


|  |   |   |                |        |
|--|---|---|----------------|--------|
| <br><b>SOUTHEAST MISSOURI</b><br><b>STATE UNIVERSITY · 1873</b> | <b>INFORMATION<br/> SECURITY<br/> INCIDENT<br/> PROCEDURE</b> | Date Issued:                                | Revision Date: | Page:  |
|  |   | 09/17                                       | 12/23          | 1 of 8 |
|  |   | Classification Code:                        |                |        |
|  |   | Section:                                    |                |        |
|  |   | INFORMATION TECHNOLOGY                      |                |        |
|  |   | Subject:                                    |                |        |
|  |   | INFORMATION SECURITY INCIDENT<br>MANAGEMENT |                |        |

**GENERAL STATEMENT**

This document describes the procedures associated with Southeast Missouri State University's Information Technology Incident Management Policy 10-04. Policy 10-04 comprises strategic statements for managing security incidents at the university's main and regional campuses. These procedures detail the required processes, based on incident severity, to comply with IT Policy 10-04.

**INCIDENT REPORTING:**

Members of the university community must report any suspected security incidents using one of the methods below:

- For suspected high-severity events, such as potential breaches of personal identity data, report directly to the Information Security Officer as quickly as possible via phone, email, or in person.
- Report all other suspected incidents either to the Information Security Officer or to IT support personnel, who can then contact the Information Security Officer.
- If the Information Security Officer is unavailable, contact the Assistant Vice President for Information Technology as the initial point of contact.


**INCIDENT CLASSIFICATION:**

When the Information Security Officer receives notification, discovers, or suspects an incident, they will initiate an investigation. They will then determine if the incident is a false positive or a genuine occurrence. If the incident is real and requires action, the Information Security Officer will assess its severity level by considering the following factors:

- a. Scope of impact – how many individuals, departments, or systems does it affect?
- b. Criticality of the system or service – How crucial is it to the institution's ongoing operation? What would be the functional or financial impact on the business if the system or service became unavailable or compromised?
- c. Sensitivity of the information - Does the system or service store or provide access to confidential data, such as personally identifiable information or credit card details?
- d. Probability of propagation – What is the likelihood of malware or negative effects spreading to other systems, particularly those off-campus?

If the Information Security Officer is unable to determine an incident's severity level, they will consult the Assistant Vice President for Information Technology for guidance.

Each Incident Severity Level follows a specific set of procedures, including escalation, action items, and personnel involvement.

|  |   |   |                         |                 |
|--|---|---|-------------------------|-----------------|
|  <p><b>SOUTHEAST MISSOURI<br/>STATE UNIVERSITY · 1873</b></p> | <p align="center"><b>BUSINESS<br/>POLICY<br/>AND<br/>PROCEDURE<br/>MANUAL</b></p> | Date Issued:<br>09/17                                   | Revision Date:<br>12/23 | Page:<br>2 of 8 |
|  |   | Classification Code:<br>10-04                           |                         |                 |
|  |   | Section:<br>INFORMATION TECHNOLOGY                      |                         |                 |
|  |   | Subject:<br>INFORMATION SECURITY INCIDENT<br>MANAGEMENT |                         |                 |

**Severity Levels:**


The severity level of an incident subjectively measures its impact on or threat to the institution's operation or integrity and its information. This level determines the incident handling priority and the response's timing and extent. During an incident investigation, the severity level can change based on newly discovered information.

- a) **High** - A security incident will have a "high" severity level under any of the following conditions:
- It significantly and adversely affects numerous systems or people (e.g., a large portion of the student population).
  - It compromises confidential data (e.g., a server breach that exposes credit card numbers or names with social security numbers).
  - It disrupts an enterprise system or service crucial to a major portion of the university's operation (e.g., email, student information system, financial information system, human resources information system, learning management system, Internet service, or a significant part of the campus network).
  - It has a high likelihood of spreading to many other on-campus or off-campus systems and causing significant damage or disruption (e.g., a malicious infection spreading between departments).

High severity incidents necessitate an immediate response and dedicated attention from the ISO, relevant University officials, and IT staff until resolved. These incidents also require extensive notification and reporting, as outlined in the table below. A Post-Incident Report is mandatory. If the incident potentially exposes personal identity data, notifying individuals according to state or federal law may be required.

