INFORMATION TECHNOLOGY SECURITY INCIDENT RESPONSE PROCEDURE

OVERVIEW

This document provides the University's guide for responding to the receipt of an IT Security Incident or Major IT Security Incident report. The goal of this procedure is to limit and contain the impacts, identify and reduce risk, and restore services quickly to systems impacted by a security incident. It outlines the steps University Community Members can follow for reporting IT threats or security concerns, the essential steps for how the Information Technology Services division will identify or classify an incident, roles and responsibilities for incident response teams, and the workflow that incident response teams should follow during the incident lifecycle.

According to the National Institute of Standards and Technology ("NIST") Computer Incident Handling Guide, an incident is defined as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." Some examples include, but are not limited to, the following:

- Exposure or compromise of sensitive information (compromised integrity)
- Loss or breach of information confidentiality and/or availability
- Health and Safety Investigations
- Forensics and other types of subpoena requests
- Violation of campus security policy
- Violation of computer or network acceptable use policy
- Misuse of services, systems, or information
- Physical damage to systems
- Theft/loss of computers
- Denial of service or large-scale attacks and intrusions to systems or groups of systems
- Malicious attacks such as rootkit, malware, ransomware, exploitation of systems, virus outbreaks
- Unauthorized computer access and/or stolen credentials
- Unexpected or unapproved modifications to programs

SCOPE

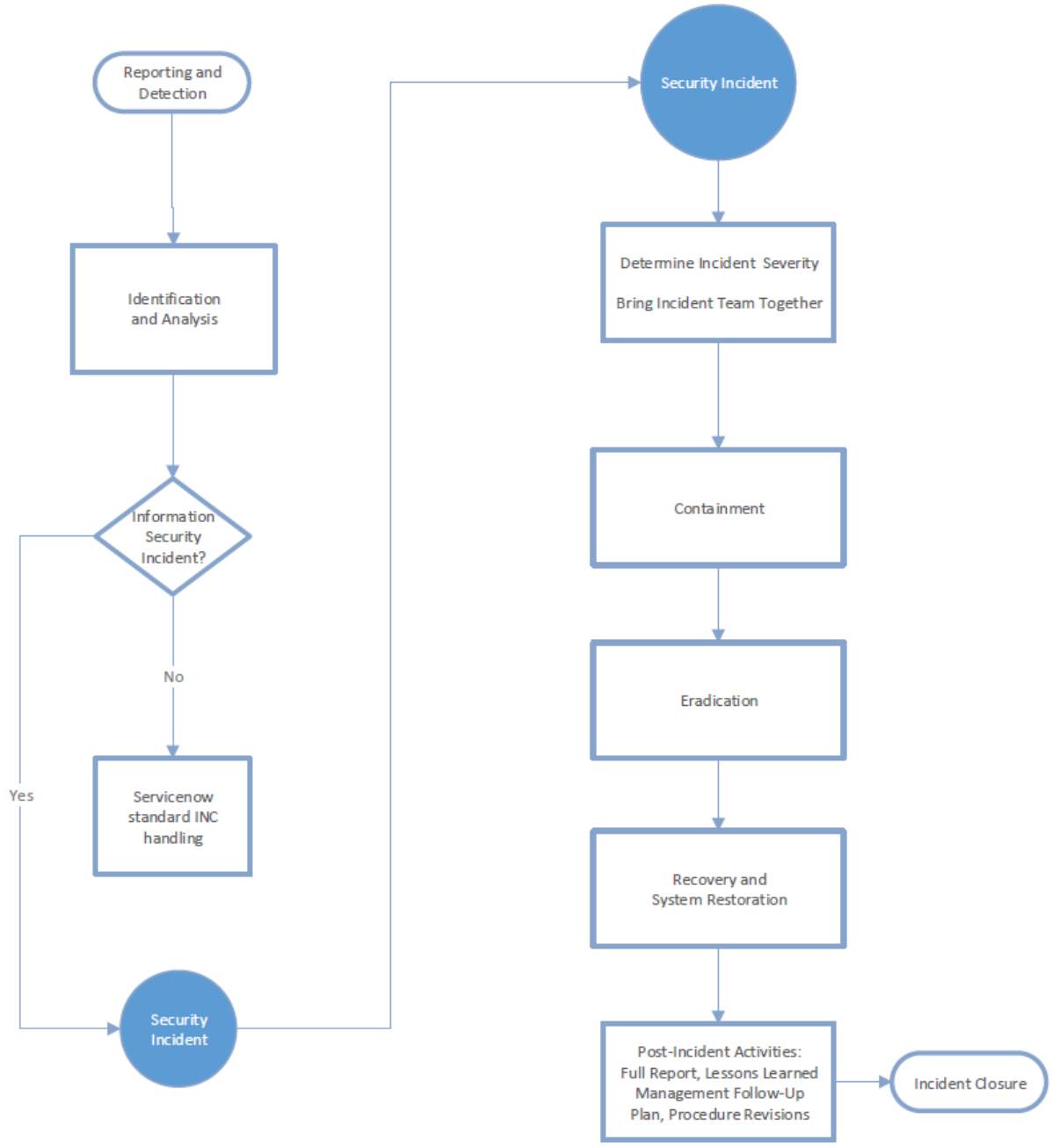
This guide applies to all NAU-owned systems and any devices that store or transmit NAU data.

