DT-20-2023-PE

SAGRADO
Universidad del Sagrado Corazón

Disaster Recovery Procedure

Effective: 2023.10.01

I. Purpose

The purpose of these procedures is to establish a proactive approach to safeguarding the University's assets and ensuring the continuity of critical operations during and after a natural or man-made disaster at Universidad del Sagrado Corazón ("University") pursuant to the Disaster Recovery Procedure (the "Procedure"). This includes natural and man-made disasters, such as earthquakes, hurricanes, and other emergencies. This procedure covers both on-premises and cloud hosting environments to ensure comprehensive coverage and recovery.

II. Roles and Responsibilities

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

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

3. 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).

4. Personal Identifiable Information – 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

A. For Members of the University Community

1. Backup Data
    a. Regularly backup all-important data and files to ensure their safety.
    b. Use cloud-based backup solutions provided by the Integrated Information Technology Office (ITI for its Spanish acronym) for added protection and accessibility.

2. Secure Physical Devices
    a. Safeguard laptops, mobile devices, and other equipment in protective cases.
    b. Keep devices charged and disconnect them from power sources during a natural disaster.
    c. Store devices in a safe and elevated location (preferably 24 inches from the ground) to protect them from flooding.

3. Communication
    a. Stay informed about news updates and emergency instructions issued by local authorities and the University.
    b. Follow communication channels provided by the University for official updates and announcements.
    c. Report any damages or concerns regarding IT infrastructure to the appropriate IT support personnel.

4. Power Management
    a. Unplug electronic devices and turn off power sources during the storm to protect against power surges.
    b. Utilize uninterruptible power supply (UPS) systems to provide temporary power to critical devices.
    c. Have backup power sources, such as generators, available for extended power outages.

B. For Administrators

1. Facility Preparedness
    a. Secure data centers and server rooms against potential flooding and water damage.
    b. Implement backup power solutions and ensure fuel supplies are available for extended outages.
    c. Regularly inspect and maintain backup systems, such as generators and UPS devices.

2. Cloud-Based Solutions
    a. Leverage cloud hosting for critical systems and data to ensure resilience and accessibility during and after a disaster.
    b. Review cloud service provider's disaster recovery and business continuity capabilities.
    c. Regularly test cloud-based recovery processes to ensure their effectiveness.

3. Communication and Updates
    a. Establish communication channels to provide updates to the University community during a Disaster.
    b. Coordinate with emergency management agencies and local authorities to stay informed and aligned with official instructions.
    c. Ensure regular communication with ITI staff to assess damages, monitor recovery progress, and provide timely updates.

4. Post-Disaster Assessment and Recovery
    a. Conduct a thorough assessment of ITI infrastructure, equipment, and systems after the Disaster.
    b. Prioritize recovery efforts based on the criticality of systems and the availability of resources.
    c. Restore data and systems from backups, ensuring data integrity and testing functionality.

All damages should be reported to the ITI Office at 787.728.1515, ext. 8044 or via email at misagrado@sagrado.edu

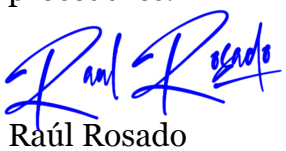
V. Interpretation of this Procedure

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 or misagrado@sagrado.edu

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