Auburn University at Montgomery
Policies and Procedures

Title: Information Security Incicent Reporting Policy

Responsible Office: Office of Technology

I. PURPOSE

This policy informs the Auburn University at Montgomery (AUM) campus community of their responsibilities regarding how information security incidents must be reported to the proper departments to allow AUM to take appropriate actions.

II. POLICY

Information – whether in printed, verbal, or electronic form – and information systems have become critical parts of the infrastructure supporting AUM. This increased dependence has occurred against a backdrop of increasing uses of information for business purposes, technological complexity, security and privacy threats, legal mandates, and ethical expectations leading to more significant operational, reputational, and financial consequences of service interruptions and unauthorized information exposures or modifications.

In spite of the most vigilant efforts to minimize them, incidents will occur that jeopardize the security and privacy of information and information systems. The University's process of preparing for, preventing, detecting, responding to, and tracking these events has a significant impact on reducing their frequency and severity.

Legal and contractual mandates increasingly require expeditious reporting of certain breaches to regulatory or governmental authorities, **in some cases as soon as 24 hours after discovery**, and/or to the individuals affected.

This policy is intended to protect AUM from the effects of compromised data or information that can lead to severe financial losses and damage to the University's reputation, which adversely affects students, employees, and partners in business, industry, government and researchers.

An information security incident may involve any or all of the following:

- Unauthorized computer access
- Loss or compromise of information confidentiality, integrity, or availability
- Exposure of confidential information
- Denial of service condition
- Misuse of services, systems, or information
- Physical or logical damage to systems
- An attempt of an unauthorized device to connect to the University's secure networks
- Use of AUM computing resources in the commission of fraudulent activities
- Violation of other campus information security policies and standards

Examples include lost or stolen computers, installation of a malicious application (e.g., a virus or ransomware), unauthorized system or network activity, unauthorized wireless access points, a compromised account, or the compromise or exposure of confidential data.

III. EFFECTIVE DATE

August 1, 2018

IV. APPLICABILITY

This policy applies to all persons with access to University information resources.

V. RESPONSIBILITY

Policy Responsible Office: Office of Technology
Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

An **information security incident** is an event that compromises the confidentiality, integrity, or availability of Auburn University at Montgomery information resources.

A **denial of service** attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources.

VII. PROCEDURES

The procedures below describe the proper response in suspected information security (IS) incidents. There are two exceptions when the first step should, instead, be to contact AUM Campus Police. Threats to persons or property, and instances of child pornography, should be reported to the AUM Campus Police at (334) 244-3424. **In case of emergency, call 911.**

All suspected information security (IS) incidents must be reported immediately upon discovery. The following courses of action must be taken in the event of discovering an information security incident:

1. Notify the Information Technology Services (ITS) department.

2. Notify the Information Security Group of any suspected IS incident by sending an email to infosec@aum.edu or by calling 334-328-9652. Include detailed information if the incident involves:

   - Inadvertent release, exposure, or compromise of confidential data
   - The loss or compromise of portable computing devices or removable media containing sensitive data
   - The discovery of unauthorized access to sensitive data on a computer or data storage device
   - The use of AUM computing resources in the commission of fraudulent activities.

3. The Information Security Group will inform the CIO and further investigate the suspected IS incident. Upon initial investigation, the CIO or Information Security Group will contact the Auburn University Chief Information Security Officer (CISO) who may activate the Information Security Incident Response Plan.

4. If the suspected incident involves any of the following, the Information Security Group will work with the individual to further report:

   - Credit or debit card account information and notify the Auburn University Office of Cash Management, (334) 844-8190.
   - Protected Heath Information (PHI), in electronic or paper form, and notify the Auburn University HIPAA Officer at (334) 844-4333 or the Risk Management Office at (334) 844-4533.
   - Fraudulent activity committed using AUM computing resources and notify the Auburn University Department of Internal Auditing at (334) 844-4389).

5. When a subpoena or court order is issued pursuant to any investigation related to information technology the AU Office of General Counsel must be notified. The AU Office of General Counsel will direct the actions to be taken.

6. AUM Campus Police or the AU Office of the General Counsel will serve as liaison with all external law enforcement agencies (FBI, other federal, state, local) for all IT security investigations.

7. While the reporting requirement above are mandatory, the University encourages stakeholders to report other concerns or suspected violations to their supervisor or other campus entities as appropriate.

VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy will be considered a Group I infraction under the University Personnel Manual and is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

NONE

X. INTERPRETATION

The Chancellor has the authority to interpret this policy.

APPROVAL TO PROCEED: ____________ **DATE:** 8/10/18

APPENDICES

NONE