IT Security Incident Response Policy

Policy Statement

Purpose and Scope

This policy defines how Mu ("MU") responds to a security incident. It applies to the entire MU organization, all MU systems, and all 3rd party systems carrying MU data. It also potentially has an impact on MU students and business partners. The MU leadership team recognizes the rapidly evolving IT security threat landscape, and understands that regardless of the security controls in place and the implementation of an appropriate "defense-in-depth" security architecture, it is inevitable that security incidents will occur, and that a well-planned response capability must be in place to deal with them. Management recognizes that intrinsic to an effective incident response plan, the incident response team has:

A) Explicit authorization to monitor networks, systems and storage as required.
B) An understanding that end users have no expectation to privacy and consent to such monitoring.

These two key preconditions to this policy are addressed in End User Responsibilities.

Responsibilities

Title or Role	What They are Responsible For
Chief Information Officer	Maintains and enforces this policy.
Technical Director	Acts as the primary head of the Incident Response Team.
IT Professionals	Monitor systems and activity, respond to potential security events and incidents. Forms the core of the incident response team.
Legal Counsel	Legal should review incident response plans, policies, and procedures to ensure their compliance with law, including the right to privacy. In addition, the guidance of counsel will be sought if there is reason to believe that an incident may constitute a crime or have other legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a binding agreement involving liability limitations for information sharing. Legal counsel also assists in the proper communication to external Law Enforcement agencies as required. Acts as an integral component of the incident response team.
University Communications	Handles external communications as required to the media and to the public. Acts as an integral component of the incident response team.
Human Resources	If an employee is suspected of causing an incident, the human resources department may be involved—for example, in assisting with disciplinary proceedings. HR may also be involved if personally identifiable information for employees was exposed, for example, if credit monitoring services need to be provided to affected employees. Will act as part of the incident response team as appropriate.
Public Safety	Coordinates with the incident response team for incidents that may affect the physical safety of MU employees, students or facilities. Some computer security incidents occur through breaches of physical security or involve coordinated logical and physical attacks. Provide access to incident response team to facilities during incident handling—for example, to acquire a compromised workstation from

	a locked office. Will act as part of the incident response team as appropriate.
3rd party system providers	Communicate adverse events to the incident response team, work with incident response team to prioritize and remediate any incidents with their systems and cooperate with law enforcement as necessary
3rd party security system providers	Outsourced security systems (e.g. intrusion prevention systems provided as a managed service) levy additional requirements on these providers. They will be a frequent source of events, will be integrally involved in incident response and remediation, and may drive the overall response. These providers are considered an integral part of the security response team and should have defined service level agreements (SLAs) specifically around incident response.
End Users	Report potential adverse events, cooperate with the incident response team as they prioritize and remediate any incidents.
President and Cabinet	Participate in the risk assessment of an incident and decision-making on communication with the media and other organizations. Supports the activities of the incident response team.

Policy

Events vs. Security Incidents

An event is any observable occurrence in a system or network. Examples of events include a user connecting, a server receiving a request, a user sending email, or a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, or execution of malware that destroys data. This policy addresses only adverse events that are computer security-related, not those caused by natural disasters, power failures, etc.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Security incidents may compromise the *Confidentiality* (e.g. data breaches), *Integrity* (e.g. hackers authorizing fraudulent transactions), or the *Availability* (e.g. Denial of Service attacks) of the MU network or systems. Security incidents can be *intentional* (e.g. an outside agent attacking MU systems, or an employee misusing confidential data) or *accidental* (e.g. unintentionally publishing employee personal information to the public or other employees who don't have a need to know).