- b) **Medium** - A security incident is classified as "medium" severity if it meets any of the following criteria:
- Negatively affects a moderate number of systems or people, such as a single department, unit, or building.
  - Negatively affects a non-critical enterprise system or service.
  - Negatively affects a departmental system or service, like a departmental file server.
  - Interrupts a building or departmental network.
  - Possesses a moderate probability of spreading to other on-campus or off-campus systems and causing moderate damage or disruptions.

Personnel from the affected unit, primarily responsible for addressing the incident, must respond quickly to medium severity incidents. The table below outlines the notification requirements. The Assistant Vice President for Information Technology or another relevant administrator will request a Post-Incident Report if needed.

|  |   |   |                         |                 |
|--|---|---|-------------------------|-----------------|
| <br><b>SOUTHEAST MISSOURI</b><br><b>STATE UNIVERSITY · 1873</b> | <b>BUSINESS</b><br><b>POLICY</b><br><b>AND</b><br><b>PROCEDURE</b><br><b>MANUAL</b> | Date Issued:<br>09/17                                   | Revision Date:<br>12/23 | Page:<br>3 of 8 |
|  |   | Classification Code:<br>10-04                           |                         |                 |
|  |   | Section:<br>INFORMATION TECHNOLOGY                      |                         |                 |
|  |   | Subject:<br>INFORMATION SECURITY INCIDENT<br>MANAGEMENT |                         |                 |


c) **Low** - Classify the severity of a security incident as "low" if any of the following conditions are present:

- Affects a very limited number of systems or individuals.
- Disrupts a very small number of network devices or segments.
- Poses negligible risk of propagation or would cause minor disruption or damage during propagation attempts.

Since a single compromised system can activate and harm other systems at any time, the relevant personnel (typically the technical support staff responsible for the system) must respond as swiftly as possible, no later than the next business day. The table below outlines notification requirements. A Post-Incident Report is necessary only if requested by the Assistant Vice President for Information Technology or another suitable administrator.

d) **NA** ("Not Applicable") - Use this designation for events reported as suspected IT security incidents that, upon investigation of the suspicious activity, reveal no evidence of a security incident. This designation typically corresponds to the incident category, "No Incident."

| <b>Severity</b> | <b>Characteristics (one or more conditions present determines the severity)</b>  | <b>Response Time</b>  | <b>Incident Manager</b>                   | <b>Who to Notify</b>   | <b>Post-Incident Report Required</b> |
|-----------------|--|---|---|--|--------------------------------------|
| <b>High</b>     | 1) Significant adverse impact on many systems and/or people<br>2) Threatens confidential data<br>3) Adversely impacts a critical enterprise system or service<br>4) Significant and immediate threat to human safety<br>5) High probability of propagating to a large number of other systems on or off-campus and | Immediate or as quickly as possible after investigation or triage | ISO, AVP for IT, or an IT Department head | 1) Information Security Officer<br>2) Assistant Vice President for IT<br>3) Department Administrator(s) affected<br>4) Technical support for affected device(s)<br>5) Public notification as recommended by university leadership if the situation warrants. | Yes                                  |


|  |   |  |                         |                 |
|--|---|--|-------------------------|-----------------|
| <br><b>SOUTHEAST MISSOURI STATE UNIVERSITY · 1873</b> | <b>BUSINESS POLICY AND PROCEDURE MANUAL</b> | Date Issued:<br>09/17                                | Revision Date:<br>12/23 | Page:<br>4 of 8 |
|  |   | Classification Code:<br>10-04                        |                         |                 |
|  |   | Section:<br>INFORMATION TECHNOLOGY                   |                         |                 |
|  |   | Subject:<br>INFORMATION SECURITY INCIDENT MANAGEMENT |                         |                 |