This document provides guidance during an information security incident, regardless of the size and represents typical steps taken by the Information Technology Services ("ITS") division. The identification and classification steps in the workflow are where decisions are made. Decisions will be based on the level of risk assessed. If an information security incident response team is deemed necessary, the roles, responsibilities, and steps defined in this document will be followed as they detail an approved and consistent process.

The steps identified in this document may be determined inappropriate in certain circumstances. The Chief Information Officer ("CIO") and/or the Chief Information Security Officer ("CISO")/Director of Information Security Services ("ISS") may decide to follow different steps in these cases. All such decisions will be documented and reviewed during lessons learned and response wrap-up.

WORKFLOW

The diagram below provides the high-level security incident response cycle. Stages of the cycle are detailed in a section following the diagram.



A. **Reporting and Detection**.
   - Suspected Security Events, Incidents, and Breaches **must be reported immediately** to ISS Security events may be detected by ISS and handled internally

B. **Identification and Analysis**. The reported or detected Security Event is analyzed and details confirmed to determine if it is an information Security Incident.

- Analyze the details of report in order to validate that an information Security Incident has occurred
- If it is determined that an information Security Incident has NOT occurred, a standard ServiceNow ticket should be created
- Identify the affected systems, devices, data type(s) involved
- Determine if the information Security Incident, from here on referenced as Incident, is still/currently in progress or not
- Evaluate the potential effect of the Incident
- Classify and prioritize the incident, such as Critical, High, Medium, Low risk or threat. (See Incident Classification Table in the Appendix)

