INFORMATION SECURITY POLICY

Referenc	31_Information Security Policy_4_2024
Title of the Standard	Information Security Policy
Geographical scope	Global
Category	Policy
Date of approval	19 December 2024
Approval body	Board of Directors
Current version	19 December 2024

INDEX

1. Introduction

The Board of Directors of ACS, Actividades de Construcción y Servicios, S.A. (hereinafter referred to as "**ACS**" or the "**Company**"), in its capacity as a listed company, is legally entrusted with the non-delegable authority to determine ACS's general policies and strategies. This authority is also established in the Bylaws of the ACS Board of Directors.

ACS and the companies forming part of the Group, of which the Company is the parent entity (hereinafter, the "**ACS Group**" or "**Group**"), are committed to ensuring the security of information, networks, and Information Systems supporting various business processes, with the goal of enhancing their Digital Operational Resilience. They align their practices with applicable regulations and corporate values.

In this regard, ACS is committed to developing and implementing the highest capabilities in information security to mitigate threats to information, networks, and Information Systems used within the organization.

In line with the above, the Company's Board of Directors has approved this *Information Security Policy* (hereinafter, the "**Policy**"), which serves as the cornerstone of ACS's Information Security Management System and is integrated into the Company's Governance System, with projection over the ACS Group.

2. Definitions

The following definitions apply to this Policy and all associated procedures within ACS, without prejudice to its projection across the Group:

- ***Governance and Compliance Committee****:* The ACS body assigned general Compliance functions, as well as specific functions related to each identified Compliance Area. It also provides consultative and support functions regarding governance for coordination purposes when required by the Head of Corporate Governance, the Artificial Intelligence and Cybersecurity Manager (CISO), the Head of Sustainability, and the Data Protection Officer (DPO).
- ***Cybersecurity****:* All activities aimed at ensuring both information security and the protection of networks, Information Systems, their Users, and other individuals potentially affected by cyber threats.
- ***Personal Data****:* Any information about an identified or identifiable natural person. This includes any data that directly or indirectly can be used to identify an individual, such as names, photographs, email addresses, bank details, social media information, location, or a computer's IP address, among others. Personal Data is protected by various regulations, and proper practices must be followed for its collection, processing, and storage to respect the privacy rights of the individuals involved.

- ***Artificial Intelligence and Cybersecurity Manager (CISO)**:* Responsible for the security of networks and Information Systems.
- ***Risk Control and Management**:* Coordinated activities to direct and manage identified Risks within ACS.
- ***Incident Management**:* A set of measures and procedures aimed at preventing, detecting, analyzing, and mitigating an Incident. This includes resolving the Incident and incorporating performance measures to evaluate the protection system's quality and detect trends before they become major issues.
- ***Cybersecurity Incident or Cyber Incident**:* An unexpected or undesired event that could compromise the availability, authenticity, traceability, integrity, or confidentiality of stored, transmitted, or processed data, or services provided by or accessible through Network and Information Systems.
- ***Information**:* A key asset of any company that may exist in physical or digital format. It includes all types of files (text, images, multimedia, databases), programs and applications that manage such files, and the equipment and systems supporting these services.
- ***Professional**:* Members of governing bodies, executives, employees, collaborators, interns, and trainees, regardless of the legal framework defining their labor or service relationship, hierarchical level, geographic or functional location, or the specific ACS Group entity they serve.
- ***Principle of Authenticity**:* Ensures that the origin and identities associated with the information are as stated in its attributes. This principle is tied to non-repudiation, which guarantees that a User cannot deny authorship of an action in the system or association with a specific data set.
- ***Principle of Confidentiality**:* Ensures that information is accessible only to authorized Users and cannot be disclosed to third parties without proper authorization.
- ***Principle of Availability**:* Ensures that information is consistently accessible and usable, guaranteeing the continuity of processes and activities. This principle is tied to resilience, which ensures the recovery capability of systems and information following an Incident that temporarily prevents access.
- ***Principle of Integrity**:* Ensures that data remains free from unauthorized modifications and that existing information has not been altered by unauthorized persons or processes.
- ***Principle of Traceability**:* Ensures the ability to determine at all times the identity of individuals accessing information, their activities concerning it, and the different states and paths the information has followed.
- ***Digital Operational Resilience**:* The entity's ability to build, secure, and review its operational integrity and reliability, directly or indirectly ensuring the use of services provided by third-party ICT providers. This includes the full range of ICT-related capabilities necessary to preserve the security of the networks and Information Systems used by the entity, ensuring the continuity and quality of service delivery, even in the event of disruptions.

