SUARDIAZ Group

PL 16.2_1

INFORMATION SECURITY POLICY

CHANGE HISTORY

Issue	Date	Page	Description of change
01	15/09/2026		Initial Issue

INTERNAL DISTRIBUTION LIST

Person/Position	Date	Method
IT Department	15/09/2026	Shared on the network

ELABORADO	REVIEWED	APPROVED
Ciriaco Guisasola Alonso Information & Technologies Director	Laura Rodriguez Caviedes Integrated Management System Coordinator (QHSE)	Laura Cajade Frías Compliance & Sustainability (ESG) Director
15/09/2026	15/09/2026	15/09/2026

Controlled Copy

Uncontrolled Copy

ALL RIGHTS RESERVED

SUARDIAZ Group owns the original of this document. Copies supplied are confidential and may not be used for purposes other than those for which they were requested, nor may they be reproduced without the authorisation of SUARDIAZ Group. Anyone other than an authorised person who finds this document must send it to: C/ de Ayala, 6, 28001 Madrid, Spain, or via the contact form on the website: https://www.suardiaz.com.

Contenido

1. PURPOSE 1
2. SCOPE 1
3. REFERENCE DOCUMENTS 1
4. DEFINITIONS 2
5. RESPONSIBILITIES 2
6. GENERAL INFORMATION SECURITY PRINCIPLES 4
   6.1 Context and interested parties 4
   6.2 Information protection and classification 5
   6.3 Risk and opportunity management 5
   6.4 Threat intelligence 6
   6.5 Compliance with applicable requirements 7
   6.6 Information security objectives 8
   6.7 ISMS continual improvement 9
   6.8 Roles, responsibilities and authorities 9
7. POLICY COMMUNICATION 10
8. POLICY REVIEW, UPDATE AND CONTROL 11
9. RELATED DOCUMENTATION 11
10. ANNEXES 11

1. PURPOSE

The purpose of this document is to establish the SUARDIAZ Group Information Security Policy as the general framework for protecting the confidentiality, integrity and availability of information, and, where appropriate, its authenticity and traceability, within the scope of the Information Security Management System (hereinafter, the ISMS), in accordance with ISO/IEC 27001:2022. This policy covers the protection of information and the assets, services, processes and environments that support it, regardless of its format, medium, location or method of processing.

2. SCOPE

This policy applies to SUARDIAZ Group and is mandatory for all areas, processes, information systems, assets, employees and third parties included within the scope of the ISMS. It applies to all information managed within that scope, regardless of its format, medium or method of processing.

This policy provides the overall framework with which the ISMS rules, procedures and other documents must comply, in line with the approved scope and the applicable requirements identified by the organisation.

The protection established by the ISMS extends to the information, the systems that process it, and the technological assets, support services, infrastructures and associated environments included within its scope. Where applicable, it also covers services provided by third parties whose disruption or compromise could affect the information security of SUARDIAZ Group.

3. REFERENCE DOCUMENTS

Reference documentation for this policy includes, among other applicable ISMS documentation, ISO/IEC 27001:2022, ISO/IEC 27002:2022, the ISMS Management and Description Document, the context and interested parties analysis, the roles and responsibilities documentation, the information security objectives, the Statement of Applicability, and the current documentation on communication and control of documented information.

Likewise, this policy shall be interpreted consistently with the legal, regulatory, contractual and corporate framework applicable to SUARDIAZ Group in relation to

information security, business continuity, use of technological assets, personal data protection, intellectual property, confidentiality and any other obligations relevant within the scope of the ISMS, including, where applicable, Regulation (EU) 2016/679 (GDPR) and Organic Law 3/2018 (LOPDGDD

) and other relevant sector-specific or contractual provisions.

4. DEFINITIONS

ISMS: Information Security Management System established, implemented, maintained and continually improved by SUARDIAZ Group in accordance with the applicable requirements of ISO/IEC 27001:2022.

Information security: preservation of the confidentiality, integrity and availability of information, and, where appropriate, other relevant properties such as authenticity and traceability.

Relevant interested parties: persons or organisations that can affect, be affected by, or perceive themselves to be affected by the performance of the ISMS, and whose requirements are relevant to information security within the defined scope.