|               |  |                   |                                       |   |   |
|---------------|--|-------------------|---------------------------------------|---|---|
|               | causing significant disruption   |                   |                                       |   |   |
| <b>Medium</b> | <ol style="list-style-type: none"> <li>1) Adversely impacts a moderate number of systems and/or people</li> <li>2) Adversely impacts a non-critical enterprise system or service</li> <li>3) Adversely impacts a departmental scale system or service</li> <li>4) Moderate risk of propagating and causing further disruption</li> </ol> | Same day          |                                       | <ol style="list-style-type: none"> <li>1) Information Security Officer</li> <li>2) Assistant Vice President for IT</li> <li>3) Department Administrator(s) affected</li> <li>4) Technical support for affected device(s)</li> </ol> | No, unless requested by AVP for IT or another appropriate administrator |
| <b>Low</b>    | <ol style="list-style-type: none"> <li>1) Adversely impacts a very small number of non-critical individual systems, services, or people</li> <li>2) Little risk of propagation and further disruption</li> </ol>   | Next business day | Technical support for affected device | <ol style="list-style-type: none"> <li>1) ISO</li> <li>2) Assistant Vice President for IT</li> <li>3) Department Administrator(s) affected</li> </ol>   | No, unless requested by AVP for IT or another appropriate administrator |
| <b>NA</b>     | "Not Applicable" – used for suspicious activities which upon investigation are determined not to be an IT security incident.   |                   |                                       |   |   |

### Campus Security Incident Response Team (CSIRT) Membership:

The primary task of the CSIRT involves investigating, reporting, and resolving incidents in a timely manner. To accomplish this, the CSIRT comprises subject matter experts who can effectively address and respond to incidents.

The CSIRT membership may vary based on the specific incident. However, the CSIRT typically includes a core group of the following individuals:

|  |   |   |                |        |
|--|---|---|----------------|--------|
|  <p><b>SOUTHEAST MISSOURI<br/>STATE UNIVERSITY · 1873</b></p> | <p align="center"><b>BUSINESS<br/>POLICY<br/>AND<br/>PROCEDURE<br/>MANUAL</b></p> | Date Issued:                                | Revision Date: | Page:  |
|  |   | 09/17                                       | 12/23          | 5 of 8 |
|  |   | Classification Code:                        |                |        |
|  |   | Section:                                    |                |        |
|  |   | INFORMATION TECHNOLOGY                      |                |        |
|  |   | Subject:                                    |                |        |
|  |   | INFORMATION SECURITY INCIDENT<br>MANAGEMENT |                |        |

- Information Technology staff responsible for maintaining the breached device, such as:
  - Security Analysts
  - System Administrators
  - Network Engineers
- Other affected department staff. Depending on the severity of the incident, the CSIRT will invite other executive staff to include Assistant Vice President, Marketing & Communications, Vice-President for Administration and Finance and the University Chief of Staff.

Depending on the scope and impact of the incident, additional members may include, but are not limited to:

- Application Administrators
- Database Administrators
- Web Developers / Administrators
- Other IT Staff

The Information Security Officer leads the CSIRT, directing the activities and assignments of its members until the resolution of the incident. This officer collaborates with appropriate management to prioritize the work of CSIRT members. Once the incident is fully resolved, the Information Security Officer relieves the CSIRT of its responsibilities and disbands the team. If the Information Security Officer is unavailable, the Assistant Vice President for Information Technology assumes this role.


**CSIRT RESPONSIBILITIES:**

Throughout the incident response, CSIRT members must maintain a log of all incident-related activities and submit copies to the Information Security Officer upon incident resolution for inclusion in the Incident Summary Report. These logs must contain:

- Dates and times of incident-related phone calls, emails, etc.
- Dates and times of incident-related event discoveries or occurrences
- Time spent on incident-related tasks
- Contacted individuals or those who contacted the CSIRT member
- Affected systems, programs, or networks

While not comprehensive, the following items represent many tasks the CSIRT may perform:

- analyze data related to the incident (log files, changes made to files, physical evidence, threats, etc)
- determine the scope of the incident, including which networks, systems, or applications are affected
- determine how the incident is occurring and who or what originated the incident
- create recommendations to remediate the problem and return to normal
- take action to mitigate the effects of the incident, and protect other University assets
- coordinate with outside entities, including law enforcement, third-party vendors, and computer forensics experts

|  |   |   |                         |                 |
|--|---|---|-------------------------|-----------------|
|  <p><b>SOUTHEAST MISSOURI<br/>STATE UNIVERSITY · 1873</b></p> | <p align="center"><b>BUSINESS<br/>POLICY<br/>AND<br/>PROCEDURE<br/>MANUAL</b></p> | Date Issued:<br>09/17                                   | Revision Date:<br>12/23 | Page:<br>6 of 8 |
|  |   | Classification Code:<br>10-04                           |                         |                 |
|  |   | Section:<br>INFORMATION TECHNOLOGY                      |                         |                 |
|  |   | Subject:<br>INFORMATION SECURITY INCIDENT<br>MANAGEMENT |                         |                 |

