THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

IT INCIDENT REPORTING AND BREACH NOTIFICATION

Number 06.01.07

Division Finance and Administration - Office of Information Technology (OIT)

Date June 2018

Purpose The purpose of this policy is to clearly state the processes for documenting IT incident reporting and for notification of breaches.

Policy The University of Alabama in Huntsville (UAH) continually handles data that is designated as public, private, or confidential or sensitive. Prompt and consistent reporting of electronic security incidents protects and preserves information technologies resources and institutional data and information, and aids the university's compliance with applicable laws.

This policy establishes the process for documenting incident reporting and the steps and requirements for notification of breaches. This policy applies to all IT usage by faculty, staff, students, researchers, or other users of UAH owned IT resources.

All usage of the term data in this policy is in reference to electronic data.

Procedure

1.0 Reporting

Immediately report to the university IT Security Incident Response Team (IT-SIRT) at it-sirt@uah.edu or (256) 824-3333 any of the following:

1. Suspected or actual incidents of loss, inappropriate disclosure, or inappropriate exposure of confidential or sensitive or private data, as outlined in the "Protection of Data" policy, such as:
    i. Critical data such as, but not limited to, Personally Identifiable Information (PII), credit card numbers, Social Security numbers, driver's license numbers, or bank account numbers.

ii. Lost or stolen mobile devices or media such as laptops, tablets, smart phones, USB drives, and flash drives.
iii. Viewing of data without a demonstrated need to know (e.g., snooping).

2. Abnormal systematic unsuccessful attempts to compromise IT resources or data or information systems, such as:
    i. Abnormal unsuccessful login attempts, probes, or scans.
    ii. Repeated attempts by unauthorized individuals to enter secured areas.
3. 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 transport 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, the university IT-SIRT team will:

1. Ensure appropriate information and evidence is collected and logged.
2. Immediately assess initial actual or potential loss, corruption, inappropriate disclosure, inappropriate exposure, or breach of data.
3. Immediately advise and assist in containing and limiting the loss, corruption, inappropriate disclosure, inappropriate exposure, or breach.
4. Invoke incident response procedures commensurate with the situation.
5. As appropriate, assemble an IT Incident Team, with concurrence of the UAH President, to advise and assist in ongoing investigation and decision-making. The nature of the incident and the type(s) of data involved will determine the composition of the Incident Team, and it typically will include the following, or their designee:

    - Chief Information Officer (CIO)

- Chief Information Security Officer (CISO)
- Office of Counsel
- Provost
- Vice President of Finance and Administration
- Vice President or Dean for the university unit(s) involved
- Office of Risk Management

6. As appropriate, ensure the CIO and/or the CISO is informed of the initial situation and kept updated throughout the investigation.
7. As appropriate, ensure that executive administration is informed of the initial situation and kept updated throughout the investigation.
8. As appropriate, contact law enforcement for assistance.
9. As appropriate, consult with and/or assign a security engineer to perform forensics or other specialized technical investigation.
10. As appropriate, provide technical advice to the unit technician involved in the incident and ensure that legal, compliance, data owner, media, and executive administration advice is made available to unit administration in a timely manner.
11. Initiate steps to warn other university units or technicians if the situation has the potential to affect other university data or information systems.
12. Confirm actual or probable events from investigatory information and facilitate decision-making by the IT Incident Team.
13. In coordination with the IT Incident Team members and following internal procedures, determine if notification to individuals and/or regulatory or governmental authorities is required and/or desired, and invoke breach notification procedures commensurate with the situation.
14. Ensure appropriate university approvals are obtained prior to any notifications to individuals or regulatory and government officials.
15. Document decisions and any notifications made to individuals or regulatory and government officials.
16. Schedule a debriefing meeting with the unit and IT Incident Team after the response, to ensure appropriate corrective action in the affected unit is taken, to identify any actions that could be taken to reduce the likelihood of a future similar incident, and to improve continuously the response processes.
17. If the incident involves student data, add a notice to the involved student(s)' academic record to document the disclosure without prior consent as required by FERPA.

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 IT Investment Advisory Council is responsible for the review of this policy every five years (or whenever circumstances require).