GRANSOLAR GROUP

INFORMATION SECURITY POLICY

DOC. CODE: GGR-CO-POL-0005-A3
VERSION: A3
DATE 25/03/2026

SUMMARY:

TITLE	Information Security Policy
SCOPE OF APPLICATION	Gransolar Group (as defined below)
DISCIPLINE	Corporate
CATEGORY	Policy
PREPARED BY	Manager of IT Department (as defined below)
RESPONSIBLE DEPARTMENT	IT Department
APPROVAL DATE	25/03/2026
APPROVAL BODY	Board of Directors (as defined below)
REPLACING VERSION	A2
ACTUAL VERSION	A3
USE	Public

VERSION HISTORY:

VERSION	DATE	PREPARED BY	CHANGES MADE	REVIEWED BY
A1	15/09/2021	Manager of IT Department	Creation	Board of Directors
A2	17/12/2024	Manager of IT Department	Policy harmonization	Governance Department (as defined below)
A3	25/03/2026	Manager of IT Department	Update to align with the latest version of ISO 27001 and the NIS2 Directive	Governance Department

APPROVAL HISTORY:

VERSION	DATE	APPROVED BY
A1	15/09/2021	Board of Directors
A2	17/12/2024	Board of Directors
A3	25/03/2026	Board of Directors

TABLE OF CONTENTS

1. GLOSSARY

For the purposes of this information security policy (hereinafter, the "**Policy**"):

(i) "**Board of Directors**" means the Board of Directors of Grupo Gransolar, S.L.;

(ii) "**Bylaws**" means the bylaws (*estatutos sociales*) of Grupo Gransolar, S.L.;

(iii) "**Commercial Code**" means the Spanish Commercial Code;

(iv) "**Corporate Macro Policy**" means the corporative corporate macro policy of Gransolar Group;

(v) "**Data Protection Law**" means the Organic Law 3/2018 of 5 December on Personal Data Protection and guarantee of digital rights (*Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*);

(vi) "**Data Protection Regulation**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

(vii) **"ESG Committee**" means the advisory body of the Board of Directors responsible for managing and overseeing environmental, social and governance (ESG) matters of Gransolar Group, prior to their final approval by or submission to the Board of Directors;

(viii) "**Governance Department**" means the governance department of Gransolar Group;

(ix) "**Governance Director Plan**" means the governance director plan of Grupo Gransolar, S.L.;

(x) "**Gransolar Group**" means the Group whose parent company is Grupo Gransolar, S.L.;

(xi) "**Group**" means a group of companies within the meaning of Article 42 of the Spanish Commercial Code, i.e., a group of companies which, in accordance with such article, is under the direct or indirect control of a parent company;

(xii) "**Information**" means any data or set of data, regardless of its format, medium or method of transmission, generated, collected, processed, stored or transmitted by Gransolar Group in the course of its activities, including, among others, information (a) relating to Gransolar Group itself, its directors, officers and employees, as well as information relating to suppliers, contractors, subcontractors, business partners, customers or other third parties, or provided by such parties to Gransolar Group, and (b) which qualifies as personal data in accordance with the applicable data protection regulations, in particular the Data Protection Regulation and the Data Protection Law;

(xiii) "**Information Security Incident**" (collectively, the "**Information Security Incidents**") means any event that compromises or may compromise the availability, authenticity, integrity or

confidentiality of the Information or Information Systems of Gransolar Group, or that affects the provision of services supported by such systems;

(xiv) "**Information Systems**" means the set of systems, processes, technologies, applications, devices, networks, media, infrastructures and information and communication technology services and any other resources that enable the creation, collection, processing, storage, transmission or protection of the Information used by Gransolar Group, whether in physical or digital environments;

(xv) "**ISO 27001**" means the international standard ISO/IEC 27001 establishing the requirements for establishing, implementing, maintaining and continually improving an information security management system;

(xvi) "**IT Department**" means the information technology (IT) department of Gransolar Group;

(xvii) "**NIS2 Directive**" means Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148;

(xviii) "**SDGs**" means the Sustainable Development Goals established under the 2030 Agenda for Sustainable Development;

