INFORMATION SECURITY POLICY

1. Introduction

The Management of **Torrecid** acknowledges that **information** is a fundamental strategic asset for the development of its activity, its competitive advantage, and the trust placed by its **customers, suppliers, collaborators, and other stakeholders**. Therefore, it is committed to continuously implementing, maintaining, and improving an **Information Security Management System (ISMS)** in accordance with international best practices (ISO 27001, National Security Framework - ENS, GDPR, LOPDGDD, and applicable industrial sector regulations) and in particular with **Directive (EU) 2022/2555** of the European Parliament and of the Council, known as NIS2.

This Information Security Management Policy establishes a framework that allows information to be managed securely, realistically, and effectively, and in accordance with the organization's purpose. To this end, the involvement of all personnel in the application of the determined measures is sought.

Torrecid expressly states its commitment to enhancing the Security and Cybersecurity of the Information of the service provided, and is committed to meeting the needs and expectations of stakeholders, according to the legal and regulatory framework in which the activities are carried out. Furthermore, it is fully aware of the relevance of the security of the information it manages, as well as the need to guarantee the **confidentiality, integrity, availability, authenticity, and traceability** of its information systems. These principles constitute an essential and inseparable element of daily work and a fundamental part of the quality, efficiency, and reliability of the service the company offers its customers, within the highest standards of technological and productive excellence.

In this regard:

- The **management of information security** must be developed in accordance with the requirements established by the **Information Security Management System (ISMS)** and, where applicable, by the **National Security Framework (ENS)**, and in particular with **Directive (EU) 2022/2555 (NIS2)** of the European Parliament and of the Council, complying at all times with current legal regulations and recognized national and international best practices.
- **Information** is a **strategic asset** for **Torrecid** and, therefore, its adequate protection must be guaranteed both in the performance of daily activities and in relationships with **customers, suppliers, collaborators, and other stakeholders**, ensuring the secure processing of all technical, commercial, and confidential data handled.
- **Information security and cybersecurity** are responsibilities that concern all Torrecid personnel, both individually and through cooperation among the different departments, areas, and business units. The company promotes an organizational culture based on the **awareness, responsibility, and commitment** of all employees regarding information security.
- The **internal security regulations** and the procedures derived from the ISMS and the ENS will be **disseminated, understood, and adopted** by all Torrecid personnel, being **mandatory** at all hierarchical and functional levels.
- **Risks and opportunities** related to information security must be **identified, assessed, and managed**, in order to ensure that the system achieves the planned results, prevents or mitigates undesirable effects, and promotes **continuous improvement**.

Protection measures proportional to the **value of information assets**, the **existing risk level**, and the **potential impact** of threats will be adopted, including those derived from the processing of **personal data**, in accordance with the **LOPDGDD**, the **GDPR**, and the **internal regulations of Torrecid**.

- Torrecid is committed to **preserving the confidentiality, integrity, availability, authenticity, and traceability** of information throughout its life cycle, regardless of the medium it is in or the place where it is processed, guaranteeing its protection in both physical and digital format.
- The company maintains a firm **commitment to continuous improvement** of the process and the information security management system.

2. Scope of Application. Reach

This policy applies to all **areas, employees, systems, processes, and locations** of Torrecid. Likewise, it extends to relationships with collaborators, contractors, and other stakeholders with whom the company maintains labor or professional ties, always within the framework of current legislation and the Company's corporate values.

3. General Objectives

Torrecid establishes a **risk and opportunity analysis and management strategy** aimed at an exhaustive understanding of the threats that may affect information security and the definition of the necessary **safeguards** for its correct protection. This strategy is integrated into management processes and decision-making, contributing to the continuous improvement of security, operational efficiency, and the trust of our **customers, suppliers, collaborators, and other stakeholders**.

Within the framework of this strategy, the Management of **Torrecid** defines the following commitments or general **objectives**:

- **Establish the basic protection needs** of information and develop the **security plans** that allow the application of appropriate safeguards to mitigate identified risks and leverage improvement opportunities detected in the technological and organizational environment.
- **Organize information security** based on clear criteria of classification, ownership, and responsibility, assigning the obligation of protection to each information owner. Security procedures and tasks, protocols for action in the event of security incidents or violations, as well as disciplinary measures applicable in case of non-compliance with internal regulations, will be defined and kept up-to-date. Likewise, periodic conformity checks on security matters will be carried out and configuration management and change control mechanisms will be applied, ensuring the coherence, traceability, and continuous updating of the system.
- **Promote continuous improvement** of the services and technical support provided, integrating information **security and cybersecurity** as an **inherent and transversal element** in all organizational processes. Security is not conceived as an additional requirement, but as an **essential pillar of the service**, aimed at guaranteeing the quality, efficiency, and reliability of operations.
- **Strengthen Torrecid's positioning** as a reference company in the ceramic sector, recognized for its commitment to innovation, information protection, and excellence in its services, within a secure management framework and conforming to the highest national and international standards.
- **Provide secure and efficient solutions** that allow our **customers** to transform data and information into useful knowledge, facilitating strategic decision-making and the optimization of their production processes.
- **Ensure the availability of a highly qualified and specialized human team**, capable of offering immediate, effective, and coordinated technical attention, guaranteeing service continuity and information protection in all circumstances.
- **Maintain service provision based on the continuous improvement** of management systems, integrating **information security and cybersecurity** as fundamental and default components in all phases of the operating cycle. Risk and opportunity management will also be reviewed periodically, promoting constant adaptation to technological, regulatory, and business environment changes.