- Collaborate with the Information Security Officer in follow-up analysis
- Implement replacement servers/systems to maintain operations during incident investigation

**INCIDENT TRACKING:**

The Information Security Officer (or designated member of the CSIRT) will open a helpdesk ticket containing information about the security violation:

1. Name of reporting Faculty/Staff Member or, if external, contact from complainant organization
2. Location of reporting Faculty/Staff Member or external contact (if known)
3. Brief description of the incident
4. If applicable, information from the complainant organization

The Information Security Officer (or designated member of the CSIRT) will log incident-related details during the course of the incident handling process such as:

1. Dates and times of incident-related communications
2. Dates and times when incident-related events were discovered or occurred
3. Amount of time spent working on incident-related tasks
4. People you have contacted or who have contacted you
5. Systems, programs, or networks that have been affected


**INCIDENT REPORTING:**

Upon incident conclusion, the Information Security Officer or a designated CSIRT member will finalize and close all open help desk tickets related to the incident. They will also finalize the related incident tracking logs and store them appropriately.

If the incident's severity requires or if an appropriate administrator, such as the Assistant Vice President for IT, requests it, the Information Security Officer or a designated CSIRT member will create a post-incident report containing at least the following details:

- A description of the incident
- A summary of lessons learned
- Any suggested changes to existing procedures
- Recommendations to protect against future attacks, if identified during the incident


The Information Security Officer or the Assistant Vice President for IT will decide on the dissemination of any logs and reports. The executive team must determine any exceptions, but the incident logs and reports should generally be considered confidential and not for public release.

|  |   |   |                |        |
|--|---|---|----------------|--------|
| <br><b>SOUTHEAST MISSOURI</b><br><b>STATE UNIVERSITY · 1873</b> | <b>BUSINESS</b><br><b>POLICY</b><br><b>AND</b><br><b>PROCEDURE</b><br><b>MANUAL</b> | Date Issued:                                | Revision Date: | Page:  |
|  |   | 09/17                                       | 12/23          | 7 of 8 |
|  |   | Classification Code:                        |                |        |
|  |   | Section:                                    |                |        |
|  |   | INFORMATION TECHNOLOGY                      |                |        |
|  |   | Subject:                                    |                |        |
|  |   | INFORMATION SECURITY INCIDENT<br>MANAGEMENT |                |        |

## Appendix A: Example Incidents

The examples listed are not meant to be exhaustive.

- Confidential data exposure
  - Social Security Numbers with or without names
  - Credit Card information
  - Identity theft
- Criminal activity/investigation
  - Litigation holds request (aka e-Discovery)
  - Online theft, fraud
  - Threatening communication
  - Child pornography
- Denial of Service
  - Single or distributed (DoS or DDoS)
  - Inbound or outbound
- Malicious code activity
  - Worm, virus, Trojan
  - Botnet
  - Keylogger
  - Rootkit
- Reconnaissance activity
  - Port scanning
  - Other vulnerability scanning
- Rogue server or service
  - Rogue file/FTP server for music, movies, pirated software, etc.
  - Phishing scam web server
  - Botnet controller
- Spam source
  - Spam relay
  - Spam host
- Spear Phishing
  - Scam e-mail targeting a relatively large number of university e-mail addresses
- Unauthorized access
  - Abuse of access privileges
  - Unauthorized access to data
  - Unauthorized login attempts
  - Brute force password cracking attempts
  - Stolen password(s)
- Web defacement
  - Defacement of web site

|  |  |   |                         |                               |
|--|--|---|-------------------------|-------------------------------|
|  <p><b>SOUTHEAST MISSOURI<br/>STATE UNIVERSITY · 1873</b></p> | <p><b>BUSINESS<br/>POLICY<br/>AND<br/>PROCEDURE<br/>MANUAL</b></p> | Date Issued:<br>09/17                                   | Revision Date:<br>12/23 | Page:<br>8 of 8               |
|  |  |   |                         | Classification Code:<br>10-04 |
|  |  | Section:<br>INFORMATION TECHNOLOGY                      |                         |                               |
|  |  | Subject:<br>INFORMATION SECURITY INCIDENT<br>MANAGEMENT |                         |                               |

- Redirected web site
- No Incident
  - When the investigation of suspicious activity finds no evidence of a security incident