TRINATRACKER, the brand under which **NCLAVE RENEWABLE SLU**, **NCLAVE MANUFACTURING SLU**, and **the Tracker organizational unit of Trina Solar Spain S.L.U.** operate (hereinafter referred to as **TRINATRACKER**), recognizes the importance of protecting its information assets. The organization, specialized in the **design**, **manufacturing**, **engineering** and **project management**, **installation**, **maintenance**, and **commercialization** of fixed structures, solar trackers and smart energy solutions, is committed to preventing the destruction, disclosure, modification, and unauthorized use of information related to **customers**, **employees**, **collaborators**, **processes**, **technologies**, and other critical resources. Therefore, the Senior Management is committed to developing, implementing, maintaining, and continuously improving the **Information Security Management System (ISMS)** in compliance with the **UNE-EN-ISO 27001** standard, as well as integrating it into the company's strategic plans, declaring and assuming the following **fundamental principles** of information security:

- **Confidentiality**: Ensuring that access to information is granted only to authorized individuals.
- **Integrity**: Guaranteeing that information and its processes are accurate and complete.
- **Availability**: Ensuring that authorized users have access to information and associated assets whenever required.

To achieve these principles, TRINATRACKER commits to:

- ✓ **Defining information security objectives:** Establishing annual objectives aligned with security principles, ensuring their periodic review and continuous improvement.
- ✓ **Conducting risk analysis:** Identifying risks that could compromise the security of information assets and developing action plans to address them according to the criteria established in the Management System Manual.
- ✓ **Complying with legal and contractual requirements:** Ensuring compliance with applicable regulations and contractual obligations with customers and third parties.
- ✓ **Promoting a security culture:** Providing training and awareness programs on information security for all personnel.
- ✓ **Ensuring business continuity and rapid recovery of critical services and operations:** Establishing necessary measures to minimize the impact of security incidents and ensure the operability of critical processes.
- ✓ **Sanctioning violations:** Applying disciplinary measures in response to violations of this policy or procedures related to the ISMS.
- ✓ **Shared responsibilities:** Engaging all employees, suppliers, and partners in protecting information by assigning specific roles and encouraging the reporting of suspected or confirmed incidents.
- ✓ **Comprehensive protection:** Safeguarding business processes, technological infrastructure, and assets against internal and external threats.

Senior Management is committed to providing the necessary resources to ensure compliance with this policy, fostering continuous improvement of the ISMS, and aligning it with business needs and stakeholder expectations.

Scope of Action:

- **Managing** and **protecting** technological assets and critical processes.
- **Implementing effective access controls**.
- Ensuring **security by design** and throughout the entire lifecycle of information systems.
- **Continuously improving** through security event management.

This policy has the full support of TRINATRACKER's Governing Bodies, which are committed to ensuring its strict compliance across all areas of the company and providing all necessary resources to fulfil this Information Security Policy.

Signed by Qi ZhongHua – Legal Representative