## 1. Purpose and application scope

**1.1 Purpose.** This document establishes the information security principles and guidelines of the Abertis Group and provides the reference frame by which Abertis defines the information security guidelines, and standards under which all activities related to information processing will be governed within the Group.

The aim of the Information Security Policy, hereinafter referred to as 'the Policy' is to:

- Guarantee the protection of the Group information in accordance with the criteria of confidentiality, integrity, availability, accountability, and resiliency of data.
- Establish the general principles that the Group will apply for the protection of its information and associated assets.
- Provide guidelines for compliance with the laws and regulations associated with information security and mandatory compliance.
- Reference information security guidelines and associated documents for the secure handling of information.

**1.2 Scope of application.** This policy applies to all companies controlled[1] by the Abertis Group and to all third-party collaborators who have relationships with the Group when they have direct and/or indirect access to non-public information of the Abertis Group and/or non-public information managed by Abertis Group

The Managing Director in each company shall ensure that internal norms and standards are developed and adapted to this policy and applicable laws.

## 2. Basic principles

Information is one of the assets that adds more value to the Abertis Group and requires protection against illicit use, dissemination, alteration, destruction, theft or other misuse or illegitimate practices. The effective management of information security enables the treatment and reduction of risks caused by potential threats and vulnerabilities through the information lifecycle.

Abertis Group is committed to the protection of our people, our facilities, the Abertis businesses and brand through the following principles:

- Including the information security in all the processes, services and technologies following the principle of "security by design and by default".
- Raising awareness and training all employees on information security risks by providing mechanisms to detect, report and react to threats that may jeopardise information security.

[1] **Controlled companies:** companies in which Abertis owns more than 50% or otherwise where the shareholders' agreement states that Abertis holds a controlling stake.

- Managing information security risks based on a risk management methodology aligned with the Group standards and industry best practices.
- Complying with all legal, regulatory, industry and contractual obligations affecting information security in the jurisdictions in which the Group operates.
- Establishing the organizational, technical and control measures necessary to guarantee information security and business resiliency at each stage of the threat and incident management: identification, detection, prevention, response, and recovery.
- Ensuring information security in collaboration with third parties by identifying, analysing, mitigating, and monitoring information security risks and controls in the supply chain before, during and at the end of the contractual relationship.

This policy, where applicable, is aligned with best practice standards such as ISO/IEC 27002 "Code of Practice for Information Security Management", ISO/IEC 27701 "Privacy Information Management", ISO/IEC 22301 "Business Continuity Management Systems", ISO 3100 "Risk Management", NIST standards such as 800-14 "Generally Accepted Principles and Practices for Information Technology Systems Security", NIST 800-53 "Security and Privacy Controls for Information Systems and Organizations" or NIST 800-30 "Guide for Conducting Risk Assessments", CIS Critical Security Controls for Effective Cyber Defence (commonly known as "CIS Controls") and ISO/IEC 62443 "Industrial Network and System Security".

It is essential that the Group's professionals are aware of the importance of information security as part of their daily business activity. For this reason, they are encouraged to actively participate in its development and continuous improvement to provide a safer environment for all.

## 3. Specific guidelines

**3.1 Responsibilities.** The security of information and the assets supporting it is the responsibility of each collaborator and Third Parties who collaborate with the Abertis Group, who will actively participate in this responsibility by acting ethically with respect to the protection of information, complying with contractual obligations regarding information security and guaranteeing that they will only use the information and information systems for the purpose established by Abertis Group.

Abertis shall establish, write, and maintain the Group's Information Security Policy to reflect current international security standards, general business requirements and general legal and regulatory requirements. Additionally, Abertis is responsible for the development of the framework for the information security governance throughout all the Group considering business requirements, risks identified, the state-of-the-art technology, controls, and security measures applicable.

**3.2 Information Security Framework.** Aligned to the group regulations, each Business Unit should develop its own internal information security policy body, which will establish at least:

- Management commitment.
- The company's approach to managing information security.
- The definition and assignment of generic and specific responsibilities in matters of information security management and operation.

In relation to the protection of the information, the information security body has to regulate and provide guidance over the following areas:

- Information security governance: including not only the governance committees, but also the periodical review and update of standards, guides, and procedures to adapt them to the business changes and needs as well as the evolution of risks and protection systems.
- Information security risk management: applying a risk methodology and managing information security risks and controls accordingly.
- Organization of information security: assignment of responsibilities, segregation of duties, contact with authorities and special interest groups, as well as security in project management.
- Human resource security: aspects related with user permissions and roles and that should be considered before, during and for the termination or change of employment.
- Asset management: asset responsibilities, information classification and management of assets containing information.
- Access control: access requirements, user responsibilities and information asset access.
- Cryptography controls.
- Physical and environmental security: ensuring the protection of areas and equipment storing sensitive information.
- Operations security: procedures and responsibilities, vulnerability management, threat protection, backup management, activity logging, monitoring, and systems auditing.
- Communications and network security, including information transfer.
- Operation Technology (OT) security, including all the particularities for the information security management in the industrial systems.
- System acquisition, development, and maintenance: applying security throughout the software lifecycle (SSDLC).
- Safe use of artificial intelligence solutions.
- Supplier relationship: assessing the information security risk of suppliers and implementing appropriate controls before, during and after the contractual relationship.
- Information security incident management considering all the stages of an incident form the detection, analysis, response, recovery, communication to stakeholders and lessons learned.

- Business continuity management including Business Continuity Plan ('BCP') and Disaster Recovery Plan ('DRP') management.
- Compliance: enforcement of the legal, regulatory, and contractual requirements, as well as reviewing the Policy compliance.

Information Security Policies, guidelines, standards, and procedures should be periodically reviewed and updated to adapt them to the business changes and needs as well as the evolution of risks and protection systems.

## 4. Monitoring and control

- Each company's internal rules and standards must establish the monitoring and control mechanisms used to identify and report any irregularity in compliance with Group policy.
- Abertis reserves the right to request each company to apply the internal controls considered necessary by Abertis.
- Abertis will also measure the level of compliance across all Business Units on a periodic basis using a formal assessment process.
- All exceptions to this Policy should be in writing, follow formal procedures and be formally approved by the Abertis Group management.
- This Policy should be reviewed by the policy owner at least on an annual basis to ensure that the contents remain aligned to the business needs, risk posture and information security requirements.

Information Security Policy_v2
Publication date: 11/12/2024
Approved by: Chief Executive Officer