INFORMATION SECURITY POLICY

INDEX

1. INTRODUCTION

The Board of Directors of Técnicas Reunidas, S.A. ("**Técnicas Reunidas**" or the "**Company**") as a listed company, has the legal power to determine the general policies and strategies of the Company and of the Group of which it is the parent company ("**TR Group**" or "**Group**"), a power that has also been included in the Regulations of the Board of Directors.

Técnicas Reunidas and the companies that are part of the Group are committed to protecting information as one of their most important assets, guaranteeing the security of the Information Systems and Networks on which the different business processes are based, in order to strengthen their Digital Operational Resilience, aligning their practices with the current regulations that are applicable, as well as with its corporate values.

In this sense, the security strategy and objectives pursued by the TR Group are aimed at the development and implementation of the maximum capabilities in the field of Information Security, in order to reduce threats to the Information Systems and Networks used to provide the services, taking into account, in particular, their presence in critical sectors such as the development of sustainable infrastructures and plants for the creation of renewable energies, so that their products and services generate sustainable benefits and are aligned with the highest ethical and legal standards.

In accordance with the aforementioned objectives, the Board of Directors of Técnicas Reunidas has approved this *Information Security Policy* (the "**Policy**") which is part of the Information Security Management System (the "**ISMS**"), applies to the TR Group and is integrated into the Company's Governance System.

2. DEFINITIONS

For the purposes of this Policy, the following definitions shall be taken into account:

- **Committee on Information Security, Privacy and Artificial Intelligence**: Interdisciplinary committee with supervisory and regulatory responsibilities to adopt any resolution, with relevance in terms of Information Security within the TR Group, with the aim of ensuring that the measures for Risk Management related to the security of the Information Systems and Networks are suitable and that their implementation is aligned with the values, policies and regulations applying to the TR Group in the different jurisdictions in which it operates.

- **Information Security**: all the activities that make up a correct Risk Management to ensure the protection of the Information Systems and Networks, Users of such systems and other persons who may be affected by Cyber Threats within the TR Group.

- **Chief Information Security Officer (CISO)**: member of the Committee on Information Security, Privacy and Artificial Intelligence, and responsible for the Security of the Information.

- **Chief Systems, Security and Communications Officer (CIO)**: member of the Committee on Information Security, Privacy and Artificial Intelligence in his capacity as Chief Systems, Security and Communications Officer, and responsible for Systems and Network Security Information.

- **Risk Management**: coordinated activities to manage and control the identified risks within TR Group.

- **Incident Management**: a set of measures and procedures aimed at preventing, detecting, analysing and limiting an Incident, resolving and incorporating performance measures that make it possible to know the quality of the protection system and detect trends before they become major problems.

- **Information Security Incident or *Cyber incident***: unexpected or unwanted event that may compromise the availability, authenticity, traceability, integrity or confidentiality of the data stored, transmitted or processed, or the services offered by Information Systems and Networks, or accessible through them.

- **Professional**: members of administrative bodies, managers, workers, collaborators, trainees and interns, regardless of the legal modality that determines their employment or service relationship, their hierarchical level, their geographical or functional location and the TR Group company for which they provide their services.

- **Responsible(s)**: directors, middle managers or any other person with responsibility for making decisions in matters of Information Security.

- **Digital Operational Resilience**: the ability of the TR Group to build, ensure and review its operational integrity and reliability by ensuring, directly or indirectly through the use of services provided by third-party information and communications technology service providers, the full range of ICT-related capabilities necessary to preserve the security of the Information Systems and Networks used by the TR Group and which underpin the continued provision of services and their quality, even in the event of disruptions.

- **Information Security Management System (ISMS)**: a set of information security policies and procedures that aims to compose an organization and management system, designed to implement, maintain and improve these policies and procedures, based on the *Information Security Policy* of the TR Group. The ISMS aims to ensure the confidentiality, integrity and availability of information assets, while minimizing information security risks by taking into account the risks analyzed within business processes.

- **Information Systems and Networks**: An organized set of people, processes, and tools that are used to collect, process, store, and distribute information. These systems allow data to be easily accessible and usable to make decisions, manage operations, and support organizational activities.

- **Information and Communication Technologies ("ICT")**: An organized set of people, processes, and tools that are used to collect, process, store, and distribute information.

- **User**: any person linked to a TR Group company by a civil or commercial relationship, as well as customers, suppliers, subcontractors, consultants or any other persons or entities authorised to use, guard or access the Information Systems and Networks of the TR Group.

- **Vulnerability**: any weakness, susceptibility, or defect of an asset, system, process, or control that can be exploited.