(xix) "**Significant Information Security Incident**" means any Information Security Incident that has, or may have, a significant impact on the provision of Gransolar Group's services or on the security of its Information Systems, taking into account, among other factors, the number of users affected, the duration of the incident, its geographical scope, the severity of the disruption of services or the economic or reputational impact it may cause; and

(xx) "**User**" (collectively, the "**Users**") means any:

(a) employee of the companies forming part of Gransolar Group, understood as any person linked to such companies through an employment, commercial, training or any other similar legal relationship;

(b) officer or senior manager of the companies forming part of Gransolar Group;

(c) director of the companies forming part of Gransolar Group;

(d) contractor, supplier, joint venture partner, customer, consultant or authorized third party, as well as their respective employees;

(e) any external or temporary personnel;

who accesses or uses Information or Information Systems of Gransolar Group.

2. INTRODUCTION

Gransolar Group bases its management model on operational excellence, responding to the needs and expectations of its stakeholders, creating value for society and promoting sustainable development in its social, economic and environmental dimensions.

In this context, the corporate governance system of Gransolar Group is structured through a set of internal rules (the "**Internal Regulatory Framework**"), including corporate policies, which constitute an essential element to (i) ensure compliance with applicable regulations, (ii) establish clear guidelines for the development of activities, and (iii) promote the harmonization and efficiency of internal processes.

The Internal Regulatory Framework is inspired by the highest international standards in the fields of sustainability, business ethics and corporate governance. In particular (and by way of example only), as a participating member of the United Nations Global Compact, Gransolar Group promotes the SDGs and actively assumes its responsibility as an agent of change in matters of sustainability.

Likewise, Gransolar Group maintains a firm commitment to:

(i) the respect for and protection of Human Rights, adopting a preventive and due diligence approach in relation to potential violations in the territories in which it operates (this commitment extends to all stakeholders of Gransolar Group, who are provided with access to a whistleblowing channel); and

(ii) the promotion of the highest standards of transparency, business ethics and accountability, applying a zero-tolerance policy towards any conduct contrary to the provisions of the Internal Regulatory Framework and extending these principles throughout its entire value chain.

In line with the above, Gransolar Group promotes an organizational culture based on regulatory anticipation, fostering the early adoption of new regulations, as well as the incorporation of guidelines, standards and recommendations issued by leading international organizations.

3. PURPOSE AND AIM

The purpose of this Policy is to establish the principles, criteria and guidelines governing the actions of Gransolar Group with regard to the security of its Information and Information Systems (strategic assets for Gransolar Group which must therefore be protected against threats such as errors, sabotage, terrorism, extortion, industrial espionage, privacy breaches, service interruptions and natural disasters), with the aim of:

(i) promoting within Gransolar Group:

(a) a responsible and consistent management of the Information and the Information Systems, in compliance with the regulations on data protection and cybersecurity, in particular the Data Protection Regulation, the Data Protection Law and the NIS2

Directive (the "**Data Protection and Cybersecurity Regulations**"), and aligned with the applicable reference standards in the field of information security and cybersecurity in force from time to time, such as ISO 27001;

(b) a secure environment for the use and management of the Information and the Information Systems at all organizational levels;

(ii) ensuring the security, quality, resilience and continuity of the Information Systems and of the services supported by them; and

(iii) reducing, as far as possible, the likelihood of Information Security Incidents occurring and, where such incidents do occur, minimizing their impact.

4. SCOPE OF APPLICATION

4.1. OBJECTIVE SCOPE OF APPLICATION

This Policy shall apply to all Information and Information Systems of Gransolar Group.

4.2. SUBJECTIVE SCOPE OF APPLICATION

This Policy shall apply to (and, therefore, shall be binding upon) the Users.

4.3. GEOGRAPHICAL SCOPE OF APPLICATION

This Policy shall apply in all countries in which Gransolar Group carries out its activities, without prejudice to any adaptations that may be required in order to comply with the applicable local regulations in each jurisdiction.