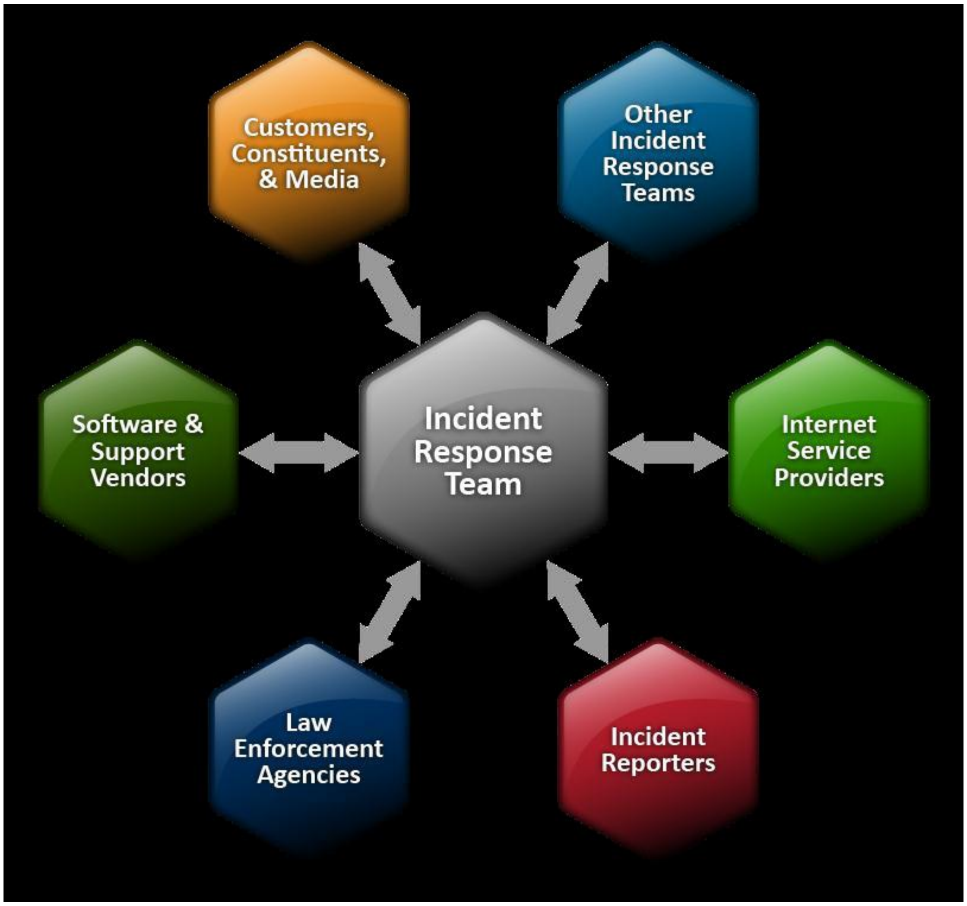
The Incident Response Team

The incident response team:

- Evaluates events and determines if a security incident may have occurred
- Prioritizes the incident
- Coordinates the response to the incident. This includes:
  - Determination if a specific adverse event may be a security incident. This includes intrusion detection.
  - Collection of data and evidence surrounding the incident
  - Remediation of the vulnerability
  - Attempt to determine the scope of impact. This includes duration, what data was potentially accessed or altered, or what systems and networks are unavailable.
  - Communicate and coordinate with Management, Legal, Public Relations, Building Safety and Security
- Provide advisories to the rest of the MU organization about new vulnerabilities as appropriate.

- Provide training and awareness on incident response policy and procedures to the rest of the MU organization
- Share information with other organizations on newly identified threats as appropriate. Specifically, this may include other area universities, ISACs (Information Sharing and Analysis Centers) such as www.IT-ISAC.org, state or regional partnerships.
- Prepares for handling an incident, by maintaining and walking through incident response procedures, and by selecting and maintaining up-to-date tools that can assist in responding to an incident.

The relationship between the Incident Response team and other groups is shown in the figure below (courtesy NIST 800-61):


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

The exact composition of the incident response team for a specific incident will vary somewhat depending on the circumstances. The table below shows the standing and optional members of the MU incident response team, their role, and for optional team members, when they are activated. The structure below gives a minimum incident response team size of two, and a maximum size of six to eight. Keeping the team as small as possible and empowered to make decisions is a vital element of a rapid, effective incident response.

Role	Who	When Included and What They do
Head of Incident Response Team	Normally the CIO. IT Director will act as backup	Always – will coordinate the overall response, be responsible for communications, and engage other incident response team members as required.
Technical Team Member(s)	Member of the IT team	Always – will have primary responsibility for identification, containment, eradication and remediation of the threat. This may be multiple team members to cover the necessary set of skills, but should be identified beforehand. In combination, they must have adequate administrative rights to sniff networks, change firewall configurations, administer server and network devices, apply server patches and install software upgrades.
Legal	Designated member of legal department – e.g. Associate Counsel	Optional – engaged if an incident may have legal ramifications, and assists with proper communication to Law Enforcement.
Public Relations	Designated member of Corporate/Public Relations/Community Relations who can make decisions – e.g. Director, Corporate Communications	Optional – engaged when the incident either affects the public (e.g. compromise of student credit card information), or could cause damage to the MU brand or reputation.
HR	Designated member of HR department who can make decisions – e.g. VP, Human Resources	Optional – engaged either when the incident involves employee misbehavior or a compromise to employee personal information.
Public Safety	Designated member of the Public Safety team who can make decisions – e.g. Director, Public Safety.	Optional – engaged if the attack could have physical security ramifications, or if required for access during the incident response.

