APPENDIX A

Information Security Incident Response Plan for the University of Southern Mississippi

Date: 04/13/16

Prepared By: Bob Wilson

Technology Security Officer

University of Southern Mississippi

1. **Introduction**
   1. The exposure of university computing and network resources to various threats is inevitable. A consistent and structured response procedure is necessary to effectively manage information security incidents.
2. **Purpose**
   1. This document details the expected actions and procedures used to respond to an Information Security Incident.
3. **Scope**
   1. The Information Security Incident Response Plan applies to:
      1. Computer workstations, laptops, servers, networks, network capable devices, data, information, and other technology resources owned, leased, or managed by USM.
4. **Incident Response Overview**
   1. The Incident Response Process will flow through 6 primary phases, each phase with response activities, documentation activities, and communication activities. These phases are:
      * Preparation
      * Identification
      * Containment
      * Eradication
      * Recovery
      * Lessons Learned
5. **Incident Handler and Incident Response Team** 
   1. An iTech Security Analyst will typically act as the Incident Handler. If a Security Analyst is not available, the Technology Security Officer will designate an incident handler.
   2. Duties of the Incident Handler:   
      Evaluates reported events  
      Classifies Incidents  
      Coordinates response activity for incidents  
      Documents incident response  
      Communicates the existence and status of incidents to the Technology Security Officer.
   3. Incident Handler may convene an Incident Response Team, if necessary.
   4. Other Incident Response Participants and their roles:  
      1. Office of the CIO:   
         Communicates the existence and status of incidents to University Senior Leadership, Data Owners, and Stakeholders.
      2. Operations and Infrastructure Personnel:   
         Performs response activities and recovery services for devices, systems, and information maintained or managed by iTech; or for 3rd party devices, systems, and applications, as specified by existing agreement.
      3. Help Desk Technicians  
         Receive initial event reports.  
         Communication of event reports to Incident Handler
      4. Desktop Technicians  
         Performs response activities and recovery services for University owned client endpoint systems.
      5. University Communications  
         Provides communication of Incident information to the public and to the University Community
      6. General Counsel  
         Provides guidance on regulatory compliance and legal issues related to information or systems affected by Incidents
      7. The Director of Student Financial Services  
         Provides guidance in matters related to financial services and Payment Card Industry.
6. **Preparation Phase**
   1. The preparation phase of the Incident Response will comprise of the following activities:  
      1. The TSO will review the Incident Response Policy and Incident Response Plan at least annually, and modify as necessary.
      2. The TSO will ensure the Incident Response Policy is published and available to the campus community.
      3. The TSO will ensure Incident Handlers are trained on how to properly execute this plan.
      4. The TSO will recommend and acquire, if possible, tools relevant to incident response efforts.
7. **Identification Phase**
   1. Don’t Panic
   2. There are three specific types of events that do not require evaluation by an Incident Handler or the creation of an Incident Report:  
      * Malware or virus infections of endpoint client systems that do not have the potential to expose regulated or private data.
      * Incidents involving the complaints of alleged violations of the Digital Millennia Copyright Act (DMCA).
      * Incidents involving Rogue Wifi Access Points that do not affect PCI Card Holder Data environments.
   3. For any other event not excluded by 7.2, when an event is reported, the Incident Handler will start an Incident Report using the Information Security Incident Report form.
   4. The Incident Handler on duty will investigate the facts of the matter by collecting evidence; examining system and network behavior; and interviewing relevant personnel.
   5. The Incident Handler will evaluate the impact of the event based on the following factors:  
      * Impact on the confidentiality, integrity, and availability of information
      * Impact to business
      * Ability to recover systems or information

|  |  |  |
| --- | --- | --- |
| Information Impact | | |
| Impact | Score | Description |
| None | 0 | No impact on information |
| Data unavailable | 1 | Data necessary for business has been made unavailable |
| Integrity Loss | 2 | Information was modified |
| Proprietary Breach | 3 | Non Private Information accessed by unauthorized actors |
| Privacy Breach | 6 | Private or regulated information accessed by unauthorized actors |
|  |  |  |
| Business Impact | | |
| Impact | Score | Description |
| None | 0 | No impact on business |
| Low | 1 | Non critical business process affected or interrupted |
| Med | 2 | Business efficiency significantly affected |
| High | 3 | Critical business function is interrupted |
|  |  |  |
| Recoverability | | |
| Impact | Score | Description |
| None | 0 | No recovery needed |
| Low | 1 | Full recovery with little or no effort |
| Extended | 2 | Recovery effort involves extended time or additional resources |
| Unrecoverable | 3 | Data or system cannot be recovered. |

* 1. The Incident Handler will then prioritize the event, based on the total impact scores of the event.

