

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE
IT INCIDENT REPORTING AND BREACH NOTIFICATION

-INTERIM-

Number 02.01.41

Division Office of Information Technology (OIT)

Date August 2015

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. 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 faculty, staff, students, researchers, or other users of IT resources that connect to UAH networks, and/or store or transmit UAH data, regardless of ownership of the device or system, including personally owned devices or systems.

Procedure

1.0 Reporting

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

- Suspected or actual incidents of loss, inappropriate disclosure, or inappropriate exposure of confidential or private data, as outlined in the "Protection of Data" policy, used in the pursuit of the university's mission. The information can be in any form – printed, verbal, or electronic – including but not limited to those incidents involving the following information, systems, or processes:

- Critical information such as, but not limited to, Personally Identifiable Information (PII), credit card numbers, Social Security numbers, driver's license numbers, or bank account numbers.
- Lost or stolen mobile devices or media such as laptops, tablets, smart phones, USB drives, and flash drives.
- Viewing of information without a demonstrated need to know (e.g., snooping).
- Abnormal systematic unsuccessful attempts to compromise IT resources or data – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission, such as:
 - Abnormal unsuccessful login attempts, probes, or scans.
 - Repeated attempts by unauthorized individuals to enter secured areas.
- Suspected or actual weaknesses in the safeguards protecting information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission, such as:
 - Weak authentication processes.
 - Ability to access information without proper authorization.
 - Weak physical safeguards such as locks and access controls.
 - 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

The unit(s) experiencing the incident is/are responsible for all monetary, staff, and other 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 information.
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 to advise and assist in ongoing investigation and decision-making. The nature of the incident

and the type(s) of information 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
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 information 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

Failure to abide by this policy may result in the loss or suspension of IT privileges, claims for reimbursement of damages, disciplinary action, and/or referral to appropriate state/federal law enforcement authorities.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, or the Staff Handbook will be referred to appropriate authorities. OIT personnel may take immediate action as needed to abate ongoing interference with system or network operations or to ensure integrity of university systems or data.

Review The UAH Cybersecurity and Policy Advisory Council is responsible for the review of this policy every three years (or whenever circumstances require).

Approval

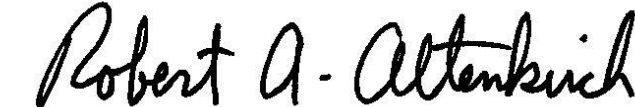


Chief University Counsel



Provost and Executive Vice President for Academic Affairs

APPROVED:



President