DT-32-2023-RE

SAGRADO
Universidad del Sagrado Corazón

Incident Response Procedure

Effective: 2023.10.01

I. Purpose

The purpose of these procedure is to provide a structured and efficient approach for managing and responding to security incidents or events that may affect the University's IT infrastructure, systems, and data at Universidad del Sagrado Corazón (“University”) pursuant to the Disaster Recovery Procedure (the “Procedure”). The primary goals of this procedure are as follows:

1. Minimize Impact: Respond promptly to security incidents to minimize their impact on the University's operations, systems, and services.
2. Protect University Assets: Safeguard critical systems, data, and resources from unauthorized access, breaches, or disruptions during and after security incidents.
3. Ensure Business Continuity: Implement effective containment, mitigation, and recovery measures to ensure the continuity of essential operations and services.
4. Preserve Evidence: Preserve and document evidence related to security incidents for forensic analysis, investigation, and potential legal proceedings.
5. Improve Incident Handling: Establish a defined incident response team and clear roles and responsibilities to ensure a coordinated and efficient response to incidents.
6. Enhance Detection Capabilities: Implement proactive monitoring and detection mechanisms to identify potential security incidents in a timely manner.
7. Foster Communication and Collaboration: Establish clear communication channels and mechanisms to facilitate timely reporting, information sharing, and coordination among team members, stakeholders, and relevant authorities.
8. Promote Continuous Improvement: Conduct post-incident reviews and analysis to identify areas for improvement, refine response procedures, and enhance incident response preparedness.
9. Comply with Regulations and Policies: Ensure compliance with applicable laws, regulations, and internal policies while handling security incidents.

10. Protect Reputation and Stakeholder Trust: Maintain transparency and effective communication during incident response to minimize reputational damage and maintain trust among stakeholders, including students, faculty, staff, and partners.

By following this Incident Response Procedure, the University aims to effectively respond to security incidents, mitigate their impact, and swiftly restore normal operations. Continuous improvement based on lessons learned and emerging best practices will enhance the University's incident response capabilities and strengthen its overall security posture at the university.

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. Incident - Any security-related event that poses a potential threat or harm to the IT infrastructure, systems, data, or operations. Incidents may include but are not limited to unauthorized access, data breaches, malware infections, system disruptions, and policy violations.

2. Incident Response - The process of detecting, analyzing, containing, mitigating, and recovering from security incidents. It involves a coordinated effort by the incident response team to minimize the impact of incidents, restore normal operations, and prevent future occurrences.

3. Incident Response Team - A group of individuals responsible for managing and executing the incident response process. The team typically includes representatives from IT, security, management, legal, and other relevant departments, or stakeholders.

4. Containment - The immediate actions taken to isolate and limit the impact of a security incident. Containment measures prevent the incident from spreading further and causing additional damage or harm.

5. Mitigation - The steps and measures taken to reduce the effects of a security incident and restore normal operations. Mitigation involves removing the root cause of the incident, patching vulnerabilities, and implementing controls to prevent similar incidents in the future.

6. Root Cause - The underlying factor or vulnerability that allowed a security incident to occur. Identifying and addressing the root cause is crucial for preventing similar incidents from recurring.

7. Post-Incident Review - An evaluation conducted after the resolution of a security incident. The review involves analyzing the incident response process, actions taken, and outcomes to identify strengths, weaknesses, and areas for improvement in incident response procedures, technologies, and preventive measures.

8. Business Continuity - The ability to maintain essential operations and services, even in the face of security incidents or disruptions. Business continuity measures ensure that critical functions can continue or be rapidly restored to minimize downtime and mitigate financial and operational losses.

9. Stakeholders - Individuals or groups that have an interest in or are affected by the security incidents, including students, faculty, staff, administrators, partners, regulatory bodies, and the broader University community.

10. Incident Reporting - The process of notifying the incident response team or designated authorities about a security incident. Incident reporting should include relevant details such as incident type, time of occurrence, affected systems or data, and any available evidence.

11. Lessons Learned - Insights and knowledge gained from the analysis and review of security incidents. Lessons learned help improve incident response procedures, identify areas for enhancement, and guide future incident prevention strategies and investments.

IV. Proceedings

A. Preparation Phase

1. An incident response team comprised of relevant stakeholders, including IT personnel, physical security, and legal.
2. Management Conducts regular training sessions and exercises to familiarize team members with their roles, the incident response procedure, and the tools and technologies involved.

B. Detection and Reporting

1. Monitoring systems have been established and implemented threat detection mechanisms to identify potential incidents.
2. All community members should report any suspicious activities or incidents promptly to the ITI Office at 787.728.1515, ext. 8044 or via email at misagrado@sagrado.edu

C. Assessment and Triage

1. Upon receiving an incident report, the incident response team should promptly assess the severity, impact, and nature of the incident.
2. Classify the incident based on predefined severity levels to determine the appropriate response actions.
3. Incidents will be prioritized based on their potential impact on critical systems, data, or the University's operations.

D. Containment and Mitigation

1. Isolate affected systems or networks from the rest of the infrastructure to prevent further spread of the incident.
2. Implement temporary mitigation measures, such as disabling compromised accounts, blocking network access, or disconnecting affected devices from the network.
3. Preserve any relevant evidence for further investigation or legal purposes.

E. Investigation and Analysis

1. Gather and analyze information about the incident, including system logs, network traffic data, and any other relevant evidence.
2. Identify the root cause, extent, and potential impact of the incident.
3. Determine with the legal counsel if any laws, regulations, or internal policies have been violated.

F. Response and Recovery

1. The designated incident response team will communicate a response plan based on the incident's severity and impact, outlining the necessary actions to mitigate the incident and restore normal operations.
2. Appropriate measures will be implemented to remove or remediate the cause of the incident.
3. Restore affected systems, data, or services using backups, redundancy, or disaster recovery procedures.
4. The CIO will Communicate with affected stakeholders.

G. Reporting and Documentation

1. The CIO or designated personnel will document the incident details, actions taken, and the outcomes of the response and recovery efforts.
2. The incident report will summarize the incident, its impact, the response actions, and any recommendations for future improvements.

H. Post-Incident Review

1. Updates to the incident response plan, procedures, and preventive measures based on findings will be evaluated and implemented if needed.
2. The lessons learned will be shared with the incident response team and other relevant community members to enhance incident response preparedness and resilience.

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.

Raul Rosado

Raúl Rosado
Chief Information Oficer