C. Containment

- Build and convene the Incident Response Team based on initial incident classification.
  - Assign Incident Leader (see ITS Major Incident Handbook as reference if needed)
    - ✓ For highly critical incidents – CISO or the CIO
    - ✓ For all others – Manager, IT Security Administration or IT Security Analyst
  - Incident Response Team may be different based on severity level, priority of incident, type of incident, and/or systems and services affected
    - ✓ A list of potential response team members can be found in the appendix with typical roles, responsibilities, and contact information
    - ✓ Other possible team members, such as distributed teams or pertinent campus offices, can be found in the appendix with typical roles, responsibilities and contact information
  - Develop an appropriate communications plan (see ITS Major Incident Handbook as reference if needed)
- Third Party Assistance: If the incident is classified and considered severe enough, third party assistance will be brought in to lead the response. Third party contact information is found in the appendix and decisions to engage will be made by the Incident Leader, CIO, or CISO in coordination with Risk Management and the Office of General Counsel.
- Internal Management: If the incident is managed internally, the forms of containment will depend on the type of incident but must be implemented in order to limit damage to university resources
  - Identify and assign appropriate investigators from the response team and/or coordinate with network administrators, system administrators, and/or departmental IT staff
  - Network containment if necessary
    - ✓ Disconnect system from network to stop malicious traffic from expanding and to disable remote access by attacker. If ransomware is suspected turn the machine off to prevent spreading encryption.
    - ✓ If available and appropriate, redirect an attacker to a sandbox in order to monitor behavior.
    - ✓ If decided that full content network dump can be performed, allow very temporary network until completed and/or reduce open ports or do port blocking to acquire data and evidence.
  - Isolate, quarantine, and obtain system if necessary for evidence gathering
    - ✓ Containment takes precedence over preservation if incident is current/active.
    - ✓ Preservation of evidence must follow chain of custody standards.
- Investigation of the incident will involve many, if not all, of the following, plus any other steps determined critical to the investigation:
  - If live system is available, perform memory dump and live evidence gathering, such as network flow dump, listings of mapped drives or attached storage, connected users
  - Perform forensics backup, disk image
  - Perform vulnerability analysis, PII search if applicable
  - Perform full system analysis and remove cause of incident if possible
- Notify all parties affected by the incident and initiate the communications plan
  - Examples of communications for Low-Medium incident levels include:
    - ✓ Owner of system, owner of data
    - ✓ Supervisor of employee
    - ✓ Other system administrators if assumed to be more widespread

D. Eradication and Recovery

- Eradication may include:
  - Deletion of all malware on a specific host
  - Identifying additionally affected hosts and removing malware
  - Disabling of breached accounts
  - Changing security credentials such as dropping level of escalated user account
  - Removing phishing email from mail inboxes
- Recovery may include some steps that result in eradication:
  - Depending on the severity level, may or may not be able restore/reintroduce system
  - Restore system from backup or build as new and apply all patches, fixes, updates
  - Perform vulnerability scans, audit the results, verify
  - Take data from investigation to understand how incident occurred and include as part of a penetration test
  - Determine/coordinate timeline for reinstatement
- Monitor system for backdoors, continuous monitoring of logs (potentially at increased verbosity for a temporary time period) and vulnerability scans, PII searches, and periodic penetration testing, if applicable.

E. Post-Incident Activities. This step involves management follow-up, incident team debriefing, and lessons learned activities at a minimum, with notifications and reports to required parties as needed.

- ServiceNow Ticketing System will be used to track incidents, unless highly confidential, in which case an out-of-band solution is available for the response team.
- Microsoft Teams will be used for real-time communications and coordination when appropriate, and notes from those conversations can be collected for incident reporting
- Debriefing Meetings
  - May be with the impacted business unit; will always be with the incident team after the recovery step. Reasons include, not limited to:
    - ✓ Lessons learned
    - ✓ What exactly happened, at what times?
    - ✓ How well did the team respond and perform steps?
    - ✓ Were there any precursors we missed that can be alerted on in the future?
  - Ensure that the best and most appropriate corrective action is taken
  - Important to identify any actions that could have been taken to expedite the response and edit the response plan
    - ✓ Also identify any tools that would aid in those actions
  - Identify any pre-incident actions or protections that could have been implemented that would have lowered the risk
- Change Management debrief
  - What actions were taken quickly during incident in regards to containment
    - ✓ Access control lists, blocking of ports/IP addresses, suspended systems or accounts
    - ✓ Should those changes be reverted? Modified? How should they be documented?
- Full incident response report
  - For record-keeping, future incident reference point
  - Be able or ready to report on:
    - ✓ The number of incidents in a specific time range, such as the past year
    - ✓ The time-per-incident, such as from initial report to closure
    - ✓ The resources required, such as staff time, as well as hardware/software
    - ✓ The estimated damage, if any, from the incident in terms of downtime, money, and hardware replacements
  - For those who should receive such reports (upper management, VP, Admin, President)

- Communications: Wrap-up of notification to all associated and relevant parties

Review & Publication

This procedure will be shared with and reviewed annually with ITS Leadership. The plan will be placed in the ITS Disaster Recovery SharePoint site and the NAU Policy Library.