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

3. PURPOSE AND SCOPE

The purpose of this Policy is to establish the basic principles and general rules that allow Técnicas Reunidas, applying them to the Group's companies, to develop Information Security strategies, technologies, procedures and standards to maintain a high level of Digital Operational Resilience, within the framework of the ISMS, strengthening the appropriate operational and control framework, aligned with the business objectives, for the management of the Information Security of the TR Group in a way that allows the companies of the Group to fulfill their corporate purpose,all in accordance with current regulations, as well as with the Group's corporate values.

Notwithstanding the provisions of the previous paragraph, in those investee companies in which this Policy does not apply, Técnicas Reunidas will promote, as far as possible, through its representatives in its management bodies, the alignment of its own policies with those of Técnicas Reunidas, in any case, within the framework of respect for the decision-making autonomy of the investee companies.

In addition, this Policy will also apply, as appropriate, to consortia, *joint ventures* and other equivalent associations, whether national or foreign, when any of the companies that make up the TR Group have control of their management and always within the legally established limits.

4. GENERAL PRINCIPLES OF ACTION

The TR Group understands Information Security as a fundamental element to protect business assets, considering it as a comprehensive process based on risk management and control in order to achieve its objectives and fulfill its mission. In this regard, Técnicas Reunidas is committed to providing the different areas of the Group with all

the technical, human, material and organisational resources necessary to ensure adequate management of the security of the TR Group's Information Systems and Networks.

In accordance with the above, all Professionals and Users of the TR Group must respect and guide their actions based on the following principles:

I. **Definition, development and maintenance**: in order to achieve the objectives, values, strategy and commitments acquired, the Company will promote the definition, development and maintenance of the technical, legal and Information Security management controls incorporated in the ISMS essential to constantly ensure compliance with the relevant legal, regulatory and contractual requirements in the relevant matter.

II. **Promoting a culture of Information Security**: Técnicas Reunidas is committed to actively promoting a culture of Information Security among all its Professionals and Users, both internally and among its customers and suppliers.

III. **Daily management:** entails the obligation of the TR Group to safeguard the security of the Information Systems and Networks, developing sound security strategies, in line with the demands of the various stakeholders, as well as with the current legislation in force on this subject. To this end, Técnicas Reunidas will validate the specific policies and/or procedures by area that will establish the fundamental Information Security principles and requirements.

IV. **Proactive Protection**: in such a way that the protection of the defined levels of privacy, availability, authenticity, tracking and integrity is actively maintained to protect its information assets and guarantee the Digital Operational Resilience of the TR Group.

V. **Continuous improvement**: understanding Information Security as a fundamental pillar in all sectors and business processes, with the aim of achieving constant progress in all processes related to the ISMS and the management of theInformation Systems and Networks security, in order to strengthen the reliability of the relationship with all stakeholders and/or enhance the positive reputation of the TR Group.

5. BASIC REQUIREMENTS FOR INFORMATION SECURITY

To carry out the daily management of security and Information Security, the following basic requirements will always be followed:

- **Prevention, detection, response and conservation.**

  Processes, policies and/or procedures for the prevention and management of Information Security Incidents will be defined, recorded and implemented, ensuring

that they are known by all the Professionals of the TR Group and other subjects linked to this Policy, in order to identify, examine, contain or react to Incidents, recover from them, record them and notify them in a timely manner.

- **Differentiation of responsibilities.**

  The tasks and obligations related to Information Security will be precisely defined, so that all the Professionals of the TR Group and other subjects linked to this Policy understand and know them.

- **Analysis and management of risks and vulnerabilities.**
  Risk assessments will be carried out and recorded based on continuous monitoring, in accordance with the internal risk analysis methodology approved by Grupo TR, and these will be reviewed on a regular basis, always taking the risk levels of the previous analysis as a reference.
  Likewise, scans will be carried out periodically to detect vulnerabilities in the Information Systems and Networks that can potentially be exploited. Based on the results, a Risk and Vulnerability Management plan will be defined, implemented and supervised.

- **Personnel management.**

  All Professionals and, if necessary, other subjects linked to this Policy will understand and assume their obligations in relation to Information Security. On the other hand, awareness and training programs will be implemented, so that all Professionals, including members of the governing bodies, together with direct suppliers and service providers, and other persons subject to this Policy are aware of the relevance of Information Security and adopt the recommended cyber hygiene practices.

- **Authorisation and access control.**

  Procedures and/or policies for logical and physical access control must be established, documented and applied, managing access rights to Information Systems and Networks, as well as to physical facilities, based on the principle of least privilege.

