Incident Response

Contents

Purpose

Albany State University's (ASU) information, information systems, and infrastructure are critical resources for accomplishing the mission of the university. All ASU users have an interest in the security of these resources, and share in the responsibility for protecting them. Prompt and consistent reporting of and response to information technology (IT) incidents protects and preserves the confidentiality, integrity, availability, and privacy of information, information systems and associated infrastructure resources which helps the university to comply with applicable law.

Scope

This policy applies to all Albany State University faculty, staff, students, and affiliates (vendors, contractors, consultants, etc.). This policy also applies to information in any tangible form whether it is written, filmed, typed, recorded electronically or printed, and to all ASU information and technical resources.

Policy

The Albany State University IT Security Incident Response Policy and subordinate procedures define standard methods for identifying, tracking and responding to network and computer-based IT Security Incidents.

The ASU Chief Information Security Officer (CISO) is responsible for ensuring that incidents are reported promptly upon discovery, that incidents are investigated, and escalated to the University System Georgia Board of Regents (USGBOR) and local, state, and federal law enforcement agencies where applicable.

All IT system users are responsible for promptly reporting any suspected incidents to the Chief Information Security Officer through the ASU Help Desk. A preliminary investigation into all suspected incidents will be conducted to determine if the event is an actual incident requiring a coordinated incident response. The affected end user, academic and business owners and their

associated Vice President and the ITS VP/CIO will be notified immediately upon discovery of an incident.

Any computing device that is involved in an incident is subject to being confiscated by ITS staff as a precautionary measure to protect the ASU networking infrastructure. The device will returned immediately once it has been tested and deemed safe to operate.

- **Identification of Incidents**
  Any faculty, staff, student of ASU or outside organization may refer an activity or concern to Information Technology Services. Once identified, ITS will use standard procedures to log and track incidents, work with others as appropriate, take steps to investigate, escalate, remediate, and refer to others or otherwise address as outlined in the remainder of this policy.
- **Establishment of an IT Security Incident Response Team** The CISO is responsible for Incident interdiction and remediation of information and information systems and associated resources affected by these incidents. The CISO will consult administrators, Information Technology Services, Academic and Administrative Systems departments, USGBOR CISO, ASU Police Chief, State and Federal agencies or other units, as warranted. The CISO establishment of an IT Security Incident Response Team in response to specific incidents will be based on the level and severity of the incident.
- **Risk Assessment Classification Matrix**
  The CISO will establish an internal risk assessment classification matrix. The matrix will be applied to focus the response to each Incident, and to establish the appropriate team participants to respond. This classification matrix will correspond to an "escalation" of contacts across the university, and will indicate which authorities at ASU to involve and which procedure would be applicable for each class of incident.
- **Documentation and Communication of Incidents**
  The Information Technology Services will ensure that Incidents are appropriately logged and archived. Documentation of such Incidents will be catalogued and cross-reference other event databases within the university. The Help Desk, CISO and IT Security Incident Response Team representatives will be responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident. The CISO will maintain subordinate procedures for the response and investigation of each Incident and securing the custody of any evidence obtained in conjunction with the ASU Chief of Police in the investigation. The procedures will specify the location and method of custody for each incident, if custody of evidence is required.
- **Relationship to USGBOR, State and Federal Agencies**
  A response plan or remediation defined by this policy may be preempted as required or at ASU's discretion by the intervention of USGBOR or federal and state executive officials.
- **Incident Prevention, Detection, and Correction**
  ASU will undertake measures to prevent Incidents by monitoring and scanning for anomalies, and developing clear protective procedures for the configuration of its IT resources. Proactive measures are undertaken to detect information security related incidents by use of malware and antivirus tools, network monitoring tools, and logging and event monitoring. After an incident has been discovered or reported, ASU ITS will take aggressive action to resolve the incident as deemed appropriate by the IT Security Incident Response Team.

- **Modifications and Adjustments**
  This procedural documentation will be reviewed periodically to adjust processes, identify new risks and remediation.

Definitions

Sensitive Information
Sensitive Information is information that is not to be publicly disclosed. The disclosure, use, or destruction of Sensitive Information can have adverse effects on ASU and possibly carry significant civil, fiscal, or criminal liability. This designation is used for highly sensitive information such as open legal investigations, sealed bids, research activity, social security numbers, etc., whose access is restricted to selected, authorized employees

Academic or Business data owner
The individual who has ultimate responsibility and ownership for a particular set of data (e.g. a department head, dean, or V.P.)

Forensic Analysis
The process of making a duplicate of the computer system hard drive(s) using some form of hardware write protection, such as a hardware write blocker, to ensure no writes are made to the original drive.

Information Security Incident Response Team (ISIRT)
The role of the ASU ISIRT is to coordinate the University response to breaches of security involving confidential or private information. The responsibilities of the ISIRT include, but are not limited to:

- Notifying affected constituents of the incident
- Coordinating responses to public inquiries
- Making the decision to involve law enforcement agencies and computer forensic experts
- Discussing, reviewing, and documenting any lessons learned from incidents

IT Incident
An activity or event that results in damage to, misuse of, or loss of, an IT resource. Incidents include but are not limited to: •

- Loss of a computing device (misplaced, stolen, vandalized)
- Detection of a malicious program, such as a virus, worm, Trojan horse, keystroke logger, rootkit, remote control bot, etc.
- Detection of unauthorized users, or users with unauthorized escalated privileges.
- Detection of a critical or widespread vulnerability or misconfiguration that might lead to a compromise affecting the confidentiality, integrity, or availability of university systems or data.

IT Resource
A computing asset provided by ASU to further its mission. Examples include, but are not limited to, network bandwidth, networking equipment, workstations, computer systems, data, databases, servers, and printers.

Local Support Provider
An individual or group with principal responsibility for the installation, configuration, security, and maintenance of an IT resource. When there is no formally identified local support provider (e.g., a personally owned computer used from home to connect to the ASU network), the user is the local support provider.

Major Incident

- Involves a device or system containing private (see definition) or confidential data
- Threatens the business continuity of college, department, or university
- Affects multiple systems or servers
- Affects multiple systems or servers

Private Information
Private Information includes information that ASU is under legal or contractual obligation to protect such as FERPA, HIPAA or GLBA data. Examples would include Employee ID numbers, birth dates, location of assets, donors, gender, etc.

Security Incident Response Team (SIRT)
The ASU SIRT consists of individuals from various departments within ITS including Network Services, Server Administration, and IT Security. The SIRT reports to the VP of Information Technology Services who assigns the team to respond to an incident:

- Which requires coordination across multiple departments
- When a single department lacks the resources to respond
- When the local support provider requests assistance
- When the ISIRT determines involvement is necessary

Security Threat Profile
A threat profile is a straightforward and repeatable way to identify, organize, document and prioritize threats to your organization. A threat profile provides a way to map threats with the source of the event or events that are evidence of specific behavior.

Accountability

Failure to abide by the requirements of this policy and / or any procedures that are developed to implement this policy may result in disciplinary action. Some violations may constitute criminal offenses under local, state, and federal laws. Albany State University will carry out its responsibility to report such violations to the appropriate authorities.

Contacts

- Albany State University Chief Information Officer
- Albany State University Chief Information Security Officer

References

- ASU ITS Security Website: https://www.asurams.edu/Technology/technologyhome/information-security/
- USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5
- SANS Institute: http://www.sans.org

Version History

Date	Version	Description
July 8, 2013	2.3	
August 11, 2015	2.4	Removed names from the positions in Contacts section