Information Security Incident Management Policy

Policy Statement

The exploitation of vulnerabilities in the University of Southern Mississippi (USM) computing, network, and information technology resources is inevitable. A consistent and structured response and procedures are necessary to effectively manage information security incidents.

Reason for Policy/Purpose

This policy is implemented as an effort to standardize responses to various information security incidents affecting the University of Southern Mississippi information technology resources.

Who Needs to Know This Policy

This policy applies to all students, faculty, staff, contractors, consultants, temporaries, and other workers of USM, including all personnel affiliated with third parties using USM information technology resources, unless otherwise excluded by a specific section.

Website Address for this Policy

www.usm.edu/institutional-policies/policy-acaf-it-027
Definitions

Breach: An incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an unauthorized party.
Cardholder: An individual issued or authorized to use a payment card.
Cardholder Data (CHD): The full primary account number, either with or without the cardholder’s name, the expiration date, and/or the service code.
Cardholder Data Environment (CDE): People, processes, and technology that store, process, or transmit CHD.
Device: An instrument used to process or store digital records and data; including, but not limited to, personal computers, workstations, laptops, tablets, externally connected hard drives, flash drives, removable media, and any other equipment or media capable of electronically storing data.
Event: Any anomalous occurrence affecting the normal operation of an information system, device, or network; or the deviation from an institutional policy or process that affects an information system or process.
Incident: One or more events that negatively impacts the confidentiality, integrity, or availability of information or an information system.
Incident Handler: Individual responsible for evaluating events and coordinating incident response efforts.
Incident Responder: Individual participant to an incident response effort.
Payment Card Industry Data Security Standards (PCI DSS): A set of information security standards that sets expectations for how organizations handle payment card data and information.
PCI Scope: Devices, processes, and areas affected by the PCI DSS.
Protected Health Information (PHI): Individually identifiable information concerning a person’s health, maintained by a covered entity or business associate, including demographic information.
Personally Identifiable Information (PII): Information, when used by itself or with other information, can be used to uniquely identify an individual.

Policy

1. Plan
   1.1 A University Incident Response Plan detailing the methodology for responding to incidents must be developed and published as a separate document.
   1.2 The Incident Response Plan must include specific procedures for addressing incidents affecting PCI scoped systems and software.
   1.3 The Incident Response Plan must include specific procedures for addressing rogue and unmanaged wireless access points.

2. Notification
   2.1 Events that pose an immediate risk to the life or health of persons must be reported to law enforcement.
   2.2 Information Technology Services (iTech) personnel must report events to either the Incident Handler on duty or to the Help Desk.
2.3 Non-iTech personnel must report events affecting devices owned, leased, or managed by the University of Southern Mississippi to The Help Desk by phone (601-266-4357) or by email to helpdesk@usm.edu.

3. **Incident Response**
   3.1 Individuals not designated as a responder must not attempt any remediation activity that may directly affect the device. This includes, but is not limited to: restart, shutdown, file maintenance, installation of software, removal of software, malware scanning, or process termination.
   3.2 Devices that have been affected by an event or incident should be removed or disconnected from the network, if possible.
   3.3 Individuals witnessing an event should document as much information about the incident as possible. Examples of information to document include: date, time, description of events, duration of events, any dialog boxes or messages, system behavior, or anomalies.
   3.4 If an incident has occurred and the affected/offending device or its responsible party cannot be immediately identified, iTech may disrupt the network connectivity of that device.
   3.5 iTech employees and other university personnel will not provide incident response for devices owned and operated by a third-party, with the exception of response activities and services previously specified in an existing agreement.

4. **Incident Prioritization**
   4.1 The Information Security Incident Response Plan will define prioritization levels of incidents based on the impact to business functionality, impact on information, and the recoverability of systems and information.
   4.2 Incidents will be prioritized as “Low”, “Urgent”, or “Critical”.
   4.3 Any incident resulting in the potential breach of federal or state regulated information, PII, PHI, or payment card information must be prioritized as “Critical”.

5. **Responsibilities**
   5.1 Persons responsible for information technology resources involved in an incident must cooperate with incident responders.
   5.2 Responders, witnesses, and individuals affected by an incident must respect the privacy and confidentiality of any information, documents, and data they may be exposed to, either intentionally or unintentionally.

6. **Documentation and Communication**
   6.1 iTech shall maintain an information store that will be used to record contact information for responders, responsible parties of major systems, liaisons to college and administrative units, and pertinent external entities.
   6.2 iTech shall maintain an information store that will provide for the retrievable storage of documentation detailing information security incidents and response actions.
   6.3 iTech must notify stakeholders and data owners affected by an incident.
   6.4 Responders, witnesses, and individuals affected by a security incident must not comment to news agencies, general public, or the university community about the details of an incident or response to an incident.
7. **Enforcement**

7.1 Failure to comply, in whole or in part, with this policy may result in revocation of access to the University of Southern Mississippi information technology resources, and/or disciplinary action in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.

7.2 Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be subject to revocation of access privileges to the University of Southern Mississippi network, as well as any penalties provided by any existing contracts with USM.

---

**Review**

The Technology Security Officer is responsible for reviewing this policy annually.

**Forms/Instructions**

N/A

**Appendices**

Appendix A – Incident Response Plan
Appendix B – Incident Response Report Form

**Related Information**

Information Security Incident Response Plan

**History**

**Amendments:** 2/7/17 – Inclusion of Appendices
Authorization

Title: Information Security Incident Management Policy

Policy number: ACAF-IT-027

RECOMMENDED BY:

Responsible University Administrator

Responsible University Officer

REVIEWED BY:

Director of Compliance and Ethics

Office of General Counsel

APPROVED:

President