- **Protection of the facilities.**

  Controls and actions will be implemented to prevent the loss, damage or impairment of the facilities where the Information Systems and Networks and other assets are located, in addition to the interruption of their operations due to the failure or interruption of support services.

- **Integrity and updating.**

  Processes shall be established and implemented to establish requirements for security updates applicable to Information Systems and Networks during their useful life.

- **Protection of Information in Storage and in Transit.**

  Appropriate controls shall be established, implemented and applied with a view to ensuring the appropriate and effective use of cryptography to protect the confidentiality, authenticity and integrity of information, both in storage and in transit, in line with the asset classification and the results of the risk assessment carried out.

- **Network segmentation.**

  Actions will be implemented to segment the Information Systems or Networks into networks or areas (both their own and those provided by third parties).

- **Activity logging and detection of malicious code.**

  Processes will be implemented and instruments will be used to monitor and document the activities within the TR Group's Information Systems and Networks, with the aim of identifying events that can be classified as Incidents and act in the appropriate way to mitigate their effect, ensuring that the findings of these evaluations are considered in the learning and improvement processes.

- **Continuity of activity.**

  A business continuity and disaster recovery plan will be defined - which will be kept up to date - to be activated in situations of Incidents, including, among other aspects, conditions for its activation, essential contacts, roles and responsibilities, and required resources. The aim is to ensure that operations are reincorporated in accordance with this plan, as well as business continuity in the TR Group.

- **Supply Chain Security.**

  Security procedures and/or policies will be implemented and executed in the supply chain that establish the criteria for approval and supervision of relationships with suppliers, as well as the appropriate actions and controls to minimize the risks arising from these third parties for the protection of the TR Group's Information Systems and Networks.

The TR Group will establish specific procedures so that all Professionals and interested parties are aware of, understand and comply with the Policy and all its implementing regulations.

In this sense, all the Information Security documentation that is developed in execution of the aforementioned principles and that will be integrated together with this Policy in the ISMS, is managed, structured and preserved in accordance with the documented procedures that the TR Group has developed taking into account the regulations, as well as the national and international standards that are applicable in each case.

6. GOVERNANCE

Information Security governance in the TR Group is essential to manage and mitigate potential risks, to ensure decision-making based on the real risk of threats materializing on the organization, as well as for the continuity of business operations, this Policy being a fundamental tool for the proper management and governance of Information Security.

6.1. THE BOARD OF DIRECTORS AND ITS COMMITTEES

The Board of Directors of Técnicas Reunidas is responsible for establishing the TR Group's management strategy and guidelines in the field of Information Security, through this Policy and, where appropriate, other corporate rules implementing it.

In turn, it is the responsibility of the Audit and Control Committee to ensure the implementation and development of this Policy and the measures adopted in application thereof, as well as to review, and, where appropriate, propose to the Board of Directors the updating of this Policy.

Likewise, the Audit and Control Committee is responsible for supervising the effectiveness of the control and Risk Management systems in the field of Information Security of the Company and its Group, as well as the report on them.

In the exercise of its supervisory functions, the Audit and Control Committee shall periodically receive from the Committee on Information Security, Privacy and Artificial Intelligence, through the Chief Information Security Officer, with the support of the Chief Systems, Security and Communications Officer, information on the management developed by the Committee on Information Security, Privacy and Artificial Intelligence.

6.2. COMMITTEE ON INFORMATION SECURITY, PRIVACY AND ARTIFICIAL INTELLIGENCE

6.2.1. Principles of action

Técnicas Reunidas, through the Chief Information Security Officer and the Chief Systems, Security and Communications Officer, which will be supported by the Committee on Information Security, Privacy and Artificial Intelligence, will observe and promote within the TR Group the following principles in relation to the Information Security governance:

a) **Principle of strategic alignment and vision of the future**: Information Security will be considered as another part of the business, understood as a tool that helps the TR Group to achieve its objectives, aligned with the Group's mission and perspective. Consequently, the Committee on Information Security, Privacy and Artificial Intelligence will promote a holistic approach in the TR Group so that

Information Security is not considered as an obstacle, but as an additional tool, essential for the development of its business.

b) **Principle of ethics and compliance**: the Information Security governance within the TR Group must not only focus on compliance with the established regulations, but also on good security practices and the ethical use of the Group's resources.

c) **Principle of responsibility and accountability**: Information Security is an interdisciplinary and complex field that impacts all the operations of an entity. Therefore, it needs appropriate leadership and a structure that, to be established and managed correctly, must be made up of professionals with the appropriate training and experience.

