INFORMATION SECURITY POLICY

1. CONTROL DE DOCUMENTO

1.1. Aprobación

Aprueba	Fecha
Dirección	24 de octubre 2022

1.2. Revisión

Última revisión publicada	24 de octubre 2022

Revisión	Fecha	Autor	Descripción
1	24 de octubre 2022	Responsable SGSI	Confección de la política

2. INFORMATION SECURITY POLICY

The Security Policy of Entornos de Formación SLU reflects the principles and objectives in terms of information security, which allow our company to offer software development solutions and implement customised systems.

Through the preparation, communication and maintenance of this policy, the Management of Entornos de Formación SLU shows its commitment to protecting the confidentiality of the information with which it operates in the provision of its services, to guarantee its integrity in all the treatment processes it carries out, as well as the availability of the information systems involved in these treatments.

To this end, the Management has defined and implemented an Information Security Management System that enables the company to guarantee that the information systems and the information created, collected, stored and processed comply with:

- Security in Human Resources Management before, during and upon termination of employment.
- Appropriate asset management involves classifying the information and handling media, and establishing robust logical access control to its systems and applications, managing user permissions and privileges.
- Protecting facilities and the physical environment by designing secure work areas and securing equipment.
- Ensuring the security of operations by protecting against malicious software, backing up, logging and monitoring and controlling operating software.
- Management of technical vulnerabilities and the choice of appropriate techniques for auditing systems.
- Communications security, protecting networks and information exchange.
- Ensuring security in acquiring and maintaining information systems, limiting and managing change.
- The realisation of secure software development, separating development and production environments, and performing appropriate functional acceptance testing.
- Controlling relationships with suppliers, contractually requiring compliance with relevant security measures and acceptable service levels.
- Effectiveness in managing security incidents, establishing the appropriate channels for notification, response and timely learning.
- The implementation of a business continuity plan that protects the availability of services during a crisis or disaster.
- Identification of and compliance with applicable regulations, with special emphasis on intellectual property and personal data protection.
- Periodic review and continuous improvement of our information security management system to ensure compliance with and effectiveness of these requirements.

All the organisation's personnel have the duty to comply with this policy, for which the Management has the necessary means and sufficient resources for its fulfilment and assumes the responsibility of communicating and keeping it accessible to all interested parties.

In order to improve compliance with Information Security, the company has established different policies with the aim of establishing principles and guidelines on specific and relevant aspects of Information Security.

Signed on 24 October 2022 by the company's management.