is on paper, magnetic media such as USBs, DVDs, etc.

7.2 CLASSIFICATION LEVELS

Depending on the sensitivity of the information, the Amper Group should catalogue the information at five levels, see the precise definition in the Annex “Classification Levels”:

- Public use
- Limited dissemination
- Confidential information
- Information reserved
- Secret information

7.3 PRIVILEGED INFORMATION MANAGEMENT

Information deemed to be reserved, confidential or secret should be treated with particular care. Extraordinary or additional security measures should be defined for the proper insider trading.

7.4 INFORMATION LABELLING

The Amper Group shall label using manual or, to the extent possible, automated methods to facilitate the proper processing of the security measures they apply in each case.

Documents or materials, as well as annexes, copies, translations or extracts thereof, shall be labelled according to the levels of classification of the information defined in the previous subparagraph, except for the information considered to be "Public use".

A process or procedure for labelling information shall be defined in accordance with the following requirements:

- Ensure that the labelling of the information reflects the classification scheme of the information adopted.
- Ensure that labels are easily recognizable among all employees.
- To guide employees on where and how labels will be placed or used, in function of the process of access to the information or to the assets that support it.
- to indicate the exceptions in which labelling is allowed to be omitted, without omission of the duty to classify information.

Particular attention should be paid to the labelling of physical assets that require maximum care and contain secret or restricted information, in order to prevent their theft, as they are easily identifiable

Technical measures should be established, if necessary, and feasible for automatic labelling of information supported in digital media.

The Amper Group should ensure the training and training of all its employees in the labelling of information, as well as specifically train and train employees who treat information at the secret or reserved level.

7.5 MANIPULATION OF INFORMATION

The Amper Group will be responsible for developing and implementing an appropriate set of procedures for the proper handling of information. The necessary measures should be taken to protect the information according to its classification.

The inside information shall be kept at all times throughout the life cycle of the information.

7.6 PRIVACY OF INFORMATION

The Amper Group must ensure the privacy of personal data in order to protect the fundamental rights of natural persons, in particular their right to honour, personal and family privacy and image, by establishing measures to regulate the processing of data.

The Amper Group must comply with the legislation in force concerning the protection of personal data according to the jurisdiction in which it is established and operates (in an illustrative manner, Organic Law 3/2018, of 5 December, on the Protection of Data and Guarantees of Digital Rights for the case of Spain) and must include the necessary measures to comply with the regulations.

Appropriate measures should be implemented to ensure the privacy of information at all stages of your life cycle (in accordance with Section 6.2 Information Lifecycle Management).

8 PREVENTION OF SOURCES OF INFORMATION

The leak of information is an uncontrolled exit of information (intentional or unintentional) that causes it to reach unauthorized persons or that its owner loses control over access to it by third parties.

Information leakage vectors should be analysed, depending on the working conditions and operation of each Amper Group company. For this purpose, assets whose leakage poses the greatest risk to each society must be identified, based on the criticality of the asset and the level of classification that the information has. In addition, the possible means of theft, loss or leakage of each asset in its different life-cycle states should be identified.

The Amper Group should define procedures to avoid situations that may lead to loss of information, as well as procedures for action if information leaks are reported.

Training and training of all employees on good practices for the prevention of information leaks should be ensured. In particular, at least the following aspects should be taken into account:

- Process for handling known high criticality devices
- Appropriate use of removable devices such as USBs, CDs/DVDs or the like
- Use of e-mail
- Oral transmission of information
- Printing of documentation
- Documentation output
- Use of mobile devices
- Use of the Internet
- Clean and orderly desks (see section 5.2 Clean tables policy)
- Unserved equipment

9 ACCESS CONTROL

All Amper Group information systems must have an access control system. Access control also focuses on ensuring user access and preventing unauthorized access to information systems, including measures such as password protection.

Access control shall be understood from both a logical perspective (focusing on information systems) and a physical perspective (see paragraph 11 Physical and Environmental Security).

9.1 BUSINESS REQUIREMENTS FOR ACCESS CONTROL

The Amper Group shall assume a number of business requirements for access control, which shall be at least the following:

- Users must be unique and cannot be shared. In addition, the privileges of users will be initially assigned by the principle of minimum privilege.
- Where possible, multiple authentication factor (MFA) for the access to information systems, being mandatory for those accessible from public networks.

9.2 ACCESS RIGHTS

The Amper Group should implement access controls to ensure that users are only granted privileges and rights necessary to perform their role.