   The Committee on Information Security, Privacy and Artificial Intelligence will be responsible for establishing, promoting and regulating Information Security, in addition to participating in decision-making and strategies in this field. In addition, the Committee on Information Security, Privacy and Artificial Intelligence will assume the responsibility of providing an appropriate periodic report at appropriate levels on the risks associated with Information Security, along with the mitigation and control mechanisms that are required.

6.2.2. Composition and functions of the Committee on Information Security, Privacy and Artificial Intelligence

The Committee on Information Security, Privacy and Artificial Intelligence will act as a support body for the Chief Information Security Officer and the Chief Systems, Security and Communications Officer for the performance of their functions.

The Committee on Information Security, Privacy and Artificial Intelligence, in addition to any other functions attributed to it, will be responsible for:

- Review this Policy, ensuring that it complies with the applicable regulations and the ethical principles of Técnicas Reunidas, as well as with the best practices in the sector. In this regard, when it deems it appropriate, it may submit proposals for amendments to this Policy to the Board of Directors for approval.

- Review and promote the continuous improvement of the ISMS of Técnicas Reunidas, including, where appropriate, the identification and evaluation of new risks associated with the ISMS.

- Coordinate the continuity plans of the different areas of Técnicas Reunidas to ensure a seamless action in the event that they must be activated.

- Resolve conflicts of responsibility that may arise between the different Controllers and/or between different areas of Técnicas Reunidas, raising those cases in which it does not have sufficient authority to decide.

- Regularly inform senior management and different areas of Técnicas Reunidas in relation to security and control measures adopted, recommending possible actions in this regard.

- Coordinate and monitor the performance of Cyber Incident management processes.

- Promote periodic audit processes to verify compliance with applicable regulations.

- Promote training and the development of skills related to Information Security, as well as basic cyber hygiene practices, in Técnicas Reunidas.

- Ensure compliance with the applicable regulations.

- Approve internal procedures, standards or protocols aimed at the development and implementation of this Policy in Técnicas Reunidas.

- Monitor the performance of these functions by the corresponding bodies or instances of the TR Group companies in order to supervise the implementation of the principles and commitments that inspire this Policy, being able to collect from them any information it deems necessary for the fulfilment of this coordination function at Group level.

7. MONITORING, INTERPRETATION AND REVIEW

7.1. MONITORING

Compliance with this Policy will be overseen by the Committee on Information Security, Privacy and Artificial Intelligence. Mechanisms for auditing and periodic review of the measures established in execution of this Policy will be established.

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 development of their work, to the extent that understanding and adherence to the definitions and principles established in the Policy is essential to maintain a solid ISMS.

The monitoring and measurement of the effectiveness of the measures that develop the general principles and rules of this Policy will be carried out in accordance with the internal policies and/or procedures of objectives and review indicators that Técnicas Reunidas approves internally.

It will be the responsibility of the Information Security Department to establish the Information Security indicators that must be monitored during the year, and which must be analyzed at least in the review of the system by the Directorate of the

Information Systems, Communications and Security Department, leaving a record in the minutes of the relevant meeting.

Based on the results of these measurements, as well as the results of Information Security audits, managed Cyber Incidents, vulnerabilities detected and feedback from interested parties, the Information Security measures established for the development of this Policy will be regularly reviewed and integrated into the framework of the regular review of the ISMS.

7.2. INTERPRETATION

The contact body for any questions and/or queries in relation to the interpretation and execution of this Policy will be the Committee on Information Security, Privacy and Artificial Intelligence, which may be contacted through the channels enabled for this purpose.

7.3. REVIEW AND UPDATE

This Policy will be reviewed and updated at least once a year, within the annual review of the ISMS carried out by the Company, and whenever significant Incidents or significant changes in operations or risks occur, to ensure its effectiveness and adaptation to technological progress and regulatory, organizational, technical and process changes within the TR Group, as well as to incorporate the best practices identified in the field of Information Security.

The modification and/or update of this Policy will be approved by the Board of Directors of Técnicas Reunidas, following a report from the Audit and Control Committee, and will be disseminated to Professionals and Users through the usual channels.

8. DISSEMINATION OF THE POLICY

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

Notwithstanding the above, Técnicas Reunidas will carry out communication, training and awareness-raising actions for the understanding and implementation of this Policy, as well as its updates.

In any case, it is recommended to periodically access the content of this Policy through the available channels for a better understanding of it, and it should be borne in mind that ignorance of all or part of its content does not exempt from compliance.

9. ENTRY INTO FORCE

This Policy was approved by the Board of Directors of Técnicas Reunidas at its meeting on April 10, 2025, and will enter into force from the time of its publication on the Company's corporate website on April 15, 2025.