Information Security Incident Response Procedures

PURPOSE

Central Michigan University's (CMU) Office of Information Technology (OIT) has adopted the following procedures and guidelines for responding to information security incidents and to provide operation detail to complement the INFORMATION SECURITY INCIDENT RESPONSE POLICY. These procedures apply broadly to all Institutional Data, and further apply to all faculty, staff, students and third-party Agents of the University as well as any other CMU affiliate who is authorized to access Institutional Data or CMU networks.

AUTHORITY

Execution of these procedures will be managed by the Chief Information Security Officer (CISO) under the guidance of the TPC and Chief Information Officer (CIO) and as established by the INFORMATION SECURITY POLICY.

ROLES AND RESPONSIBILITES

The security incident response process incorporates the INFORMATION SECURITY POLICY definitions and extends or adds the following roles:

- **The Information Security Office (ISO)** collectively describes the CISO, other OIT employees, other CMU staff, or outside contractors who conduct the technical work to 1) gather, preserve, and analyze evidence and 2) return affected equipment to full operations so that an incident can be closed.
- **The Incident Commander** is the ISO employee (or designee) who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring the information is complete, and reporting on incident status both during and after the investigation
- **Law Enforcement** includes the CMU Police, federal, state, and local law enforcement agencies, and the U.S. government agencies that present warrants or subpoenas for the disclosure of information. Interactions with these groups will be coordinated with the Office of General Counsel ("OGC").
- **The Office of General Counsel (OGC)** for the University acts as the liaison between the ISO and external Law Enforcement and provides guidance on the extent and form of all responses and disclosures to law enforcement and the public.
- **Academic and Business Officers** are the CMU leaders overseeing significant CMU academic and business offices and/or designated for overseeing the various regulatory frameworks to which the University is required to comply.

EVIDENCE PRESERVATION

The goal of Security Incident Response is to reduce and contain the scope of a security incident and ensure that IT assets are returned to service as quickly as possible. Rapid response is balanced by the requirement to collect and preserve evidence in a manner consistent with the requirements of rules 26-34 of the Federal Rules of Civil Discovery and to abide by legal and administrative requirements for documentation and chain of custody.

PHASES OF INFORMATION SECURITY INCIDENT RESPONSE

OIT utilizes the National Institute of Standards and Technology (NIST) Special Publication 800-61 as a guide for security incident response that encompasses four phases as shown below in Figure 1:

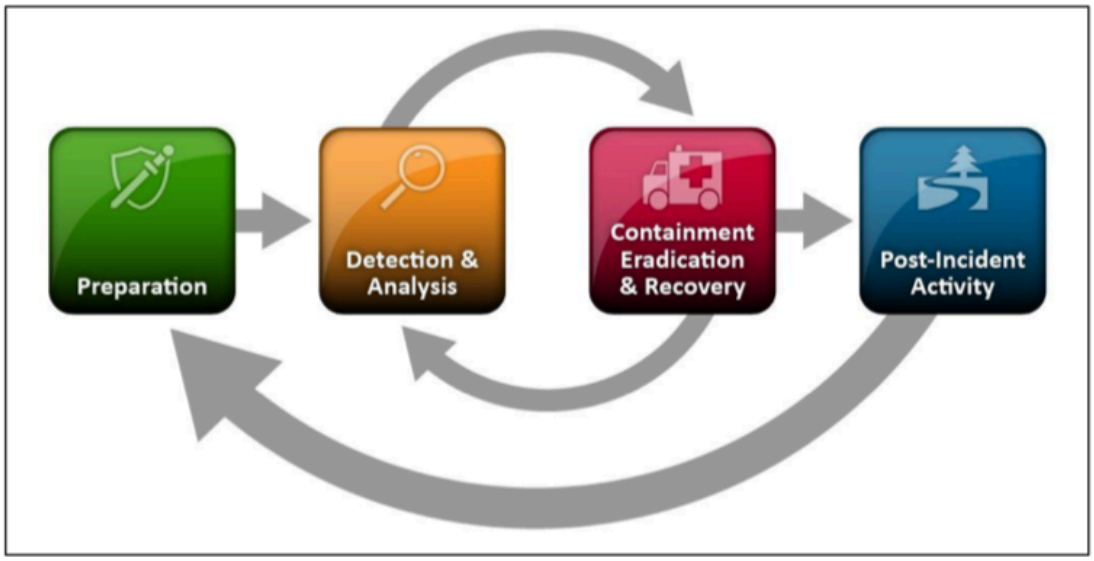

Figure 1 – Information Security Incident Response Phases

Phase I: Preparation includes those activities that enable the ISO to respond to a security incident: Policies, tools, procedures, effective governance, and communication plans. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after a security incident is discovered. Post-mortem analyses from prior incidents will form the basis for continuous improvement of this phase.