- ***Risk**:* The potential loss or disruption caused by an Incident, expressed as a combination of the magnitude of such loss or disruption and the likelihood of the Incident occurring.
- ***Information Security Management System (ISMS)**:* A set of information security policies and procedures designed to create, maintain, and improve a structured organization and management system. The ISMS ensures the confidentiality, integrity, and availability of information assets while minimizing Information Security Risks, considering the analyzed Risks within ACS's business processes. This Policy serves as its foundation.
- ***Information System**:* A discrete set of information resources supporting business applications or services, organized to collect, process, maintain, use, share, distribute, or dispose of information.
- ***Network and Information System**:* i) interconnected devices; ii) transmission systems (with or without permanent infrastructure or centralized management capabilities), switching or routing equipment, and other resources, including non-active network elements that enable signal transport via cables, wireless waves, optical means, or other electromagnetic methods. This includes satellite networks, fixed networks (circuit-switched and packet-switched, including the internet), mobile networks, power grid systems (when used for signal transmission), networks for sound and television broadcasting, and cable television networks, regardless of the type of information being transmitted.
- ***Data Processing**:* Any operation or set of operations performed on Personal Data, or data sets, whether by automated processes or not, such as collection, recording, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, communication by transmission, dissemination or any other form of enabling access, alignment or combination, restriction, erasure, or destruction.
- ***User**:* Any person linked to ACS through a civil or commercial relationship, as well as clients, suppliers, subcontractors, consultants, or any other individuals or entities authorized to use, manage, or access Corporate AI Assets (as defined in the Artificial Intelligence Policy).
- ***Vulnerability**:* Any weakness, susceptibility, or defect in an asset, system, process, or control that can be exploited.

Unless expressly stated otherwise in any section of this Policy, singular definitions include the plural and vice versa.

3. Purpose

The purpose of this Policy is to establish the basic principles and general rules that enable ACS, with projection over the Group companies, to develop information security strategies, procedures, and standards to maintain a robust Information Security Management System (ISMS). This aims to strengthen the appropriate operational and control framework, aligned with business objectives, for managing ACS’s information security.

In line with this purpose, the Policy seeks to implement processes and technologies within ACS, with projection over the Group companies, that ensure the security of information, networks, Information Systems, and ACS operations. These measures aim to minimize Risks and cyber threats to which they are exposed, thereby enabling the fulfillment of its corporate purpose toward clients and other stakeholders. This includes ensuring continuity in service delivery by acting preventively, supervising daily activities, and responding diligently to Incidents.

4. Scope of application

This Policy applies to the entire ACS organization, as well as to suppliers and clients providing services or maintaining relationships with ACS, projecting itself onto ACS Group companies.
In those affiliated companies where this Policy is not directly applicable, ACS will, to the extent possible, promote alignment of their policies with those of ACS through its representatives on their governing bodies.

This Policy will also apply, as appropriate, to temporary business alliances, *joint ventures*, and other equivalent associations, whether domestic or international, where any of the companies within the ACS Group have control over their management, always within the legally established limits.

5. General Principles of Action

ACS understands information security as a fundamental element to protect business assets, considering it an integral process based on risk management and control to achieve its objectives and fulfill its mission. In this regard, ACS is committed to providing the different areas of the organization with all the technical, human, material, and organizational resources necessary to ensure adequate management of the security of ACS's networks and Information Systems.
Specific procedures will be established to ensure that all Professionals and Users are aware of, understand, and comply with the Policy and all its associated regulations.
In accordance with the above, all Professionals and Users of ACS must respect and guide their actions based on the following principles:

I. **Integral Process Based on Risk Management and Control:** ACS carries out information security management based on the principles of risk management and control defined in the Group's General Policy on Risk Control and Management, which is built on the common methodology established in the Comprehensive Risk Control and Management System included in said policy:

    - Identification and evaluation of risks.
    - Definition of acceptable risk levels.
    - Establishment of control and mitigation mechanisms.

- Strengthening decision-making.
- Continuous monitoring and review.

Which are reflected in the Security Master Plan, which is continuously updated.

II. **Definition, Development, and Maintenance:** To achieve the implementation of the objectives, values, strategy, and commitments undertaken, ACS will promote the development of a Management System composed of the technical, legal, and management controls necessary for information security to ensure compliance at all times with the applicable legal, regulatory, and contractual requirements in this area.

III. **Promotion of a Culture of Information Security:** ACS commits to actively promoting a culture of information security among all its Professionals and Users, whether internally or among its clients and suppliers.

