DT-29-2023-RE

SAGRADO
Universidad del Sagrado Corazón

Cybersecurity Procedures

Effective: 2023.06.01

I. Purpose

This Procedure describes the cybersecurity processes for protecting the confidentiality, integrity, and availability of information, records, and transactions is critical to the mission of Universidad del Sagrado Corazón ("University" or "Sagrado") according to the Cybersecurity Policy.

II. Roles and Responsibilities

1. Board of Trustees
   - Approves Capital and Operational Budget for Information Technology.
   - Via the audit committee oversees risk management practices and security risks identified by the CIO.

2. Executive Leadership
   - Approves Expenditures for Information Security
   - Communication Path to Staff and Faculty

3. Chief Information Officer (CIO)
   - Communicates information security risks to executive leadership.
   - Reports information security risks annually to university leadership and gains approval to bring risks to acceptable levels.
   - Coordinates the development and maintenance of information security policies, procedures, and standards.
   - Establishes an information security framework and awareness program.
   - Aligns Information Security Procedure and Posture based on the University's mission and risks.

III. 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).

5. Personal Identifiable Information (PII) – information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contact of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

IV. Proceedings

Each critical process deployed at Sagrado undergoes a comprehensive risk assessment validated by the CIO to identify critical information assets, threats to those assets, and effectiveness of risk controls. The risk assessments review risks to the entire process and are not limited to specific IT systems. A comprehensive, organization-wide risk assessment is conducted on a periodic basis. For each system, service, or activity offered by or through the University, the institution conducts a risk assessment following the industry's best practices. As threats, operating environments (physical and virtual) and systems architecture change, the Integrated Technology Office (ITI for its Spanish acronym) updates the risk assessment to ensure new risks are mitigated before making changes to infrastructure, policies, or procedures.

A. Access Controls

All computers and telecommunications systems limit access to users who have a proven "need-to-know." Access to classified or Personal Identifiable Information (PII) is granted on a minimum level of access necessary to perform assigned responsibilities and is monitored for compliance. Access controls implements the following safeguards:

1. *Logical access restrictions:* The ITI Office provides an infrastructure to validate unique user identification through central authentication systems and implements user log-in monitoring to verify that only users granted access to data are allowed access.

2. Access restrictions on physical locations containing Classified or Personal Identifiable Information: Access to data centers and record storage areas containing confidential information, applications and systems are limited to authorized personnel.
3. Network Segmentation: The ITI Office reviews risk assessment data and segment systems and data storage on the network.
4. Access Reviews: The ITI Office reviews the users granted access to the data center and record storage areas containing information and key applications and systems on a quarterly basis to ensure access is appropriate based on role and job description.

Human threats represent one of the most significant hazards to the safe and secure delivery of our services. At a minimum hiring and termination procedures are in place to grant authorized access to institutional systems and data along with provisions for training. Training is an important part of ensuring the confidentiality, integrity, and availability for students and institutional information. To minimize possible security risks, all staff and faculty members are trained in their specific responsibilities under the information security program. This training includes a review of relevant ITI Policies, technology changes, and the procedures to follow in maintaining the confidentiality of classified data. The training and phishing campaign records are documented in the designated training and awareness platform. Reports and metrics are presented to the Board of trustees and Executive Leadership.

B. Physical Security

Classified or Personal Identifiable Information and all information processing systems are physically protected from unauthorized access, damage, and service disruption. For situations where hard copy documents are required, they are maintained under lock and key at all times and protected and managed. Staff, faculty, and consultants that work remotely are not permitted to print any restricted or confidential information and are bound by the university requirements remote work environments such as the access to the system shall only be via a multi-factor authentication and VPN, have installed malware and anti-virus scanning/monitoring software, and to have encrypted devices.

Data centers will have controlled access either through card swipe capabilities or key locks. Access cards and keys will be given only to those with a strict need to access, re-evaluated annually by the CIO. Regardless of the access entry system type, visitors must be accompanied by an authorized person, at all times.

C. Data Encryption

Any system or service requiring the transmission or storage of information such as Personally Identifiable Information (PII), passwords, customer account information, and non-public personal information will use an approved method of encryption or hashing as a means of protecting data. Approved methods are defined and determined by the

Chief Information Officer. Any transmission of classified information and non-public personal staff or student information sent via email must be encrypted.

D. Change Control and Configuration Management

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Sagrado has established formal Change Advisory Board (CAB) to ensure satisfactory control of all changes to equipment, software, and procedures. This Board is composed of the officials in charge of Infrastructure, Applications, and IT Projects. The CAB is a crucial component of technology change management. Its function is to review, evaluate, and approve proposed changes to ensure they align with the organization's strategic objectives, minimize risks, and promote smooth implementation. The CAB provides a collaborative platform for assessing change requests, considering potential impacts, and making informed decisions to facilitate successful change initiatives. Operational programs are subject to strict change control procedures.

Hardening guidelines (https://www.cisecurity.org/cis-benchmarks) have been adopted based on the minimum requirements established by the Center for Internet Security (CIS) and updated as new vulnerabilities are identified anti-malware is installed on all systems before being allowed on the network. System configuration documentation is created and maintained. Critical infrastructure components are reviewed for criticality classification and assignment of a minimum level of redundancy.

E. Monitoring Systems

The Chief Information Officer supervises regular monitoring of the critical systems in use by the University and evaluates whether the controls are functioning effectively and that no security breaches have occurred. This process includes the following:

1. Exception reports for security procedure violations are immediately reported to the CIO.
2. Vulnerability assessments, penetration tests, and scans are performed using approved security tools to verify the following:
    a. Critical vulnerabilities are mitigated within 30 days of receiving vulnerability notices and identification.
    b. High and medium vulnerabilities are mitigated within 90 days of receiving notices and identification.
3. Security policies and procedures will be enforced to meet time frames for remediation.
4. Report to Executive Management

F. Perimeter Security

1. Sagrado maintains security controls to protect institutional assets and information as justified by the periodic risk assessments. Perimeter security controls include the following safeguards:
   - Firewall(s)
   - Intrusion Prevention System (IPS)
   - Network Vulnerability Monitoring
   - Network Data Loss Detection
   - Virus and Malware Protection
   - DNS
   - Systems Management

2. To reduce the risks of internal abuse or misuse by authorized users as well as providing a tiered security program to protect against external attacks including non-human attacks like fire and weather-related events, the University maintains system controls such as:
   - Vulnerability management
   - Host based integrity management for critical systems
   - Configuration Management
   - Central Event log analysis
   - Back-up Procedures
   - Standards for Remote Work

G. Service Provider Oversight

While performing the procurement of services a periodic review is conducted of all outsourcing arrangements and is performed annually to confirm that service providers comply with the university policies and the industry best practices. Therefore, each service provider who has access to institutional systems or information must comply with the University's Policy for the Procurement of Goods and Services. It is the responsibility of the process owner to present new or changed requirements to ITI service providers to the Chief Information Officer for approval.

V. Interpretation of this Procedure

This Procedure is approved by the Chief Information Officer with the advice and counsel of the office of the General Legal Counsel. Questions about the scope and interpretation of this Procedure should be directed to the ITI Office at 787.728.1515, ext. 8044.

If there is any ambiguity in any provision of this Procedure, 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.

VI. Reporting Violations

Violations to this Procedure should be directed to the office of the office of Compliance, Internal Audit and Institutional Integrity at cumplimiento@sagrado.edu. Any violations

to this Procedure will be addressed in accordance with the Sagrado's policies and procedures.

Raúl Rosado
Chief Information Oficer