Information Security Incident Reporting Policy

I. POLICY STATEMENT

Information security incidents must be reported to the proper departments to allow Auburn University to take appropriate action.

II. POLICY PRINCIPLES

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

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

- Violation of campus information security policies and standards
- 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
- Unauthorized devices attempting to connect to Auburn University secure networks
- Use of AU computing resources in the commission of fraudulent activities.

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

III. EFFECTIVE DATE

January 11, 2017
Revised: September 10, 2018

IV. APPLICABILITY

All persons with access to university information resources.

V. POLICY MANAGEMENT

Responsible Office: Office of the Chief Information Officer
Responsible Executive: Chief Information Officer
Responsible Officer: University Chief Information Security Officer

VI. DEFINITIONS

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

VII. POLICY PROCEDURES

Threats to persons or property, and instances of child pornography, should be reported to the AU Department of Campus Safety and Security at (334) 844-5010 and/or autat@auburn.edu.

Information Security Incidents:

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

- Notify your departmental IT Provider.
- Notify the Information Security Group of any suspected IS incident by calling (334) 844-0888 and/or sending email to abuse@auburn.edu. Include particular 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, or the discovery of unauthorized access to sensitive data on a computer or data storage device.
    - The use of AU computing resources in the commission of fraudulent activities.
    - Systems used to process or store Controlled Unclassified Information (CUI).

- 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, also notify the Office of Cash Management, (334) 844-8190.

    - Protected Health Information (PHI), in electronic or paper form, also notify Auburn University HIPAA Officer at (334) 844-4333 or the Risk Management Office at (334) 844-4533.

    - Fraudulent activity committed using AU computing resources may also notify the Department of Internal Auditing at (334-844-4389).

    - Controlled Unclassified Information (CUI) related incident (systems and/or data), also notify the Research Security Compliance Office (334-844-5962). For Department of Defense (DoD) data, the loss or potential loss to Government information must be reported within 72 hours.

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

- The AU Department of Campus Safety and Security or the 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.

- The University encourages stakeholders to report other concerns or suspected violations to their supervisor or other campus entities as appropriate. http://www.auburn.edu/administration/oacp/compliancecontacts.php

VIII. SANCTIONS

Deliberate violation of this policy will be considered a Group I infraction under the Auburn

University Personnel Policies and Procedures Manual and is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

None.

X. INTERPRETATION

The Auburn University Chief Information Officer has the authority to interpret this policy.