INFORMATION SECURITY POLICY

Computer Aided Elearning, S.A. (CAE) are specialists in the development and commercialization of E-learning platforms for managing training activities via any modality or device, such as Virtual classrooms (videoconferencing with integrated whiteboards) which facilitate distance classes and student management. Our online educational platforms, which are the most versatile and comprehensive on the education market, are complemented by the vast catalog of training courses available. CAE's main objective is to ensure that all security measures are enforced throughout all stages; from the initial development to deployment, including the maintenance and updates of the E-learning application, both in the development environment and servers, as well as the information and data stored.

This means that both **CAE's** Management and its staff must apply the established security measures and set up control and monitoring mechanisms. For this purpose, a set of measures, controls, procedures, and actions have been implemented to protect all assets, including information and the processes that support it, as well as systems and networks. It is crucial that the principles of the Security Policy become part of the organizational culture.

To guarantee information security, the Management has developed and implemented an information security management system, whose main pillars and objectives are:

- To comply with all applicable legal provisions and regulations, ensuring legal compliance in the company's activities and meeting the requirements of our clients and stakeholders.
- To establish a continuous improvement system to optimize and enhance safety in the development of our service.
- The Information Security Management System is not the responsibility of one person alone but is the result of joint efforts by all company members, who are provided with constant and appropriate training.
- To protect the company's information resources and the technology used for its processing against internal or external, deliberate or accidental threats.
- To provide the necessary resources for the development, implementation, and continuous improvement of the information security management system across the organization's processes.
- To establish methods for reporting, managing, and recording incidents related to the Information Security Management Systems (ISMS), and to continuously review these controls to ensure compliance with security requirements, thus contributing to continuous improvement.
- To define a strict policy for backing up and storing information relevant to the company.
- To ensure proper access management to our systems through the implementation of an identification and authentication system. This not only restricts access of unauthorized persons but also facilitates a completely secure working environment for our employees.
- To define operational standards that ensure an appropriate balance between user needs, security requirements, and adherence to current laws.

All **CAE** personnel must comply with the guidelines, standards, and procedures, and as a result, assume the duty to collaborate with this organization to prevent any alterations or violations of these rules.

Everyone providing services at **CAE** must understand and fulfill their obligations regarding the proper use of IT resources. Failure to comply with these obligations by personnel may lead to disciplinary liability and the initiation of legal procedures by the company to enforce them.

Consequently, Management extends this commitment to all employees, as well as those acting on behalf of **CAE**, to comply with the guidelines of this policy, which will be reviewed periodically to ensure they remain suitable for the organization's activities.

GANDIA, May 21, 2024

SIGNED: GENERAL MANAGER