Information systems: the set of applications, services, infrastructures, networks, equipment, media and other technological resources, whether owned by the organisation or provided by third parties, that enable information within the scope of the ISMS to be processed, stored, transmitted or safeguarded.

Information classification: the process by which information and, where appropriate, associated assets are categorised according to their sensitivity, criticality, value and applicable requirements, in order to determine the appropriate protection measures.

Information asset: information, system, service, process, medium, infrastructure, application, equipment, facility or any other resource that has value to the organisation and whose impairment could compromise information security or the continuity of activities included within the scope of the ISMS.

5. RESPONSIBILITIES

Top Management demonstrates leadership and commitment to information security, approves this policy, ensures its alignment with the organisation's strategic direction and ensures that the resources required to establish, implement, maintain and continually improve the ISMS are available. In exercising this leadership, SUARDIAZ Group undertakes to meet the applicable ISMS requirements and to

continually improve its suitability, adequacy and effectiveness as the basis for protecting information within the defined scope.

Top Management also promotes a security culture, supports the integration of the ISMS into business processes and backs the decision-making required to maintain an appropriate level of protection against the risks identified.

Information security responsibilities shall be assigned consistently with the organisational structure defined by SUARDIAZ Group, promoting, where appropriate, segregation of duties and avoiding undue concentration of critical tasks in a single person.

The ISMS Manager oversees the management, maintenance, review, document control and updating of this policy, coordinates its implementation within the scope of the ISMS and reports to Top Management on system performance and identified improvement needs.

The ISMS Manager also ensures consistency between this policy and the other documented information of the ISMS, and coordinates its review whenever organisational, regulatory, technological or risk-related changes require it to be updated.

All personnel and, where applicable, third parties included within the scope of the ISMS must be aware of, comply with and apply this policy and the guidelines that implement it, contributing to the effectiveness of the system and compliance with the information security requirements established by the organisation.

This duty entails acting diligently in relation to the information and assets under their responsibility, complying with applicable internal rules and cooperating in ISMS awareness, monitoring, review and continual improvement activities.

In particular, persons included within the scope of the ISMS must use information and information systems appropriately for their duties, protect the confidentiality of the information they access and promptly report, through the channels defined by the organisation, any incident, weakness, misuse or situation that could compromise information security. This obligation forms part of a formal information security incident management framework that proportionately covers identification, recording, assessment, classification, response, escalation, resolution, recovery and lessons learned from incidents. This framework is implemented through PR16.10, the Information Security Incident Management Procedure currently in force within the organisation.

Reporting shall cover not only confirmed incidents but also vulnerabilities, control weaknesses or observed situations which, even if they have not materialised, could

increase information security risk and require assessment or treatment by the organisation.

Where the engagement, supervision or management of third parties involves access to information, systems or services included within the scope of the ISMS, the associated risks shall be considered and appropriate control, supervision and formalisation measures shall be applied in accordance with the information security requirements defined by SUARDIAZ Group.

6. GENERAL INFORMATION SECURITY PRINCIPLES

This policy establishes a general framework for protecting information and assets included within the scope of the ISMS, promoting the consistent, structured and proportionate application of information security measures according to identified risks and applicable requirements. In this context, the organisation shall consider, among other matters, access control, identity and privilege management, cryptography, physical and environmental security, operations security, logging and monitoring, vulnerability management, business continuity, security in relationships with third parties and the protection of documented information, without prejudice to the specific requirements set out in ISMS rules and procedures.

6.1 Context and interested parties

This policy is established taking into account the organisation's purpose, its internal and external context, and the needs and expectations of interested parties relevant to the ISMS.

SUARDIAZ Group determines and analyses these elements as the basis for managing information security appropriately in relation to its operating environment and applicable requirements. This information is recorded in the 'Interested Parties Document'.

The guidelines in this policy are applied consistently with the context analysis, interested parties and applicable legal, regulatory, contractual and organisational requirements, and are reviewed whenever relevant changes occur.

