INFORMATION TECHNOLOGY INCIDENT MANAGEMENT

POLICY SUMMARY

As a means of organizing and directing the University’s response to 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 University’s ability 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 integrity and availability of the University’s IT 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

Information Technology ("IT") Resource: 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, used to conduct University business, or connected to the University's IT networking or communication systems regardless of ownership, location, or access method. These resources are referred to herein as “IT Resources.”

IT Incident: an observable or recognizable occurrence that threatens or causes adverse consequences for the integrity or availability of the University's 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 but not limited to, educational and student conduct records, social security numbers, credit card or banking information, regulated research data, and health care provider records. Sensitive Information includes, but is not limited to, Level 3 – Sensitive Data and Level 4 – Highly Sensitive Data as defined in the University’s Data Handling and Classification policy.
University Information: all written or verbal data or information that the University or its employees, students, or designated affiliates or agents collect, possess, or have access to regardless of the medium on which it is stored or its format.

University Community Member: all University faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, agents, and volunteers wherever located.

**POLICY**

A. Applicability

This policy applies to all University Community Members and other persons who access or use University Information, including third-party individuals or entities. Additionally, this policy applies to all University IT Resources, all applications or data contained on these devices or systems, and all other devices, including privately owned devices, that connect to the University's information networks or data storage systems.

B. Examples

A partial list of potential IT Incidents (or Major IT Incidents depending on scale) includes:

- Unauthorized access of University IT Resources, systems, or University Information
- Violation of the Appropriate Use of IT Resources policy
- Violation of the Information Security policy
- Unauthorized changes to enterprise production systems
- Loss, theft, or damage to University IT Resources
- Unexpected disruption of or IT system unavailability
- Compromised user accounts
- Unauthorized disclosure of Sensitive Information
- Malicious attacks propagated by computer viruses, malware, or phishing schemes

C. Reporting

University Community Members who use the University's IT Resources are strongly encouraged to immediately report suspected IT Incidents or Major IT Incidents to Information Technology Services. Information Technology Services ("ITS") personnel shall utilize the University incident tracking system, ServiceNow, for all reporting and incident documentation. Reports of actual or suspected IT Incidents or Major IT Incidents should be submitted as appropriate to the following offices:

- **Students: Student Technology Center**
  - 928-523-9294
  - 888-520-7215
  - Ask-STC@nau.edu
  - https://nau.edu/stc/help
  - Cline Library, building 28 for in-person

- **Faculty & Staff: ITS Solution Center**
  - 928-523-1511
  - 888-520-7215
  - http://nau.service-now.com

D. IT Incident Management

The Chief Information Officer, in collaboration with the Information Technology Services (ITS) Leadership team, shall establish and revise as necessary or appropriate the University's IT Incident and Major IT Incident management protocols, to be maintained within the ITS system of record, that will provide for the following:
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.

**F. Incident Response**

At the discretion of the Chief Information Officer, IT Incident or Major IT Incident response actions may include
the removal of devices or systems from the University’s networks or information systems until recovery or
compliance with applicable requirements or standards is achieved.

**RESPONSIBILITIES**

- **Chief Information Officer**: ensures that appropriate and auditable information technology incident management
  procedures are in place, and has ultimate responsibility for the IT Incident management program.

- **Information Technology Services**: maintains management procedures for IT Incidents and Major IT Incidents,
  and designs and participates in IT Incident training and testing exercises; responds to and manages 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

- Arizona Board of Regents Policy 9-201
- Arizona Board of Regents Policy 9-202

APPENDIX

None.