IV. **Daily Management:** This implies ACS's commitment to protecting the security of information, networks, and Information Systems by designing robust security measures aligned with the needs of the different stakeholders and the applicable regulations in this area. For this purpose, ACS will approve specific policies and/or procedures by subject matter that will develop the fundamental principles and security requirements established in this Policy.

V. **Proactive Protection:** Proactively pursuing the safeguarding of the established levels of confidentiality, availability, authenticity, traceability, and integrity of its information assets and ensuring ACS's Digital Operational Resilience.

VI. **Continuous Improvement:** Understanding information security as a transversal axis integrated into all areas and business processes, seeking uninterrupted progress in all processes linked to the ISMS and the management of information security, networks, and Information Systems, in such a way that it contributes to making all of ACS's operations digitally resilient.

The aforementioned general principles of action shall be projected onto the ACS Group companies.

6. Basic information security requirements

To carry out the daily management of security, the following basic requirements will always be adhered to:

- Establish security requirements by design and by default.
- Prevention, detection, response, and preservation.
- Continuous monitoring and periodic reevaluation.
- Differentiation of responsibilities.

- Organization and implementation of the security process.
- Risk analysis and management.
- Personnel management.
- Authorization and access control.
- Protection of facilities.
- Procurement of security products and contracting security services.
- Minimum privilege.
- Integrity and updating of the Information System.
- Protection of stored and in-transit information.
- Prevention regarding interconnected Information Systems.
- Activity logging and detection of malicious code.
- Security incidents.
- Continuity of operations.
- Continuous improvement of the security process.
- Security in the supply chain.
- Reliability, security, and resilience.

Each of these requirements will be developed through the corresponding procedures and/or specific policies approved internally.

All information security documentation developed in execution of these principles and forming part of the ISMS is managed, structured, and preserved in accordance with the documented procedures that ACS has developed, taking into account applicable regulations as well as relevant national and international standards.

The aforementioned basic information security requirements and their development shall be projected onto ACS Group companies.

7. Governance

The governance of Information Security at ACS is essential for managing and mitigating potential Risks, ensuring decision-making based on the actual risk of threats materializing against the organization, and guaranteeing the continuity of business operations. This Policy serves as a fundamental tool for the proper management and governance of information security.

7.1. Management and monitoring guidelines

The Board of Directors of ACS is responsible, through this Policy and, where appropriate, other corporate regulations implementing it, for establishing the strategy and management guidelines with projection over the ACS Group in matters of information security.

In turn, it is the responsibility of the Audit and Sustainability Committee, through its supervisory and control functions, to monitor the implementation and development of this Policy and the measures adopted in its application, as well as to review and, where appropriate, propose updates to this Policy for approval by the Board of Directors.

Additionally, the Audit and Sustainability Committee is responsible for supervising the effectiveness of ACS's ISMS.

To carry out its supervisory functions, the Audit and Sustainability Committee will periodically receive information on its management from the CISO.

7.2. Artificial Intelligence and Cybersecurity Manager (CISO) and the Governance and Compliance Committee

7.2.1. Principles for action

Through the CISO, ACS will observe and promote the following principles regarding the governance of information security:

a) Principle of Strategic Alignment and Future Vision

Information security will be considered an integral part of the business, understood as a tool that helps ACS achieve its objectives, aligned with the Group's mission and vision.

Consequently, ACS will foster a holistic approach to ensure that information security is not perceived as an obstacle but as part of a broader framework necessary for business development.

b) Principle of Ethics and Compliance

It should guide information security governance at ACS, focusing not only on compliance with established regulations, but also on good security practices and the ethical use of Group resources.

In order to foster ethical and responsible action, ACS will promote collaboration with the best practices in this area, both within ACS and in each of the markets in which it operates and in its connection with the various stakeholders.

c) Principle of accountability

Information security is an interdisciplinary and complex field that impacts all of an entity's operations. Therefore, it requires appropriate leadership and a structure established and managed by professionals with the necessary training and experience.

d) Principle of independence and autonomy

The CISO must operate with complete independence and autonomy in the performance of their duties, thereby ensuring impartiality and objectivity. Functionally, the CISO will report to the Audit and Sustainability Committee.