5. GENERAL PRINCIPLES

In the course of its activities, Gransolar Group shall act in accordance with the following general principles:

(i) Regulatory compliance: Gransolar Group shall carry out its activities in accordance with (a) the regulations applicable in each jurisdiction in which it operates and (b) the provisions set out in the Internal Regulatory Framework, promoting a culture of compliance and zero tolerance for conduct contrary to the law or to its internal rules.

(ii) Integration into strategy and decision-making: Gransolar Group shall integrate the principles set out in all documents forming part of its Internal Regulatory Framework (including, among others, this Policy) into its corporate strategy, its decision-making processes and the management of its activities and operations.

(iii) Risk-based management: Gransolar Group shall apply a preventive and risk-based approach, promoting the identification, assessment, mitigation and monitoring of the risks associated

with the scope of application of all documents forming part of its Internal Regulatory Framework (including, among others, this Policy).

(iv) Responsibility and accountability: Gransolar Group shall promote responsible, transparent and traceable conduct, establishing appropriate supervision, control and monitoring mechanisms to ensure the proper implementation of all documents forming part of its Internal Regulatory Framework (including, among others, this Policy).

(v) Continuous improvement: Gransolar Group shall promote the review and continuous improvement of its processes, tools and management systems, adapting to regulatory, technological and business environment developments.

(vi) Training and awareness: Gransolar Group shall promote the training, communication and awareness of all documents forming part of its Internal Regulatory Framework (including, among others, this Policy), in order to ensure their proper understanding and compliance by their corresponding subjective scope of application.

(vii) Extension to the value chain: Gransolar Group shall promote the application of the principles set out in all documents forming part of its Internal Regulatory Framework (including, among others, this Policy) in its relationships with business partners, suppliers, contractors and other third parties, where appropriate depending on the nature of the relationship.

(viii) Respect for international standards: Gransolar Group shall guide its actions in accordance with internationally recognized standards, guidelines and best practices in the fields of sustainability, business ethics and corporate governance.

6. INFORMATION SECURITY PRINCIPLES

In addition to the general principles set out in Section 5 above (which shall govern all activities of Gransolar Group in general), with regard to the Information and the Information Systems, Gransolar Group shall act in accordance with the following principles:

(i) Security: Gransolar Group shall develop and maintain an Information security management system based on internationally recognized standards.

(ii) Security culture: Gransolar Group shall promote a culture of Information security at all levels of the organization.

(iii) Availability: Gransolar Group shall ensure that the Information and the Information Systems can be used at the required times and in the required manner.

(iv) Confidentiality: Gransolar Group shall ensure that only duly authorized persons have access to the Information and the Information Systems.

(v) Integrity: Gransolar Group shall adopt the necessary measures to protect Information against unauthorized or improper modifications, ensuring its accuracy and reliability.

(vi) Authenticity: Gransolar Group shall ensure that the source from which the Information originates is the legitimate owner thereof and is who it claims to be.

(vii) Legality: Gransolar Group shall process the Information and the Information Systems in accordance with the Data Protection and Cybersecurity Regulations.

(viii) Information security risk management: Gransolar Group shall adopt a risk management-based approach for the protection of the Information and the Information Systems, through the implementation of appropriate and proportionate technical, operational and organizational measures in order to:

(a) protect and maintain the confidentiality, integrity and availability of the Information and the Information Systems;

(b) continuously detect the risks of Information Security Incidents occurring (collectively, the "**Risks**");

(c) prevent or minimize the impact of Information Security Incidents; and

(d) ensure an adequate level of security of the Information and the Information Systems in relation to the Risks identified;

collectively, the "**Security Measures**", which shall address, among others, the following areas:

(a) Risks analysis and management;

(b) the prevention, detection and management of Information Security Incidents;

(c) business continuity and recovery from incidents affecting Information Systems;

(d) security in the supply chain and in relationships with suppliers and third parties;

(e) security in the acquisition, development, maintenance and operation of the Information Systems;

(f) the periodic assessment of the effectiveness of the Security Measures adopted;

(g) training, awareness and the promotion of good cybersecurity practices;

(h) the appropriate use of Information protection mechanisms, including, where appropriate, encryption and cryptography measures;

(i) identity and access management, as well as the use of enhanced authentication mechanisms and secure communications; and

(j) human resources security.

