EPICODE
Institute of Technology

POL Information security policy

V1 03 sept. 2025

Information Security Objectives

Epic Education is committed to protecting its information assets to maintain trust with students, partners, and personnel. The information security objectives shall be established, monitored, and reviewed to ensure they are consistent with the company's strategic direction. **CEO** and **ISMS Manager** are responsible for ensuring these objectives are met.

The primary objectives for the Information Security Management System (ISMS) are:

- **Confidentiality**: To ensure that information is accessible only to authorized individuals and to protect personal data of students, employee data, and proprietary information, such as course content and business strategies, from unauthorized disclosure.
- **Integrity**: To safeguard the accuracy and completeness of information and processing methods, ensuring that student records, course materials, and financial data are reliable and protected from unauthorized modification.
- **Availability**: To ensure that authorized users have access to information and associated assets when required, maintaining the operational continuity of our online learning platforms and career services.
- **Compliance**: To comply with all applicable legal, statutory, regulatory, and contractual requirements related to information security.
- **Continuous Improvement**: To continually enhance the ISMS by managing risks, responding to incidents, and adapting to new threats to improve the overall security posture.

These objectives shall be measured and reviewed at least annually as part of the management review process, detailed in the "PRO Management Review Process".

Fundamental Information Security Principles

Policy Governance

This policy and its related topic-specific policies constitute the documented framework for information security at Epic Education.

- The **CEO** shall approve this policy and ensure it aligns with the organization's strategic goals.

- The **ISMS Manager** shall be responsible for the publication, communication, and maintenance of all information security policies.
- All policies shall be communicated to relevant personnel and interested parties.
- A review of all information security policies shall be conducted at planned intervals (at least annually) or upon the occurrence of significant changes, in line with the "PRO Management Review Process" and "PRO Change management procedure".
- The management of all policy documents shall adhere to the "PRO Documented information management procedure".

Roles and Responsibilities

Information security is the shared responsibility of every member of Epic Education.

- The **CEO** holds ultimate responsibility for the effectiveness of the Information Security Management System.
- The **ISMS Manager** is assigned the responsibility for implementing, managing, and maintaining the ISMS in accordance with this policy.
- Specific information security duties for all roles within the organization are defined and assigned in the "POL Information security roles and responsibilities policy".

Risk-Based Approach

Information security controls and measures shall be selected and implemented based on the results of a formal and continuous risk management process. This process is defined and managed according to the "PRO Risk management procedure".

Acceptable Use of Information and Resources

All personnel shall use information and associated resources, including systems, networks, and devices, for their assigned and authorized business purposes only. The installation of unauthorized software or use of unauthorized services on company systems is strictly prohibited. Detailed rules governing the use of company assets are documented in the "POL Operational security policy" and the "Code of conduct".

Reporting Information Security Events

All personnel shall promptly report any observed or suspected information security events, weaknesses, or threats. Reporting shall be conducted through the official channels established in the "PRO Information security incident management procedure".

Protection of Information and Assets

- **Clear Desk and Clear Screen**: All personnel shall ensure that sensitive or confidential information in physical form, such as documents and removable storage media, is secured when not in use or when the workspace is unattended. Information processing

facilities shall be protected by screen-locking mechanisms that activate automatically after a short period of inactivity. Specific rules are defined in the "POL Operational security policy".

- **Security of Off-Site Assets**: All company assets used outside the premises, including for remote work, must be protected with the same level of security as within the office. Personnel working remotely shall adhere to established security standards, which include using company-provided security software (antivirus, firewalls), ensuring secure network configurations, and using only authorized remote access technologies configured with multi-factor authentication. Modifying or disabling security controls on company equipment is forbidden. These requirements are further detailed in the "POL Operational security policy".