4. Principles Governing this Policy

Torrecid adopts the following as fundamental principles of information security:

1. **Confidentiality**: ensuring that information is only accessible by authorized personnel and third parties.
2. **Integrity**: ensuring that information and systems are kept complete, accurate, and without unauthorized alterations.
3. **Availability**: guaranteeing access to information and systems by authorized users when necessary.
4. **Authenticity and Traceability**: verifying the identity and responsibility of those who access or modify the information.
5. **Regulatory Compliance**: complying with all applicable laws, regulations, and contractual obligations.
6. **Protection of Third Parties**: protecting the information of customers, suppliers, collaborators, and stakeholders with the same rigor.

5. Minimum Requirements

Torrecid structures and implements its **information security process** through a coordinated set of organizational, technical, and human measures aimed at guaranteeing the effective protection of information assets and business continuity. To achieve the foregoing and the strategy, the following minimum requirements are established:

- Physical and logical access control to facilities and systems.
- Backup copies and business continuity and disaster recovery plans.
- Classification and secure handling of information.
- Encryption and protection of sensitive information.
- Secure disposal of documents and media.
- Protection of networks and systems against cyber threats.
- Evaluation and periodic control of critical suppliers.
- Strict compliance with GDPR, LOPDGDD, and other applicable regulations.

6. Protection of Third-Party Information

Torrecid recognizes its responsibility in protecting the information entrusted to it by its customers, suppliers, collaborators, and other stakeholders, adopting the following measures:

- Formalization of confidentiality agreements (NDAs) before exchanging sensitive information.
- Limitation of access to third-party data to strictly necessary personnel.
- Application of encryption protocols, access control, secure storage, and controlled disposal.
- Monitoring and evaluation of security measures implemented by suppliers.
- Diligent notification of incidents affecting third-party information, in accordance with current regulations.

7. Training, Awareness, and Security Culture

Torrecid will promote **continuous training and awareness** of personnel on the importance of security and information protection. Specific programs on data protection, digital best practices, incident response, and confidentiality will be provided, both for employees and for third parties with access to company information.

8. Review, Audit, and Continuous Improvement

This policy will be reviewed **at least once a year** or when significant changes occur in the technological, regulatory, or organizational environment. Audits and management reviews will allow verifying the effectiveness of the ISMS and establishing improvement actions.

Risk and opportunity management will also be updated **annually**, ensuring the adaptation of the system to new security challenges and business evolution.

9. ISMS Management Structure / Responsibilities

The following information security management structures are established:

- **Information Security Committee (ISC):** with the objective of coordinating and supervising all activities related to information security. Within the Committee, the following roles are established, with a delegate in each case:
    - **Service Manager**: Establishes the security requirements applicable to services.
    - **Information Manager:** Establishes the security requirements applicable to information.
    - **Information Security Manager:** Directs and coordinates the Information Security Committee meetings and Supervises the application of the security strategy.
    - **Systems Manager:** Ensures the correct application of security measures.
- **Crisis Committee:** with the objective of coordinating and supervising all activities related to crisis management and business continuity. It is composed of the same members as the Information Security Committee.

Within the Information Security Management System, the following internal documents and procedures are included and defined:

01 Security Policy
02 Risk Management
03 Incident Management
04 Business Continuity
05 Supply Chain
06 Security in Acquisition, Development, and Maintenance
07 Monitoring
08 Training and Competence
09 HR Security
10 Access Control
11 Asset Management
12 Cryptography

10. Approval, Communication, and Entry into Force

This Information Security Management Policy, the composition and creation of the Security and Crisis Committees, as well as all internal procedures associated with the Information Security Management System of TORRECID, S.A., have been approved by the General Management of Torrecid, S.A. on December 03, 2025, and are mandatory for all personnel and third parties related to the organization. It will be internally communicated and disseminated, as well as made available to customers, suppliers, collaborators, and interested parties who request it.