|  |  |  |
| --- | --- | --- |
| Total Score | Prioritization | Detail |
| 0 | None | The event is either a false positive or has no impact on information, business processes, or systems. |
| 1 - 3 | Low | Low Priority incidents do not pose a threat to regulated systems or information, and can be resolved by routine procedures |
| 4 - 5 | Urgent | Urgent Priority incidents do not pose a threat to regulated systems or information, but cannot be resolved by routine procedures. |
| 6 - 9 | Critical | Critical incidents pose a threat to private or regulated information, regulated or business critical systems, or the long term success of the University. |

* + 1. Events that carry a total impact score of “0” are not incidents.
    2. Any event or group of related events that carry a score of “1” or greater is considered an incident.
    3. Incidents that involve information classified as one or more of the following categories, is automatically considered a Critical Incident:
       - Private Health Information
       - Personally Identifiable Information
       - Payment Card Information
       - Information protected by FERPA
  1. The Incident Handler will report the event.
     1. If the event is not an incident, relevant information is recorded and the incident report is closed. The event is then reported by email to the iTech Leadership, stakeholders, and systems owners.
     2. If the event is determined to be an incident, the Incident Handler will immediately notify iTech Leadership about the incident and proceed through the rest of the Incident Response Plan.

1. **Mandatory Response Procedures for Incidents Affecting Payment Card Information**
   1. If during the “Identification Phase”, an incident of unauthorized access is confirmed and card holder data was potentially compromised, the following procedures must be performed:  
      1. Don’t Panic
      2. The Incident Handler, must notify the Technology Security Officer, who will in turn notify the following University personnel:
         1. Chief Financial Officer
         2. Chief Information Officer
         3. Director of Student Financial Services
         4. University Police Department
         5. General Counsel
      3. The Director of Student Financial Services will be responsible for contacting the University’s Acquiring Bank(s), the Acquiring Bank will be responsible for communicating with the card brands (VISA, MasterCard)
      4. For incidents involving American Express cards, director of Student Financial Services must contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident.
         1. Phone number: (888) 732-3750
         2. Email: EIRP@aexp.com.
      5. If Discover Network payment cards are potentially included in the breach the Director of Financial Services must notify Discover Security within 48 hour by calling the phone number: (800) 347-3083
      6. Assist card industry security and law enforcement personnel in investigative process.
2. **Containment and Eradication**
   1. Don’t Panic
   2. The Incident Handler will assemble a team of appropriate personnel for addressing any containment and eradication functions necessary to properly remediate the incident. If a team is not necessary, the Incident Handler will delegate the response to an appropriate operations person.
   3. If at all possible, operations staff will enact the business continuity plan for the affected systems or applications and the systems or applications will be made unavailable as to mitigate any further control or interaction by threat actors.
   4. The Incident response team will meet, determine response and develop a plan to execute the response. If the response has been delegated to a single person, that person and incident handler will develop a response plan.
   5. The Incident Response Team, TSO, and related Operations personnel will occasionally meet during the response to discuss findings and progress. If response has been delegated to a single person, this person will occasionally brief the Incident Handler to the status of the response and any related findings.
   6. Specific procedures for the detection of Rogue Wireless Access points.  
      1. Any device that shares our 802.11 Wi-Fi spectrum and is not managed by USM will be considered a rogue device.
      2. Rogue devices will be contained via a method of using over-the-air packets to temporarily interrupt service on a rogue device until it can physically be removed. Containment works by spoofing de-authentication packets with the spoofed source address of the rogue AP so that any clients associated are kicked off.
3. **Recovery**
   1. When the response plan has been completed, Operations personnel and Incident Response team will brief the TSO, detailing the outcome of remediation efforts and findings.
   2. If necessary, the Operations staff will perform Disaster Recovery duties to recover systems and data to a pre-incident state, and the Incident Handler will document the Recovery efforts and outcome.
4. **Lessons Learned and Monitoring**
   1. The Incident Response team or responding individual and Incident Handler will meet and discuss the incident, remediation efforts, and recovery efforts.
   2. The Incident Handler will report the summary of the incident and any recommendations to iTech Leadership, Stakeholders, and System Owners.
      1. The incident handler will note if recommendations have been accepted or not.
      2. If recommendations are accepted, a due date and the person(s) responsible for the implementation of recommendations will be noted on the Incident Response Report.
   3. The TSO may use information from the response in consideration for purposes of modifying the Incident Response Plan or Incident Response Policy.
   4. Operational Personnel will monitor the system and network traffic for specific indications of incident relapse for a period of 21 days.  
      1. If an event is discovered and determined to be an incident, operational staff will report the event and the Incident Handler will start the Incident Response plan again.

1. **Appendices**
   1. Incident Report Form: incidentReport-Win.xlsx

