SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 09/17	Revision Date:	Page: 1 of 2
				Classification Code: 10-04
		Section: INFORMATION TECHNOLOGY		
		Subject: INFORMATION SECURITY INCIDENT MANAGEMENT		

GENERAL STATEMENT OF POLICY

An information security incident is an event that jeopardizes or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

The Computer Incident Response Team (CIRT) of Southeast Missouri State University is led by the University's Information Security Officer (ISO) and shall remain prepared to handle information security incidents until resolution.

1. Suspected or confirmed information security incidents must be reported to the University's ISO, or, in the ISO's absence, the Assistant Vice President for Information Technology (AVP for IT).

2. In the event of a malicious access to the university information resources that results in no compromise of restricted or confidential information, the ISO shall handle the incident by containing the intrusion.

3. In the event of a malicious access to the university information resources that results in no compromise of restricted or confidential, the ISO shall notify the system owner and custodian of the information for remedial action.

4. In the event of a malicious access to the university information resources, the ISO shall start a formal investigation and documentation process for that event.

5. If a public notification of the security incident is warranted, the CIRT shall consult with the appropriate University hierarchy to develop the response.

6. Any incident response to contain unauthorized access of university information resources shall be documented.

7. Any incident response to contain unauthorized access of university information resources shall be used to enhance processes, methods, and capabilities for future use.

8. Any intentional violation of university information resources by an authorized user of the resources shall result in disciplinary action against the user.

9. Any intentional incidence of failure to report violations of university information resources by a user of such resources shall result in disciplinary action against the user.

10. Periodically test incident response capabilities.

The Vice President for Finance and Administration shall be responsible for issuing and maintaining operating procedures to implement this policy.