Where applicable, SUARDIAZ Group shall maintain appropriate contacts with relevant interested parties in the field of information security, including authorities, regulatory bodies, customers, suppliers, industry associations and other relevant stakeholders, in order to facilitate coordination, awareness of applicable requirements and the exchange of information needed for effective ISMS management. All relevant contacts, who must communicate, what is to be

communicated, in which circumstances and through which channel are set out in the Communication Plan document.

6.2 Information protection and classification

Information managed within the scope of the ISMS shall be protected according to its value, sensitivity, criticality and applicable requirements, promoting classification criteria and proportionate protection measures throughout its life cycle, regardless of its format, medium, location or method of processing. To this end, the organisation shall establish and maintain defined classification criteria that distinguish, at a minimum, between Public, Internal Use, Confidential and, where appropriate, Restricted or equivalent information, associating proportionate requirements for access, handling, storage, transmission, retention and deletion with each level. The specific development of the criteria for classification, labelling, handling and review of information shall be set out in the Information Classification Procedure currently in force within the organisation.

Access to information and systems included within the scope of the ISMS must be restricted according to business needs and assigned duties, applying need-to-know and least-privilege principles and, where appropriate, segregation of duties, in order to reduce the risk arising from inappropriate access or incompatibilities in the allocation of responsibilities.

Information assets and systems made available to persons included within the scope of the ISMS shall be used exclusively for authorised purposes and in the performance of their respective professional duties, in accordance with internal rules and the security measures established by the organisation.

The organisation shall promote the identification of relevant information assets, the assignment of responsibilities for them, and their classification and periodic review where necessary, in order to apply protection measures appropriate and consistent with their criticality, use and applicable requirements.

6.3 Risk and opportunity management

SUARDIAZ Group adopts a risk-based approach to information security management. During ISMS planning, operation and improvement, risks and opportunities that may affect the achievement of the system's intended outcomes are identified, analysed, evaluated and addressed.

The organisation maintains risk assessment and acceptance criteria, determines appropriate risk treatment options, selects the necessary controls and documents these decisions in the ISMS documented information, including the Statement of Applicability and, where applicable, risk treatment plans.

Risk treatment is aimed at protecting information and associated assets through appropriate and proportionate organisational, physical and logical measures, which are periodically reviewed to ensure the effectiveness of the ISMS as the context and risks evolve.

Actions to address risks and opportunities are integrated into ISMS processes and, where applicable, into the processes affected by the scope. Their effectiveness is evaluated to contribute to the achievement of intended outcomes and the continual improvement of the system.

SUARDIAZ Group shall promote the integration of information security into the management of projects, significant changes and initiatives that may affect information, assets, systems, services or processes included within the scope of the ISMS, regardless of their nature. In such cases, applicable security requirements, associated risks, necessary protection measures, responsibilities involved and the potential impact on the confidentiality, integrity, availability, authenticity or traceability of information shall be considered from the initial planning stages and throughout implementation, consistently with ISMS principles, risk management and business needs.

Within this framework, SUARDIAZ Group expressly considers risks arising from security incidents, operational disruptions, unauthorised access, information leakage or loss, service unavailability and dependencies on third parties that may affect the confidentiality, integrity, availability, authenticity or traceability of information. The organisation shall promote proportionate treatment of these risks, aimed not only at preventing and mitigating them but also at strengthening response and recovery capabilities in situations that could compromise the continuity and reliability of activities included within the scope of the ISMS.

The organisation shall also promote measures to ensure the continuity of activities included within the scope of the ISMS and the recovery of affected information and services in the event of incidents or disruptive situations, at a level appropriate to the criticality of the affected processes and assets.

In addition, SUARDIAZ Group shall promote the physical and environmental protection of facilities, equipment, media and environments that support information included within the scope of the ISMS, at a level appropriate to the risk and criticality of the assets concerned.

6.4 Threat intelligence

SUARDIAZ Group shall promote the gathering, review, analysis and use of information on information security threats and cyber threats relevant to the

organisation, taking into account its context, activities, assets, services, relationships with third parties and the risks applicable to the scope of the ISMS.

Where relevant, this information may come from internal and external sources, including alerts from manufacturers and suppliers, information associated with the technology services used by the organisation, internal incidents or weaknesses, information obtained from relevant third parties and other specialised sources that are reasonable and proportionate to the nature of SUARDIAZ Group. The organisation shall review this information at appropriate intervals and assess its applicability and potential impact on its operations, assets and services.

