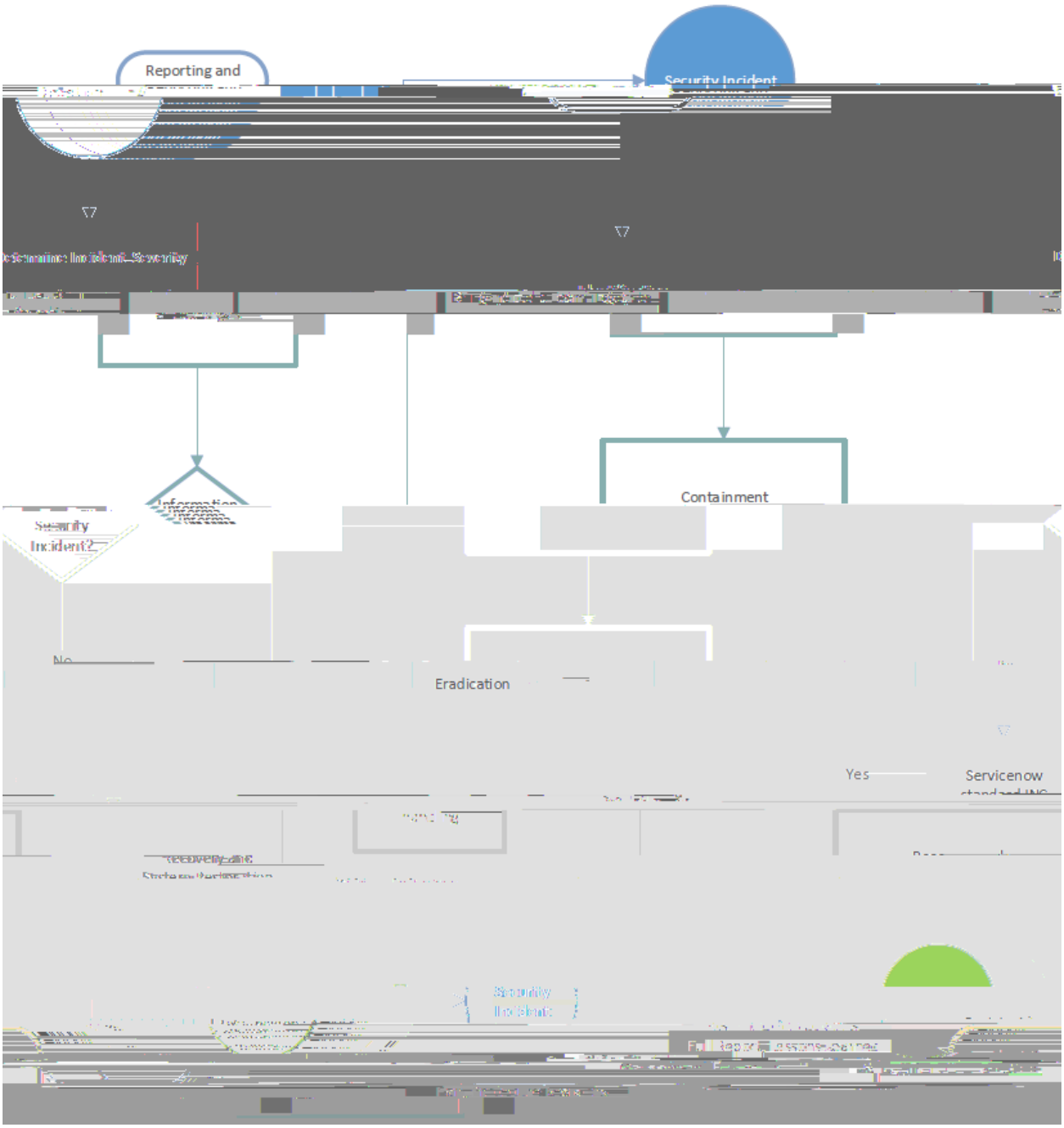
INFORMATION TECHNOLOGY INCIDENT

NCIDENT

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. Incident is reported to or detected by ITS.

A suspected incident will be reported to ITS

An incident may be detected by the Information Security Services teams and handled internally

B. Identification and Analysis. The reported or detected incident 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

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
-

APPENDIX

Security Incident Response Checklist - Example

ROLES, RESPONSIBILITIES, CONTACT INFORMATION

Technical Lead to assist Incident Leader

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 – 523-9162
- NAU HIPAA Privacy Officer – 523-6347
- NAU Office of the Registrar – 523-5490
- NAU Research, Safety, and Compliance – 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 – 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 Infrastructure & Platform Services
- 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:	

Incident Classification Table		
Severity Level	**Impact to NAU**	**Incident Response Characteristics**
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.
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.