Access rights shall be established on the basis of:

- Role-based access control: profiles or access roles should be established by application and/or systems to be able to assign them to different users.
- Need to know: access to a resource will only be allowed where there is a need legitimate for the development of the activity.
- Minimum privileges: the permissions granted to users must be the minimum.
- Segregation of functions: proper segregation of functions should be ensured for develop and assign access rights.

No user will be able to access only a controlled information system without the approval of responsible for the user (or the designated person).

9.3 LOGIC ACCESS CONTROL

The Amper Group should establish an appropriate password policy aligned with good security practices. The password policy shall define the requirements for passwords and maintenance times for the same password.

The Password Policy must be known to all employees of the Amper Group.

9.4 TELETRABASE

Remote access to the Amper Group's network should be monitored in the form of remote work, i.e. from outside its own facilities.

Remote work connection services shall be intended exclusively for Amper Group personnel. Your use by any other partner will require authorization from the security officer.

Equipment used for remote work mode connection may be owned by the employee or provided by the Amper Group. In any case, it is mandatory for the equipment to comply with the following safety requirements:

a) Ability to make a connection through a VPN.
b) Have an up-to-date operating system with the latest patches and updates of
c) security.
d) (c) Antivirus software installed.
e) Firewall software/personal firewall installed.

Teleworking from a worker's own team will require all security measures

in order to ensure that remote work does not pose a threat to the security of Amper Group information. In addition, additional security measures may be put in place to ensure a more reliable secure remote connection. The telecommuting service will be monitored and monitored, with both the connection and activity recorded in accordance with the safety protocols.

10 LIFE CYCLE MANAGEMENT OF IDENTITY

The companies of the Amper Group must define and implement an adequate system for managing the life cycle of identity. Identity is the set of characteristics that uniquely identify any person with physical or logical access to Amper Group information systems. The life cycle of identity is the process that follows the identity of a user from its creation to its elimination.

The life cycle of identity consists of the following activities:

a) Creation and allocation of identity

(b) Periodic review

(c) Modification or elimination

The management of this cycle requires defining the safety requirements and responsibilities of each stage, in order to centralize and facilitate the management processes associated with them.

The management of the identity life cycle should be aligned with the HR Department with the objective of verifying identities based on the high and low levels of employees and their correspondence in the information systems.

10.1 PRIVILEGED IDENTITIES

The allocation and use of privileged access rights shall be restricted and controlled. Privileged access is access to systems as an administrator or with a role that offers the possibility to modify the system settings.

The allocation of privileged access rights should be monitored through a formal authorisation process in accordance with access control policies. At least the following requirements shall be considered:

- The privileged access rights associated with each system or process (e.g. operating system, database management system or application) and the users to whom they are to be assigned should be identified.
- The allocation of privileged access rights should be carried out on the basis of use needs, based on the minimum privilege and need to know.
- An authorisation process including a registration of privileges should be defined privileged access rights should not be granted until the authorization process is completed.
- Requirements for the expiry of privileged access rights should be defined.
- The competences of users with privileged access rights should be reviewed regularly to verify that they are aligned with their obligations.
- Specific procedures and mechanisms should be established and maintained to avoid the unauthorized use of generic user accounts for administration, consistent with system configuration capabilities.
- Procedures and mechanisms should be established to ensure the confidentiality of secret authentication information for generic administration users (e.g. frequent password modification, secure password sharing mechanisms, etc.).

11 PHYSICAL AND ENVIRONMENTAL SECURITY

Physical spaces where Amper Group information systems are located must be adequately protected by perimeter access controls, surveillance systems and preventive measures so that the impact of security incidents (unauthorised access to information systems, theft or sabotage) and environmental accidents (fires, floods, power outages, etc.) can be prevented or mitigated.

12 WORKING SAFETY IN THE NUBBE

The Amper Group should maintain a cloud work policy that establishes appropriate security measures for confidentiality, integrity and availability of information. Depending on the type of cloud service model, different security measures should be applied:

- Infrastructure: First, the Provider must monitor the environment to detect unauthorized changes. In addition, strong levels of authentication and access control should be established for administrators and their operations. Finally, the installations and/or configurations of the common elements must be recorded and connected in order to obtain appropriate traceability.
- Platform: in addition to the measures indicated in the Infrastructure service model, the Service Provider shall provide security mechanisms corresponding to the life cycle of the secure software, in accordance with paragraph 15 Safety in the life cycle of system development
- Software: In addition to the measures indicated in the Platform Service Model, the Amper Group and the Provider must follow OWASP (Open Web Application Security) as a guide for application security.