(ix) Security by design and by default: the principle of Information security shall be integrated from the initial stages of the design, development, acquisition and implementation of the Information Systems.

(x) Responsibility: all Users shall be responsible for protecting Information and complying with the Security Measures.

(xi) Supply chain security: as mentioned above, Gransolar Group shall adopt, among other measures, Security Measures intended to ensure that suppliers, contractors and third parties who have access to the Information or the Information Systems of Gransolar Group, or who participate in the provision of technological or digital services, comply with appropriate Information security and cybersecurity standards (such Security Measures shall be applied taking into account, among other factors, the specific vulnerabilities of suppliers and service providers, the quality and security of the products or services supplied, as well as the cybersecurity practices applied by such suppliers, including, where applicable, their secure development procedures). For this purpose, Gransolar Group shall promote the assessment of the Risks associated with such third parties (provided that they are to supply goods and/or services that may have an impact on the services or the Information Systems of Gransolar Group) and, where necessary, specific Information security requirements shall be established and documented in the relevant contractual agreements with such suppliers or third parties (such requirements shall be mutually agreed), in order to mitigate the Risks identified and ensure compliance with this Policy and the applicable regulations.

(xii) Continuous improvement of Security Measures: Gransolar Group shall continuously review and improve the Security Measures through periodic assessments, audits and reviews.

(xiii) Resilience: Gransolar Group shall adopt measures aimed at ensuring the ability of its Information Systems to withstand, adapt to and recover from incidents or disruptions.

(xiv) Information classification: Gransolar Group shall establish criteria for the classification of Information based on its sensitivity, value and criticality to the organization, ensuring that such Information is handled and protected in accordance with its classification level.

(xv) Secure use of Information and Information Systems: Gransolar Group shall ensure that the Users:

(a) make proper use of the Information and the Information Systems in the performance of their functions, duties and responsibilities, without compromising the security of such Information and Information Systems;

(b) adopt, implement and continuously maintain appropriate technical, organizational and administrative measures to ensure the confidentiality, integrity and availability of the Information provided to them by Gransolar Group;

(c) comply with the Data Protection and Cybersecurity Regulations and the applicable security standards;

(d) notify Gransolar Group of any Information Security Incident; and

(e) return to Gransolar Group (or destroy) the Information received once their contractual relationship with the relevant company of Gransolar Group has ended.

7. COMPLIANCE MONITORING AND RESPONSE TO BREACHES

7.1. COMPLIANCE MONITORING

7.1.1. The manager of the IT Department shall coordinate periodic assessments intended to verify the level of compliance with this Policy by the Users.

7.1.2. In addition, audits, both internal and external, shall be carried out in order to verify compliance with this Policy, at least once a year or whenever substantial changes occur in the Information Systems.

7.1.3. The results of such assessments and audits may lead to the adoption of corrective or improvement measures where necessary.

7.2. EXCEPTIONS

Any exception to the provisions of this Policy shall be reported to the manager of the IT Department, or to the function responsible for the Information security designated by Gransolar Group from time to time, who shall analyze and assess the risk that such exception may entail for Gransolar Group and, based on the categorization of such risk, such risk shall be assumed by the requester of the exception together with the relevant business owners.

7.3. BREACHES

7.3.1. Any User who becomes aware of:

(i) suspicious or anomalous situations related to Information and/or Information Systems;

(ii) Information Security Incidents; or

(iii) breaches of this Policy or of the Security Measures;

shall report the same to the person responsible for Information security designated by Gransolar Group from time to time.

7.4. Any breach of this Policy shall be considered a serious offence and may result in:

(i) the application of the applicable disciplinary regime, without prejudice to any other legal or contractual liabilities that may arise; and

(ii) where appropriate, the termination of the contractual relationship of the breaching party with the relevant company of Gransolar Group.

7.5. Significant Information Security Incidents shall be managed and, where applicable, notified without undue delay to the competent authorities in accordance with the Data Protection and Cybersecurity Regulations, within the timeframes established therein.

7.6. Where appropriate, Gransolar Group may also inform the recipients of its services of those Significant Information Security Incidents that may negatively affect the provision of such services.