The outcome of this analysis shall be converted into useful knowledge to anticipate risk scenarios, support decision-making, strengthen preventive capabilities, improve the detection of and response to events and incidents, review the suitability of implemented controls, prioritise treatment actions and promote continual improvement of the ISMS. Where appropriate, the information analysed may lead to risk reviews, control updates, the adoption of preventive or corrective measures, follow-up or monitoring activities, communication to relevant internal or external parties, and retention of the documented information needed to evidence its consideration and treatment within the ISMS.

For these purposes, the organisation shall consider, among others, threats relating to unauthorised access, phishing or impersonation campaigns, malware or ransomware, information leakage or loss, exploitable technical vulnerabilities, service unavailability, configuration errors, compromises involving third parties and any other scenario which, due to the nature of SUARDIAZ Group and its operations, may affect the confidentiality, integrity, availability, authenticity or traceability of information.

6.5 Compliance with applicable requirements

SUARDIAZ Group undertakes to comply with the legal, regulatory and contractual requirements applicable to information security within the scope of the ISMS, as well as the obligations undertaken towards customers, employees, third parties and other relevant interested parties.

The organisation periodically reviews the suitability of its guidelines and controls to keep the ISMS aligned with the regulatory framework and applicable commitments, taking the necessary measures when changes or deviations are identified. Information relating to these requirements is recorded in the Legal, Regulatory and Contractual Requirements Document.

Likewise, where the organisation authorises the use of artificial intelligence tools in processes included within the scope of the ISMS, their use must be controlled and comply with applicable requirements, safeguarding the confidentiality, integrity and availability of information, as well as personal data protection, intellectual property and any other applicable obligations.

This commitment also extends to the information security requirements to be observed in relationships with suppliers, partners and other third parties included within the scope or having access to information, systems or services relevant to SUARDIAZ Group. The organisation shall promote the management of such relationships in a manner consistent with the associated risks and the contractual, legal or regulatory obligations applicable in each case.

When SUARDIAZ Group outsources activities or engages services involving access to information, systems or processes included within the scope of the ISMS, it shall ensure that such services are subject to an appropriate risk assessment and that security, confidentiality, continuity, notification and compliance requirements are formally established and, where appropriate, monitored throughout the contractual relationship. This entire assessment process is documented in the Third-Party Security Management Procedure.

6.6 Information security objectives

This policy provides the framework for establishing, reviewing and monitoring information security objectives at the relevant functions and levels of the organisation. These objectives must be measurable and assessable, and consistent with this policy, the results of risk management, applicable requirements and business needs.

SUARDIAZ Group promotes the communication and monitoring of information security objectives and ensures that they are supported by the resources needed to achieve them, so that they contribute to the effectiveness of the ISMS and the appropriate protection of information.

In particular, information security objectives may focus, among other things, on strengthening prevention, detection, response and incident recovery capabilities; improving personnel awareness; reinforcing oversight of relevant third parties; and ensuring the appropriate protection of the assets and services supporting information included within the scope of the ISMS.

Likewise, the objectives may include strengthening information security training and awareness, verifying the effectiveness of implemented controls and progressively

improving the level of compliance with applicable security requirements within the scope of the ISMS.

The organisation shall also promote appropriate information security training and awareness for new joiners, internal personnel and, where relevant, relevant third parties, according to their responsibilities and their level of access or exposure to associated risks.

All security objectives are recorded and defined in the Information Security Objectives Document.

6.7 ISMS continual improvement

SUARDIAZ Group remains committed to continually improving the suitability, adequacy and effectiveness of the ISMS, based on monitoring system performance, audit results, management reviews, changes in the context and risks, and the identification of improvement opportunities.

The organisation promotes the adoption of corrective actions and improvements, as well as documentary and operational adjustments where necessary, to ensure that the ISMS remains appropriate to the organisation's purpose and effective in response to internal and external changes.

As part of this commitment, the organisation appropriately addresses detected deviations, takes corrective action where necessary and uses the results of monitoring, audits and reviews to strengthen the effectiveness of the ISMS and prevent recurrence.