7.2.2. Roles of the Head of Intelligence and Cybersecurity (CISO)

It will report to the Head of Artificial Intelligence and Cybersecurity (CISO):

- Review this Policy, ensuring that it complies with the regulations applicable to ACS and its Group, as well as with the best practices in the sector. In this regard, when it deems it appropriate, it may submit proposals to amend this Policy to the Audit and Sustainability Committee, for submission to the Board of Directors.
- Review and promote the continuous improvement of ACS's ISMS, including, where appropriate, the identification and assessment of new risks associated with the ISMS.
- Coordinate the continuity plans of the information systems of the different ACS areas to ensure seamless action in the event that they need to be activated.
- Regularly inform senior management and different ACS areas through the Security Master Plan regarding the security and control measures adopted, recommending possible actions in this regard.
- Coordinate and monitor the performance of security incident management processes in the area of information security
- Promote periodic audit processes to verify compliance with applicable regulations.
- Promote training and skills development related to information security in ACS.
- Monitor compliance with the applicable regulations.
- Approve internal procedures, standards or protocols for the development and implementation of this Policy at ACS.
- Establish and promote information security and participate in decision-making and strategy in this field, taking responsibility for providing appropriate periodic reporting at appropriate levels on Information Security Risks, together with the required mitigation and control mechanisms.

The CISO shall also be responsible for monitoring the performance of these functions by the equivalent bodies or bodies of the Group companies in order to supervise the implementation of the principles and commitments that inspire this Policy, and may request from such companies any information it deems necessary to fulfil this coordination function at the Group level.

In performing these functions, the CISO shall be supported by the Governance and Compliance Committee.

7.3. Decentralisation and coordination at Group level

The ACS Group is structured according to a decentralised management model and carries out its activity through a large group of companies, which share the ACS Group's culture and values, while each one operates independently in its respective functional and responsibility areas.

In this regard, the information security strategies, procedures and standards to be followed in order to maintain a sound ISMS are the responsibility of the various Group companies within the framework of their respective functional areas and areas of responsibility.

In this regard, the ACS Group companies shall be responsible for implementing, supervising, adapting and managing the strategies and organisational model in the area of information security within their respective areas of activity, establishing their own internal policies and rules in this area, taking into account the regulations applicable in each case and their own characteristics, respecting the basic principles established in this Policy.

In any case, ACS Group companies shall provide all the information necessary for the definition of the Group's information security strategy and, likewise, for the fulfilment of all obligations corresponding to ACS in this area in accordance with applicable regulations.

8. Risk Management and Control

All systems subject to this Policy must carry out a risk analysis, assessing the threats and Risks to which they are exposed. ACS periodically and continuously carries out a risk analysis of the threats affecting information security, as developed in the corresponding procedure

9. Incident Management

The areas that make up ACS must avoid, or at least prevent as far as possible, information or services from being damaged by cybersecurity incidents. To this end, in accordance with the provisions of the corresponding procedure, these areas must implement the minimum security measures determined by the applicable regulations, as well as any additional controls identified through a threat and risk assessment, at .

10. Monitoring, Interpretation and Review

10.1. Follow-up

Compliance with this Policy will be monitored by the CISO. Periodic audit and review mechanisms shall be established to ensure that the ISMS complies with the established standards.

In the event of a problem or detection of an incident that may affect the operation or security of the Network Systems and systems, and/or the security thereof, the CISO must be notified immediately through the channels provided for this purpose and which shall be determined in the ISMS procedures.

As a metric, the results of the Vulnerability management process shall be documented on a monthly basis, including the list of managed Vulnerabilities, as well as whether they have been corrected and, if so, the measures taken.

Failure to comply with this Policy may lead to legal liabilities of various kinds as provided for in current legislation, entitling ACS, if deemed necessary, to initiate the appropriate legal action.

10.2. Interpretation

The contact body for any doubts and/or queries in relation to the interpretation and execution of this Policy shall be the CISO. Communication with the CISO shall be carried out through the channels provided for this purpose.

10.3. Review and Update

This Policy will be reviewed and, where appropriate, updated periodically to adapt to the needs and/or regulatory, organisational, technical and process changes of ACS and its Group, as well as to incorporate the best practices identified in the ISMS.

The modification and/or updating of this Policy shall be approved by the Board of Directors of ACS, following a report from the Audit and Sustainability Committee .

11. Dissemination of the Policy

This Policy will be published on the ACS corporate website, with the consequent knowledge and assumption of its full content by Professionals and Users.

Notwithstanding the foregoing, ACS will periodically carry out communication, training and awareness-raising actions for the understanding and implementation of this Policy, as well as its updates. ACS will also disseminate this Policy in ACS Group companies.

In any case, it is the responsibility of all Users and Professionals to read and understand the content of this Policy, as well as to observe and comply with its guidelines, principles and processes in the performance of their work, insofar as ignorance of all or part of its content does not exempt them

from compliance with it. In this regard, it is recommended to periodically access the content of this Policy through the channels available for a better understanding of the same.

12. Entry into force

This Policy was approved by the Board of Directors of ACS at its meeting held on 19 December 2024, coming into force from the moment of its publication on the ACS corporate website.