Phase II: Detection and Analysis includes activities to analyze symptoms that might indicate a Security Incident, and to determine the level of severity for those identified as Incidents. Initial Detection and Analysis activities will focus on determining the nature of the Security Event. The definitions below will guide OIT's actions through this phase.

- **Security Event** means any unconfirmed or reported concern or complaint related to the inappropriate access, misuse, theft, or compromise of the University's information, information technologies, or information systems.
    - ALL CMU Employees are required to report the theft or exposure of CMU's Restricted Information by the DATA STEWARDSHIP POLICY. All OIT employees are additionally responsible for identifying and reporting Security Events as defined by the INFORMATION SECURITY INCIDENT RESPONSE POLICY. No matter where the intake process begins, a ticket must be created and assigned to the IT_INFO_SECURITY ticketing group. If the employee believes that the security incident is likely to be classified as "high" severity based on the above descriptions, they must also report it to their supervisor. The CISO or designee will review all tickets, determine severity and sensitivity, and assign security incident commanders as appropriate. For insider threats, see below for appropriate intake. In the event that investigation into Security Event yields no evidence of a Security Incident or Breach, the Ticket will be closed.

- **Security Incident** means any confirmed inappropriate access, misuse, theft, or compromise of the University's information, information technologies, or information systems, requiring investigation and/or significant follow-up, and/or non-routine action. Security incidents requiring formal breach response are escalated to breach status.
    - Examples of security incidents include, but are not limited to:
        - Unauthorized access to data, especially protected or restricted data
        - Computing device infected with malware
        - Denial of Service (DoS) attacks
        - Reconnaissance activities such as scanning the network for security vulnerabilities
        - Web site defacement

        - Violation of CMU security policy
    - Security Incidents may also be established by review of sources, including, but not limited to:
        - Monitoring systems
        - Reports from CMU staff or outside organizations
        - Service degradations or outages

  Detected vulnerabilities will not be classified as incidents. OIT employs tools to scan the CMU environment and depending on severity of found vulnerabilities may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of compromise or sensitive data exposure, vulnerabilities will be communicated and documented, and the Information Security Office ("ISO") will pursue available technology remedies to reduce risk.

- **Security Breach** means any confirmed inappropriate access, misuse, theft, or compromise of the University's Protected or Restricted data or information technologies requiring formal breach response, reporting, and/or notification(s) (such as those required for HIPAA-related incidents). Security Breaches are one type of High Severity Security Incidents, as defined below.

Because the activities in the next phase - Incident Containment, Eradication, and Recovery- will be managed based on the level of severity of the Security Incident, that level of severity is assigned during the Detection and Analysis phase of response. The level of severity is a measure of its impact on or threat to the operation or integrity of the institution and its information, and determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. OIT recognizes three levels of Security Incident severity: High, Medium, and Low.

- A Security Incident will be considered "**High Severity**" if any of the following conditions exist:
    - Threatens to have a significant adverse impact on a large number of systems and/or people, such as the entire institution.
    - Poses a potential large financial risk or legal liability to the University
    - Threatens restricted data, such as the compromise of a server that contains names with social security numbers or credit card information.
    - Adversely impacts, either currently or imminently, a core system or service critical to the operation of a major portion of the University, such as the learning management system or a major portion of the campus network.
    - Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
    - Has a high probability of propagating to many other systems on and/or off campus and causing significant damage or disruption.
    - Indication that a Security Breach of protected or restricted data has likely occurred.
    - **Expectations for Response to High Severity Security Incidents**: OIT expects response time for High Severity Security Incidents to be immediate. The Chief Information Security Officer will notify and inform the CIO, then, acting in league with the CIO, coordinate the ISO's technical investigation and recovery from the Security Incident, while the CIO will act as Incident Commander and convene a steering team to guide CMU's response to the Security Incident. This steering team will include the President, the Provost, the General Counsel, the AVP for University Communications, the CISO, other appropriate business or academic officers, and, if HIPAA-related, the HIPAA Privacy and Security Officers. A "Lessons Learned" session and Post-Incident Report are required following each High Severity Security Incident.

- A Security Incident will be considered "**Medium Severity**" if any of the following conditions exist:
    - Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building.
    - Adversely impacts a non-core service
    - Adversely impacts a departmental system or service, such as a departmental file server
    - Disrupts a building or departmental network.
    - Has a moderate probability of propagating to other systems on and/or off campus and causing

moderate damage or disruption
    - **Expectations for Response to Medium Severity Security Incidents:** OIT expects to respond to Medium Severity Security Incidents within 4 hours. The CISO or appropriate OIT Director will act as Incident Commander and will convene a steering team consisting of appropriate CMU academic and business officers, OIT's University Communications Liaison, and appropriate members of the ISO to coordinate recovery and response. A "Lessons Learned" and Post-Incident Report are not required unless requested by the CIO or CISO.