Appendix

Security Incident Response Checklist - Example

DETECTION, IDENTIFICATION AND ANALYSIS		COMPLETED
1	Identify incident based on threat source and vulnerability area.	
2	Prioritize the incident based on the severity and escalation level.	
3	Identify which systems, system components, and data have been affected and forecast additional assets that may be affected.	
4	Estimate the current and potential technical effect of the incident.	
5	Report the incident to the CIO, ISS Director, and appropriate personnel. (If needed, working through Risk Manager engage with insurer or third parties)	
CONTAINMENT, ERADICATION AND RECOVERY		**COMPLETED**
6	Stop or try to contain the incident if it is still in progress.	
7	Disconnect affected systems from the network.	
8	Preserve evidence from the incident. Make copies of the drive, log files, other evidence related to the incident if possible.	
9	Clean up all effects of the incident. If a system has been compromised, rebuild it from known trusted sources.	
10	Identify and mitigate all vulnerabilities that were exploited.	
11	Remove malicious code, inappropriate materials, and other components.	
12	Recover from the incident.	
13	Return affected systems to an operationally ready state.	
14	Confirm that the affected systems are functioning normally.	
15	If necessary, implement additional monitoring for future related activity.	
POST-INCIDENT ACTIVITIES		**COMPLETED**
16	Create follow-up report (after action report).	
17	Hold a lessons-learned meeting. Review what actions were taken during the incident.	

18	Estimate damage/impact.	
20	Make changes to the policies and procedures, if necessary.	

ROLES, RESPONSIBILITIES, CONTACT INFORMATION

For use as a reference when assembling an information security incident response team - a description of typical roles and responsibilities have been included, along with up-to-date contact information.

Chief Information Officer ("CIO") / Chief Information Security Officer ("CISO")

- This position may be the Incident Leader (see below for responsibilities of that role)
- Among the responsibilities for this position:
  - Set priorities
  - Notify and provide updates as necessary to:
    - University President and Campus Leadership
    - General Counsel
    - Human Resources
    - NAU Police Department
    - NAU Risk Management
  - U.S. Department of Defense as necessary and required by DFARS 252.204-7012Ownership of the incident response team's work
  - Participate in investigation decisions
  - Define and issue compartmentalization orders for particularly sensitive issues
- Contact Information
  - CIO – Steve Burrell
    - ✓ Email Steve.Burrell@nau.edu
    - ✓ Phone 928-523-9998
    - ✓ Cell 928-525-6618
    - ✓ Alternate personal email: sburrell63@gmail.com
  - ***CISO*** – Chris Graver
    - ✓ Email Chris.Graver@nau.edu
    - ✓ Phone 928-523-5997

Incident Leader

- CISO or their designee
- Updates the CIO, IT Executive Leadership, and CISO on a regular basis during the incident.
  - Manage all resources for the incident
  - Participate in, or make, the decision that an incident is Critical
  - Communicate to Information Security Services, Network Operations, System Administrators, and other relevant IT support staff that an incident has occurred
  - Assemble an incident response team and activate the incident response plan
  - Initiate an incident tracking file for documenting the full incident lifecycle
  - Establish, with incident response team, containment procedures
  - Maintain communications between the Incident Team, CISO, and CIO
  - Participate in, or make, investigation decisions
  - Manage the incident work and task assignments
  - Convene meetings during the incident for ongoing status reports as necessary
  - Identify necessity of external support and resources for large-scale incident
  - Coordinate final meeting, reporting, documentation, incident tracking file closure
  - Send final reports to CIO and others as necessary
  - Update existing incident response plan with lessons learned, procedural changes, and update contact information

Incident Response Team

- Members and team sizes will vary depending on the type of incident and the skills needed to assist during an incident. The team will typically include IT staff from teams including Information Security,