The continual improvement of the ISMS shall also be supported by monitoring, measurement, analysis, evaluation and audit activities, as well as by the review of incidents, nonconformities and control results, in order to verify the suitability of implemented measures and continually strengthen system effectiveness.

SUARDIAZ Group shall promote periodic reviews and assessments of the ISMS and information security controls by personnel or functions with an appropriate degree of independence from the area or activity being reviewed, in order to verify their suitability, effectiveness and compliance with applicable requirements.

6.8 Roles, responsibilities and authorities

SUARDIAZ Group ensures that roles, responsibilities and authorities relevant to information security are assigned, communicated and maintained consistently with the organisational structure and the needs of the ISMS. This assignment must ensure the system's conformity with applicable requirements, the proper execution

of planned activities and reporting to Top Management on ISMS performance and identified improvement needs.

The organisation promotes awareness among all individuals of the information security responsibilities applicable to them and expects them to act accordingly, fostering coordination between functions, appropriate decision-making and accountability for protecting information within the defined scope.

SUARDIAZ Group shall promote the assignment of information security roles, responsibilities and authorities, where appropriate, in accordance with segregation-of-duties principles and consistently with the organisational structure and responsibility chart defined by the organisation, in order to reduce risks arising from conflicts of interest, unjustified access or the concentration of critical functions in a single person. Role segregation is reflected in the 'Roles and Responsibilities Document', which includes the official SUARDIAZ Group organisational chart.

This policy forms the overarching level of the ISMS regulatory framework. It shall be developed through specific policies, standards, procedures, guidelines and related documented information, which must be consistent with its principles and remain formally approved, current and controlled.

7. POLICY COMMUNICATION

This policy must be communicated within the organisation and made available to relevant interested parties where appropriate. SUARDIAZ Group determines what is to be communicated, to whom, when, by whom and through which channels, to ensure that the policy is understood, applied and available as documented information. Externally, the organisation shall ensure that this policy, or an appropriate version of it where applicable, can be provided to relevant interested parties through formally defined channels, whether publicly, on a controlled basis or upon request, according to the nature of the relationship, applicable requirements and relevant confidentiality criteria.

Communication of this policy must help persons working under the organisation's control understand their obligations and their contribution to the effectiveness of the ISMS. Where relevant, it may also be made available to relevant interested parties as evidence of SUARDIAZ Group's commitment to information protection and compliance with applicable requirements.

The organisation shall also promote appropriate communication, training and awareness activities to ensure that personnel and, where relevant, relevant third

parties included within the scope of the ISMS are familiar with this policy and the obligations arising from it.

8. POLICY REVIEW, UPDATE AND CONTROL

This policy must be reviewed at planned intervals and whenever relevant changes occur in the organisation's context, interested parties, applicable requirements, information security risks or ISMS operations that may affect its suitability, adequacy or effectiveness. Its updating, review, approval, distribution and control shall be carried out in accordance with the ISMS guidelines for managing documented information. Within this framework, ISMS documentation shall be managed according to criteria for identification, versioning, review, approval, access control, distribution, preservation, retention and final disposition, ensuring its integrity, availability, traceability and suitability throughout its life cycle.

The review of this policy must consider, among other aspects, ISMS performance, changes in risks and opportunities, audit results, management review, and changes in the internal and external context or in applicable requirements.

Any exception to the principles or requirements arising from this policy must be justified, assessed according to the associated risk, approved by the appropriate level of authority and, where necessary, accompanied by compensating measures and specific monitoring until it is closed or reviewed.

Without prejudice to planned reviews, this policy must be reviewed whenever significant incidents, major organisational changes, changes to the scope of the ISMS, regulatory or contractual changes, relevant technological changes, or audit and monitoring results warrant an update.

9. RELATED DOCUMENTATION

The documentation related to this policy comprises the current ISMS documented information that develops, supports or provides evidence of its implementation, including, as applicable, documentation on roles and responsibilities, information security objectives, context analysis, interested parties, communication, risk management, the Statement of Applicability and other corporate information security policies or documents that are formally approved, current and controlled.

10. ANNEXES

There are no annexes associated with this document.