Responsible Executive: Chief Information Officer
Responsible Office: Information Security Services
Effective Date: October 18, 2018
Last Revised: August 19, 2022

INFORMATION TECHNOLOGY INCIDENT MANAGEMENT

POLICY SUMMARY

As a means of organizing and directing observable threats to its Information Technology (IT Resources and systems, this policy establishes roles, responsibilities, and procedures for reporting and managing IT Incidents. Written directions for responding to IT Incidents increase Northern Arizona to mitigate threats, minimize risk of loss or destruction of University Information, and help to restore services more quickly when events do occur. All University Community Members that use University IT Resources are advised to immediately report any IT-related concern to Information Technology Services.

REASON FOR THIS POLICY

Responding to IT-related threats or challenges is essential to maintaining the confidentiality, integrity, and availability of the T Resources.

ENTITIES AFFECTED BY THIS POLICY

All units that interact with University Information or University IT Resources
External entities granted access to University Information
Information Technology Services

WHO SHOULD KNOW THIS POLICY

All University Community Members that use University IT Resources
Chief Information Officer
External agents granted access to University Information
Information Technology Services Leadership Team

DEFINITIONS

_____: any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the University,

IT Incident: an observable or recognizable occurrence that threatens or causes adverse consequences for the confidentiality, integrity, or availability of the University IT Resources.

Major IT Incident: an IT Incident of significant scope or scale that affects large numbers of University IT Resources and University Community Members, or that results in extended downtime of IT services.

Sensitive Information: all information that should remain private or confidential as designated by the University or as required by law, including,

1. Identification and Classification the reported incident shall be analyzed and details confirmed to determine if a reported incident does in fact constitute an IT Incident or a Major IT Incident. This classification will assist with determining the proper response procedure and the selection of appropriate personnel for managing the response.

2. Containment and Eradication the systems affected or implicated shall be isolated and/or further monitored to prevent wider or additional negative impact. Compromised systems will be immediately isolated from the network. Compromised user accounts that pose a threat will be blocked or isolated from the network.

3. Recovery and Restoration once blocked systems are secured and threats eradicated, continued monitoring, logging, and auditing of activity will be implemented when blocked systems are re-introduced into the network. All significant findings will be documented, including analysis and remediation steps.

4. Response Team Review and Lessons Learned post-incident activities will include debriefing meetings, review of incident handling procedures, and lessons learned discussions. Edits and republishing of procedures will be based on the debriefing meetings.

E. Training and Testing

ITS leadership shall ensure appropriate training of ITS personnel in effective IT Incident mitigation and response, consistent with the requirements of this policy. Testing of IT Incident response capabilities and proficiencies shall occur no less than annually using checklists, tabletop exercise, simulations, meetings, or comprehensive scenario-based exercises. Training and testing shall include lessons learned from previous IT Incident management activities. IT Incident-related training and testing shall focus on improving the ability to respond effectively to a real event while continually identifying areas for growth and improvement. In the event actual incidents have occurred during the year, they may serve as one kind of training and testing, provided the protocols were followed and a full assessment and lessons learned phase takes place.

Information Security Awareness training is required of all faculty, staff, and other Authorized Users of University Information or IT Resources.

RESPONSIBILITIES

Chief Information Officer: ensure that appropriate and auditable IT Incident management procedures are in place; has ultimate responsibility for the IT Incident management program.

Information Technology Services: maintain management procedures for IT Incidents and Major IT Incidents; design and participate in IT Incident training and testing exercises; respond to and manage IT Incident reports and responses.

University Community Members: promote the implementation of this policy within their respective areas of responsibility or jurisdiction and comply with the *Appropriate Use of Information Technology Resources* policy.

PROCEDURES

Information Technology Incident Response Procedure

RELATED INFORMATION

Forms or Tools

None.

Cross-References

- Appropriate Use of Information Technology
- Enterprise System Change Management Standard
- Information Security
- Information Security Awareness Training

Sources