8. RELATED INTERNAL REGULATIONS

8.1. ASCENDING HIERARCHY

This Policy forms part of the Internal Regulatory Framework of Gransolar Group and is hierarchically positioned below the following corporate rules, upon which it depends and in furtherance of which it is issued:

(i) the Bylaws;

(ii) the Governance Director Plan; and

(iii) the Corporate Macro Policy.

8.2. DESCENDING HIERARCHY

8.2.1. This Policy is implemented through a user security manual, which establishes the requirements (based on market best practices and aligned with the specific needs of Gransolar Group) that must be complied with by all Users with respect to the Information and Information Systems of Gransolar Group.

8.2.2. Without prejudice to the foregoing, this Policy may also be implemented through any other procedure, protocol or other internal rule specifying its practical application.

8.2.3. In the event of any contradiction between this Policy and internal rules of a lower hierarchical rank, the provisions of this Policy shall prevail, without prejudice to the provisions set forth in applicable legal regulations or in internal rules of a higher hierarchical rank.

8.3. SAME HIERARCHICAL LEVEL

In the event that Gransolar Group has specific corporate policies which, depending on the same Corporate Macro Policy, regulate matters related to the subject matter of this Policy (including those whose adoption is mandatory under the applicable regulations in a specific jurisdiction), such policies shall:

(i) comply with the general principles and guidelines established in the relevant Corporate Macro Policy; and

(ii) be applied in coordination with this Policy.

9. RESPONSIBLE DEPARTMENT

The department responsible for this Policy is the IT Department.

10. COMMITMENT OF THE BOARD OF DIRECTORS

The Board of Directors assumes responsibility for:

(i) approving the Security Measures and overseeing their implementation;

(ii) ensuring the availability of the resources necessary for the implementation, maintenance and continuous improvement of the Security Measures; and

(iii) promoting, at all organizational levels of Gransolar Group, compliance with the security principles established in this Policy.

11. CLIMATE CHANGE

11.1. Gransolar Group takes into consideration the risks and opportunities arising from climate change in the analysis of the context of its Information Systems and in the management of the Risks associated therewith.

11.2. In particular, Gransolar Group shall take into account the potential impacts arising from extreme weather events or other environmental conditions that may affect the availability, integrity or resilience of its Information Systems and the technological infrastructures supporting them..

12. COMMUNICATION AND AWARENESS

12.1. INTERNAL COMMUNICATION

This Policy shall be published on the corporate intranet of Gransolar Group, so that it is (i) disseminated among and (ii) accessible to all its employees.

12.2. EXTERNAL COMMUNICATION

This Policy shall be published on the websites of Gransolar Group, so that its stakeholders may access it.

12.3. AWARENESS

Gransolar Group shall provide training to all its employees, officers and directors on the content of this Policy, thereby ensuring an appropriate level of awareness and competence in matters relating to the security of the Information and the Information Systems.

13. REVIEW AND UPDATE

13.1. This Policy shall be reviewed and – where appropriate – updated every three (3) years by the IT Department, in coordination with the Governance Department.

13.2. Without prejudice to the foregoing, this Policy may be reviewed and, where appropriate, updated in advance when (i) regulatory or organizational changes occur, or when there are changes in the risk profile associated with its scope of application, or (ii) the IT Department and/or the Governance Department deem it appropriate due to any other circumstance.

13.3. In any case, any proposal for amendment shall be reported to the ESG Committee, which shall be responsible for submitting such proposal to the Board of Directors for approval.

14. APPROVAL

This Policy shall be interpreted in accordance with the applicable regulations (including the Data Protection and Cybersecurity Regulations) and the Internal Regulatory Framework..

15. ADDITIONAL PROVISIONS

This Policy shall be interpreted in accordance with the applicable regulations (including the Data Protection and Cybersecurity Regulations) and the Internal Regulatory Framework.

GRANSOLAR GROUP

Avda. de la Transición Española, 32

Parque Empresarial Omega, Building A, 4th Floor

28108, Alcobendas (Madrid), Spain

+34 917 364 248 | *group@gransolar.com*