DT-29-2023-PR

SAGRADO
Universidad del Sagrado Corazón

Cybersecurity Policy

Effective: 2023.06.01

I. Purpose

The purpose of this policy is to establish Universidad del Sagrado Corazón's (University) standards for the protection of electronically stored information and information systems. Confidentiality, integrity, and availability of electronically stored information and information systems are critical to the operation of the University. The University considers all electronically stored information confidential. All members of the University have the responsibility to ensure that the appropriate procedures and controls are implemented, and that information security remains a constant priority.

II. Regulatory Context

This policy is established in compliance with Federal and State Laws, regulations and other institutional policies related to cybersecurity. Also, this policy follows mandatory regulations including, but not limited to, PCI-DSS, ISO 27001, NIST Cybersecurity framework, General Data Protection Regulation, and GLBA, among others.

III. Scope

All users with access to the University's electronically stored information and information systems are responsible to comply with this policy and the procedures related to it.

IV. Definitions

1. Authorized User – any user with the required permissions to access an information system.

2. Electronically Stored Information - any documents or information that are stored in electronic form. Common examples of ESI include word processing documents, spreadsheets, digital photographs, videos, emails and their attachments, text and instant messages, communications conducted in ephemeral messaging applications or in workplace collaboration tools Information stored in databases.

3. Information System – Any system that belongs to the University and that can be accessed through a computer or similar devices.

4. Member of the University Community - includes any person or legal entity who has an interest in the University's mission, institutional activities and/or operations (e.g., trustees, faculty, administrative staff, student support services staff, students, stakeholders, third-party, suppliers and vendors).

V. General Policy

All electronically stored information and information systems are considered a University's corporate asset. It is the policy of the University to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, obstruction, transmission, and theft of information assets.

The Integrated Information Technology Office (ITI for its Spanish acronym) is the unit in charge of the development of procedures to enforce this policy. As such, it will be responsible for the development of the following procedures.

- Access Control
- Network Security
- Data Security
- Physical Security
- Disaster Recovery and Business Continuity
- Password Management
- Data Classification
- Acceptable Use
- Incident Response

VI. Interpretation of this Policy

This Policy is approved by the President of the University with the advice and counsel of the office of the General Counsel. Questions about the scope and interpretation of this Policy should be directed to the Integrated Information Technology Office at 787.728.1515, ext. 8044.

If there is any ambiguity in any provision of this Policy, the University reserves the discretion to interpret it in accordance with the purpose for which it was established, the impact to the University's operations and good faith, unless otherwise provided by law.

VII. Reporting Violations

Violations to this Policy should be directed to the office of Compliance, Internal Audit and Institutional Integrity at cumplimiento@sagrado.edu. Any violations to this Policy will be addressed in accordance with the University's policies and procedures.

Gilberto J. Marxuach Torros
President