Network Operations, Server Administrators, Database Administrators, and others deemed necessary, including potentially a third party.
    - Examples of positions that may be assigned for a particular incident:
        - ✓ Incident Leader – based on initial classification of incident
            - Large, High Impact or Priority = Incident Leader, as above
            - Small, Low to Medium Impact or Priority = Manager IT Security Administration , Jonathan Wince.
                - ➢ Email Jonathan.Wince@nau.edu
                - ➢ Phone 928-523-1005
        - ✓ Technical Lead to assist Incident Leader
            - Large, High Impact or Priority = IT Security Analyst
            - Small, Low to Medium Impact or Priority = may be selected from the area experts listed below.
        - ✓ Technical/area experts
            - Includes System Administrators, Network Operations, and other IT staff.
- Responsibilities for the team:
    - Coordinate communications and actions with the Incident Leader
    - Make recommendations to Incident Leader and other members of incident team related to response and recovery options.
    - Response
        - ✓ Assist in containment
        - ✓ Collect evidence
        - ✓ Forensics investigation
        - ✓ Remediation
    - Recovery
        - ✓ Make determination of whether affected system(s) can be restored, reinstalled
        - ✓ Make determination of lost data and ability to recover or restore
        - ✓ Re-introduce affected system(s) and sign-off/certify readiness
        - ✓ Restore to normal operations status
    - Participate in incident closure meeting, documentation tasks, final reporting
    - Contact Information
        - ✓ The nature of the incident will determine the make-up of the incident response team, therefore the On-Call List is the best source of contact information:
        - ✓ https://nau0.sharepoint.com/sites/ITSOnCall/Lists/Team/Allteams.aspx

NAU University Police
- Coordinate with external law enforcement as necessary
- Conduct interviews as necessary
- Contact Information
    - NAU Police Department – 928-523-3611

General Counsel
- Provide guidance regarding legal issues related to or arising from an incident
- Contact Information
    - NAU Office of General Counsel – 928-523-6517

Human Resources
- Advise and provide consultation to Incident Leader, CIO, CISO regarding all personnel matters involving employees
- Coordinate with General Counsel to initiate employee investigations
- Participate in investigation interviews as necessary
- Provide legally permissible personnel information as necessary
- Contact Information
    - NAU Human Resources – 928-523-2223

ITS Communications
- ***Coordinates ITS Social Media and outage communications.***

- ***928-523-5929***

Communications & Public Media
- Provide expertise and planning for public communications and notifications.
- Contact Information
    - NAU Communications – 928-523-2282

Compliance, PCI, HIPAA, FERPA, Research
- Provide guidance and expertise on federal regulations involving an incident where data such as protected health records or student information was breached.
- Contact Information
    - PCI, NAU Comptroller – 928-523-9162
    - NAU HIPAA Privacy Office – 928-523-6347
    - NAU Office of the Registrar – 928-523-5490
    - NAU Research, Safety, and Compliance – 928-523-4340

Risk Management and Cyber Insurance
- Provide guidance and expertise on state risk management processes.
- Provide guidance and assistance with cyber insurance claims, third party assistance.
- Contact Information
    - Contracting, Purchasing and Risk Management – 928-523-4557

Third-Party Assistance
- When deemed necessary, and insurance claim will be filed, Risk Management will assist with actions required under the Cyber Insurance policy, including use of pre-approved third party vendors
    - Cyber Insurance policy lists vendor contact information and specialty areas
    - Includes potential for identity theft protection, credit monitoring, additional services
- Information Security Services may choose to leverage **MS-ISAC for Forensics and/or IR Assist**:
    - Contact soc@msisac.org
- **Microsoft Premier Support offers Cybersecurity Incident Response** via 1-800-936-3100
    - This requires a Premier Access ID – ITS Information Security Services or Cloud Integration and Architecture
    - Request to open a Severity “A” Cybersecurity Incident Ticket – Callback within 1 hour
    - Provide synopsis of issue, error codes, impact to users/timeline/financial

