THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

IT INCIDENT REPORTING AND BREACH NOTIFICATION

Number 06.01.07

Division Administration - Office of Information Technology (OIT)

Date August 1, 2015; Reviewed/Revised August 31, 2018; Reviewed/Revised April 23, 2025

Purpose The purpose of this policy is to clearly state the processes for documenting information technology (IT) incident reporting and for notification of breaches at The University of Alabama in Huntsville ("UAH" or "University").

Policy The University continually handles data that is classified in accordance with the Protection of Data Policy. Prompt and consistent reporting of electronic security incidents is important for the protection and preservation of information technology resources and institutional data and information.

This policy establishes the requirements and frameworks for a process of documenting and responding to incidents and breaches. This policy applies to all IT usage by faculty, staff, students, researchers, or other users of UAH-owned IT resources.

Procedure

1.0 Reporting

All individuals at the University are responsible for reporting known or potential breaches of confidentiality, integrity, or availability of UAH data or information systems (individually, an "incident") promptly and accurately.

If a breach of confidentiality, integrity, or availability of UAH data or information systems is suspected or confirmed, immediately report to the university IT Security Incident Response Team (IT-SIRT) at it-sirt@uah.edu or (256) 824-3333. Examples of reportable items include but are not limited to the following:

(a) Suspected or actual incidents of loss, inappropriate disclosure, or inappropriate exposure of any data that is not classified as Public as outlined in the Protection of Data policy, such as:
(i) Unauthorized personnel with access to UAH data. Lost or stolen mobile devices or media such as laptops, tablets, smart phones, USB drives, and flash drives which contain UAH data.
(ii) Viewing or downloading of data without a demonstrated need to know.

(b) Attempts to compromise IT resources, data, or information systems, such as:
   (i) Successful or unsuccessful login attempts, probes, or scans.
   (ii) Repeated attempts by unauthorized individuals to enter secured areas or access UAH data.
   (iii) Responding to a phishing email and providing your UAH credentials to any other party.
   (iv) Denial of Service attacks that disrupt or prevent access to UAH services or systems.

(c) Suspected or actual weaknesses in the safeguards protecting data or information systems, such as:
   (i) Ability to access data without proper authorization.
   (ii) Weak physical safeguards such as locks and access controls.
   (iii) Lack of secure transfer methods.

In cases where a unit has an information security, privacy, or compliance officer, incidents should be reported to both the university IT-SIRT and the unit officer.

2.0 Financing Incident Response

Based on review with the UAH President, the unit(s) experiencing the incident may be responsible for all costs related to investigations, cleanup, and recovery activities resulting from the compromise, response, and recovery.

3.0 Incident Response

Upon receiving a report of an incident, the university IT-SIRT team will follow the Incident Reporting and Breach Notification Plan in the OIT Knowledge Base. Specific details will be specified in that plan and in subsequent playbooks. In general, the IT-SIRT should take action in four phases:

1. **Detection and Analysis** – Analyze, validate, and prioritize the incident and identify any appropriate playbooks to follow.
2. **Containment** – Limit the potential and future damage that can be caused by the incident, including actions such as shutting down a system, isolating it from the network, etc.
3. **Eradication & Recovery** – Eliminate the components of the incident such as deleting malicious code and disabling breached user accounts and restoring systems and accounts to normal and expected operation.
4. **Post-Incident Activity** – Document the incident and lessons learned and any appropriate reviews related to investigations or cleanup.

Evidence should be collected (such as log files archived) and systems collected where appropriate and responders advised by OIT management. The UAH Chief Information Officer (CIO), Chief Information Security Officer (CISO) and/or OIT Directors will determine when escalation is required and to whom.

4.0 Compliance with Policy

OIT personnel may take immediate action to abate identified issues impacting network or system operations.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, the Staff Handbook, or University policy, will be referred to appropriate university authorities.

Review The UAH CIO or their designee is responsible for the review of this policy every three years (or whenever circumstances require).