13 SAFETY AT THE OPERATIONAL

All Amper Group information systems that process or store information on their property shall be provided with appropriate security measures that optimize their appropriate maturity level (monitoring, change control, revisions, etc.). Networks should also be properly managed, controlled and monitored to protect against threats and to maintain the security of the systems and applications that use it, including network access controls, by protecting information that is transferred through these elements and/or environments.

14 SAFETY ON TELECOMMUNICATIONS

The network architecture of the Amper Group should include prevention, detection and response measures to avoid gaps in internal and external domains. “Internal domain” means the local network composed of the Amper Group technology elements accessible exclusively from the internal network. On the other hand, “external domain” means the network accessible from outside the Amper Group network.

The security management of networks crossing the perimeter of the Amper Group is of the utmost importance, introducing additional controls for sensitive data that circulate through public communication networks.

The Amper Group will define the security guidelines to be followed on information transfer, security measures in the use of portable equipment, Internet and e-mail services, and specific controls to connect Amper Group information systems from outside its facilities.

15 LIFE CYCLE SAFETY IN SYSTEM DEVELOPMENT

All systems acquisition, development and maintenance shall have minimum security requirements necessary for software, systems and data development in line with industry good practice. In addition, test management, change monitoring, and software inventory should be carried out.

Each Amper Group society should take into account information security in its systems and data processes, selection procedures, development and implementation of applications, products and services.

16 SAFETY IN SOURCES

The criticality of the services that can be subcontracted should be assessed in order to identify those that are relevant from the point of view of information security, whether by their nature, the sensitivity of the data to be processed or the dependence on business continuity.

For the providers of these services, the selection processes, contractual requirements such as contractual termination, monitoring of service levels, data return and security measures implemented by that provider shall be taken care of, which shall be at least equivalent to those set out in this Policy.

17 INCIDENTS MANAGEMENT

All employees of the Amper Group have the obligation and responsibility to identify and notify the social security officer of any incident or offence that could compromise the security of their information assets. The Amper Group should also implement procedures for the proper management of detected incidents.

An incident management procedure should be defined, defining an incident categorization process, business impact analysis and scaling up by the information security and cybersecurity function in the event of any information security-related incident.

18 BUSINESS CONTINUITY

In response to quality requirements and good practices, the Amper Group must have a Business Continuity Plan as part of its strategy to ensure continuity in the provision of its

essential or critical services and the proper management of business impacts in the face of possible crisis scenarios, providing a frame of reference for society to act if necessary. This Continuity Plan should be updated and tested periodically. In addition, a Disaster Recovery Plan aligned with business continuity should be defined and kept up to date, and this plan will cover the continuity of the operation of information and communication technologies.

The Amper Group will be responsible for training and training all its employees in business continuity. Training in Business Continuity should be reviewed periodically with the aim of being fully aligned with the existing Plan.

19 SAFETY AUDITS AND VULNERABILITY MANAGEMENT

Technical vulnerabilities of the information systems and applications used in the organization should be regularly identified, depending on their exposure to such vulnerabilities and appropriate measures should be taken to mitigate the associated risk.

Once vulnerabilities have been identified, the organization should implement the necessary corrective measures as soon as possible. The identification, management and correction of vulnerabilities should be done in accordance with a risk-based approach, taking into account the criticality and exposure of assets.

20 ANNEXES

20.1 ANNEX: CLASSIFICATION LEVELS

Level	Detail Level	Examples
Public use	This is information that can be known by any type of person and its fraudulent use does not pose a risk to the interests of the Amper Group.	Examples of this type of information include product catalogs and the information available on the website
Limited dissemination	It is the information used by the areas of the Amper Group and whose fraudulent use poses a risk to the interests of the Group little significant.	Emails and working documents of the areas of the Group are examples of this type of information.
Confidential information	Information It is that	Examples of this type of

	information that can only be known by a small number of people and for which fraudulent use can have a significant impact on the interests of the Amper Group.	information are the audit and strategy reports of the Group.
Information Reserved	Reserved It is the information that should only be known to the owner of the same and whose disclosure can cause serious damage to the interests of the Group.	Examples are communications between senior managers or shareholders with decisions relevant to the operation of business.
Secret information	It is the one whose unauthorized disclosure can cause exceptionally serious damage to the essential interests of the Group.	Examples are cryptographic keys, information on mergers or acquisitions or any other information that may put the value of the action at risk.