- A Security Incident will be considered "**Low Severity**" if it exhibits the following characteristics:
    - Adversely impacts a very small number of systems or individuals
    - Disrupts a very small number of network devices or segments
    - Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate.
    - **Expectations for Response to Low Severity Security Incidents:** OIT expects to respond to Low Severity Security Incidents within one business day. Recovery and response will be managed by staff assigned to the affected service(s). A "Lessons Learned" is not required, nor is a Post-Incident Report.

Phase III: Containment, Eradication, and Recovery includes two parts – 1) the technical activities that attempt to contain the incident, and if necessary, recover from it by restoring any affected resources and/or processes, and 2) the administrative activities required to communicate to affected individuals and the public.

The technical activities could lead to the identification of additional indicators of compromise and might shift the Incident back into the Detection and Analysis phase. These activities include, but are not limited to:

- Segmenting or disconnecting a device from the network
- Stopping or shutting down services on a device
- Restricting access to one or more technology services
- Confiscating a CMU-owned device to perform additional analysis or restoration
- Monitoring of suspicious activity
- Creating/modifying firewall rules
- Changing passwords
- Installing patches
- Conducting Forensics investigations, including imaging of devices
- Restoring systems and/or processes

The administrative activities include, but are not limited to:

- Engaging Beazley, Marsh, or other vendors to conduct research into reporting/communication requirements, gain access to bulk buys of ID protection services, obtain templates for communication, or conduct forensic services.
- Issuing letters or other communications to affected individuals or organizations.

Phase IV: Post-Incident Activity includes activities (such as the "Lessons Learned" meetings referenced above) to analyze the relevant security incident handling procedures with the goals of improving those processes, and to reduce the probability of similar future incidents. Post-incident reports, where applicable, will be created and disseminated during this phase. The report should minimally contain the following: A description of the security incident, the impact or potential impact of the security incident such as system downtime, the classification of any data involved in the security incident, and any suggestions for improvement of the security incident response process or future mitigation strategies. Response to every incident, regardless of severity, must include review of all applicable response metrics with suggestions for improvement if appropriate.

ADDITIONAL INCIDENT RESPONSE CONSIDERATIONS

- **Escalation**
  - Security Incidents may be escalated at any point in the recovery process based upon new developments in the investigation. Escalation from Low Severity to Medium Severity may be done unilaterally by the CISO. Escalation from Medium Severity to High Severity will be recommended to the CIO by the CISO and escalated by the CIO.
- **Interactions with Law Enforcement**
  - No communications with external law enforcement authorities may occur without the approval of the Office of General Counsel. The ISO works with these entities, where authorized by OGC, to determine the information requirements and to share the minimum necessary information as required for incident response.
- **Communications Plan**
  - Public communications about a Security Incident will be released by University Communications or their designee after appropriate conversation with the incident steering committee, or, at minimum, the OGC. Should a Security Incident become a Security Breach or suspected Security Breach, both the CISO and CIO should be notified immediately.
- **Privacy**
  - All incident response procedures will follow the current privacy requirements as set out in the DATA STEWARDSHIP POLICY. Exceptions must be approved by OGC.
- **Insider Threats**
  - In the case that the Incident Commander is a person of interest in a security incident:
    - The Chief Information Security Officer will act in their stead or appoint a designee to act on their behalf.
  - In the case that the Chief Information Security Officer is a person of interest in a security incident:
    - The normal intake process should not be used. Instead, the security incident should be reported directly to the Chief Information Officer (CIO) who will act in their stead or appoint a designee to act on their behalf.
  - In the case that another CMU administrative authority is a person of interest in an incident:
    - The Chief Information Security Officer will work with the remaining administrative authorities in the Chief Information Security Officer's reporting line to designate a particular point of contact or protocol for communications.

ADDITIONAL POLICIES AND INFORMATION

Questions or concerns related to these procedures should be directed to CMU's CISO at 989.774.7445. Additional information can also be found using the following resources:

- Information Security Policy
- Data Stewardship Policy
- Responsible Use of Computing
- SAP Security – Authority, Rights and Responsibilities
- Web Policy
- Social Security Number Policy
- Computer Disposal Policy
- Accepting Credit Card Payments
- Identity Theft Red Flags
- HIPAA Policies – see Chapter 12
- Security-Related Protocols and Standards