Incident Classification Table		
Severity Level	**Impact to NAU**	**Incident Response Characteristics**
CRITICAL	Highest severity level. Impacts are extraordinary and potentially catastrophic to the proper conduct of NAU's business, loss of public trust, and/or impact on NAU operations or personnel. Impacts that are indicators of this degree of severity are: • Threat to life or physical safety of the public, customer, or NAU personnel • Significant destruction of IT systems/applications • Significant destruction of corporate capabilities • Significant disruption of NAU business operations over a sustained period of time • Massive loss of Confidential information • Significant loss of public confidence • Dramatic corporate embarrassment • Risk of financial loss (generally more than $500,000 USD)	This level requires immediate and continual response actions from the core and extended response team. An incident of this severity has the most significant impact on NAU operations and involves an extensive, persistent, and usually very sophisticated attack that is difficult to contain, control, or counteract. Executive leadership and the Arizona Board of Regents will have an immediate and ongoing interest in the incident, the investigation, and the eventual recovery from the incident. Major external support from multiple organizations would be engaged. Would likely involve law enforcement. Would likely involve multiple levels of regulatory or compliance reporting. Would likely involve engagement by multiple Tier-1 media outlets.
HIGH	Impacts are substantial to the proper conduct of NAU business, loss of public trust, and/or impact on NAU operations or personnel. Impacts that are indicators of this degree severity are: • Impactful destruction of some IT systems/applications • Impactful destruction of some corporate capabilities • Substantial disruption of NAU business operations over a sustained period of time • Substantial loss of Confidential information • Substantial loss of Restricted information • Substantial loss of public confidence • Substantial corporate embarrassment • Risk of financial loss (generally between $100,000 and $500,000 USD)	This level requires immediate response from the core response team. This level may involve extended work hours, to include weekends, or could involve 24x7 response activities. An incident of this severity has a real and negative impact on NAU operations and involves a persistent or sophisticated attack that requires substantial resources to contain, control, or counteract. Executive leadership and the Arizona Board of Regents will likely have an interest in the outcome of the incident, the investigation, and the eventual recovery from the incident. External support from multiple organizations will likely be needed to resolve. Would likely involve law enforcement. Would likely involve some level of regulatory or compliance reporting. Would likely involve engagement by some Tier 1 and multiple Tier 2 media outlets.

Incident Classification Table		
Severity Level	**Impact to NAU**	**Incident Response Characteristics**
MEDIUM	Impacts are moderate to the proper conduct of NAU business, and/or impact on NAU operations or personnel. Impacts that are indicators of this degree severity are: • Moderate disruption of NAU business operations over a sustained period of time • Multiple sites or multiple business units affected by the incident • Moderate loss or manipulation of Restricted information • Limited loss of public confidence • Limited corporate embarrassment • Risk of financial loss (generally between $25,000 and $100,000 USD)	This level requires notification to the core response team. Several or most core response team members will be engaged in some aspect of the response effort. This level may involve extended work hours initially and will revert to a normal working schedule once initially contained. An incident of this severity has some impact on NAU operations and involves an attack that requires an organized response to contain, control, or counteract. External support may be needed, and will be engaged as needed. May involve law enforcement. May involve some limited level of regulatory or compliance reporting. Would likely not involve media outlets.
LOW	Impacts are greatly limited to the proper conduct of NAU business, and/or impact on NAU operations or personnel. Impacts that are indicators of this degree severity are: • Limited or no disruption of NAU business operations • One site or business unit affected by the incident • Limited or no unauthorized access to Restricted information • No impact to public confidence • No impact to corporate embarrassment	This level requires handling by a cybersecurity or incident response team member. This level of response is conducted during normal working hours. An incident of this severity has limited or no impact on NAU operations. External support is generally not needed. Law enforcement is generally not engaged. Regulatory reporting is not warranted. Would likely not involve media outlets.