CPSL GROUP INFORMATION SECURITY POLICY

Celer Pawlowsky S.L. and the companies that make up the group (CPSL) are leaders in the multilingual services sector, providing services such as translations, interpreting, multimedia localization, and other services arising from the need of companies to make their materials and content available in multiple languages. CPSL has four production sites located in Spain (Madrid and Barcelona), Germany (Stuttgart), and the United States (Boston).

CPSL has implemented an Information Security Management System that seeks to achieve customer satisfaction through established processes based on continuous improvement, ensuring the continuity of information systems, minimizing risks, and meeting established objectives in order to ensure **the confidentiality, integrity, and availability** of information at all times.

To this end, we are committed to information security in accordance with the **ISO 27001** and **TISAX** reference standards. Accordingly, Management has established the following principles:

- Management competence and leadership as a commitment to developing the Information Security Management System.
- Establish objectives and targets focused on evaluating security performance and continuously improving the activities governed by the Information Security Management System.
- Comply with the legislative requirements that are applicable to our activities and ensure the integrity and availability of information systems and information assets, both in the services provided to our customers and in internal management, thereby preventing unauthorized alterations to information.
- Ensure the ability to respond to emergency situations by restoring the operation of critical services as quickly as possible.
- Establish appropriate measures to address any risks arising from the identification and assessment of assets.
- Ensure the continuous analysis of relevant processes, consequently implementing improvements based on the results obtained and the established objectives.

To achieve these general objectives, company Management is firmly committed to

optimizing its Information Security Policy based on the following factors:

- Risk prevention: Establish the necessary guidelines and resources for risk prevention, with the primary objective of eliminating or mitigating risks.
- Commitment to environmental protection: Reduce and prevent the environmental impacts resulting from our activities, products, or services.
- Legal requirements: Consider legal requirements and any others specified by our customers as the minimum requirements that must be met.
- Dissemination: Disseminate and promote improvements in information security. The effective dissemination of these policies is essential to ensuring both compliance with them and the protection of information assets.
- Stakeholders: Joint participation with the various internal operational areas, customers, suppliers, and external collaborators to improve information security.
- Training: Ongoing training of our personnel in technical knowledge and skills, while encouraging their participation in and commitment to this Information Security Policy.
- Monitoring: Establish indicators at all levels that allow us to make evidence-based decisions.
- Continuous improvement: Establish and periodically review objectives and targets that provide a framework for the continuous improvement of processes and sustainable development.
- Analysis: Analyze and evaluate any deviations that might occur in relation to information security, consequently establishing the necessary corrective actions and implementing opportunities for improvement.
- Integrated system: Active participation by all groups within the organization, at all levels, with an awareness of their contribution to the system's objectives and the consequences of noncompliance.
- Periodic reviews of the Policy: To ensure that our Information Security Policy remains up to date and effective, annual reviews will be conducted. These reviews will take into account changes in regulations, evolving security threats, and changes in the organization's strategy. When necessary, the policy will be updated to reflect new circumstances and to ensure its continued alignment with industry best practices.

These principles are assumed by Management, which provides the necessary means and sufficient resources to its personnel to ensure compliance with those principles, which are embodied and made publicly available through this **Information Security Policy.**

Signed,

Tenesoya Pawlowsky Santana

Managing Director