Incident response team members must be identified by name in advance, and be aware of their responsibilities in the event of an incident. The exact composition of the incident response team, including afterhours contact information, will be reviewed and updated semi-annually. This contact list should also include contact information for all 3rd party service providers, the FBI, and local law enforcement, and an offline copy should be provided to all incident response team members.

Attack Vectors, and Examples and Indicators of Security Incidents

The threat landscape is constantly evolving, so any list of potential attack vectors or types of security incidents are illustrative, not definitive. Below are listed some common attack vectors, examples of types of security incidents, and how they might be detected. These lists are extracts from NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide.

Common Attack Vectors

■ **External/Removable Media:** An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.

■ **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).

- **Web:** An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.

- **Email:** An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.

- **Impersonation:** An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.

- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.

- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.

- **Other:** An attack that does not fit into any of the other categories.

Examples of Security Incident Indicators

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.

- Antivirus software alerts when it detects that a host is infected with malware.

- A system administrator sees a filename with unusual characters.

- A host records an auditing configuration change in its log.

- An application logs multiple failed login attempts from an unfamiliar remote system.

- An email administrator sees a large number of bounced emails with suspicious content.

- A network administrator notices an unusual deviation from typical network traffic flows.

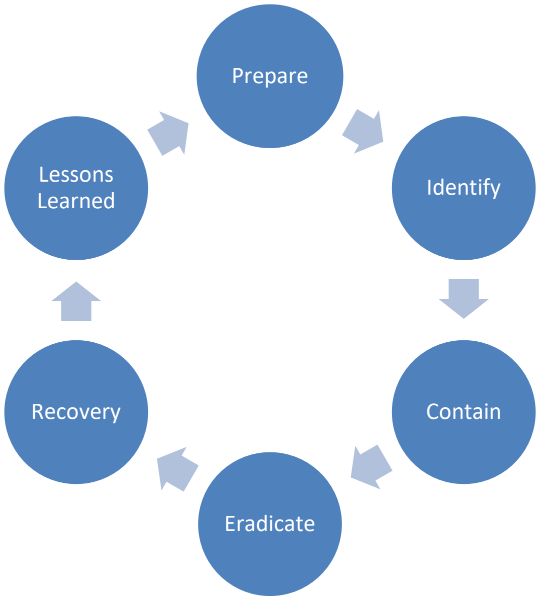
Commons Sources of Security Incident Precursors and Indicators

Source	Description
Alerts	
IDPSs	IDPS (Incident Detection and Prevention System) products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces *false positives*—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that

	the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident.
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.
Network flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Organizations such as US-CERT and CERT/CC periodically provide threat update information through briefings, web postings, and mailing lists.
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organizations	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

Incident Response Stages

The overall approach to the incident response process is shown below, and covered in detail in the rest of this policy.



This PICERL (Prepare-Identify-Contain-Eradicate-Remediate-Learn) approach was developed by the SANS Institute.

Preparing for an Incident Before it Happens

The incident response team is responsible for the following in preparation of an incident:

1. Select and keep updated tools that would be used for investigating an event. These may include network sniffing, packet logging, protocol decoding, and other computer forensic tools, unless those services will be provided by a 3rd party.
2. Participate in training on different types of incidents and appropriate response and remediation.
3. Identify ownership and responsibility for all systems (including data) in the enterprise.
4. Define alternate communication channels:
    a. Encrypted email communication (potentially not using primary email server).
    b. Encrypted chat messaging (potentially not using primary chat server).
    c. Create and Maintain contact list, including offline copies.
5. Define what additional resources are available to continue incident response work throughout a sustained (i.e. multi-day) response.
6. Confirm in-house capability or contracts with business partner for:
    a. Incident Response.
    b. Forensic Investigation.
    c. Malware Reverse engineering.
7. Predefine the containment strategy for different types of threats. These generally include:
    a. Watch and Learn, or
    b. Disconnect.

What Happens when an Incident Occurs - Incident Response Procedure

Identification

Notification of potential security threats and events may come from multiple sources, including end users, automated monitoring services that do passive detection (e.g. an IDS or IPS), by active detection, such as detecting an unusual service with a port scan, by monitoring external sources of information about new vulnerabilities or exploits, or observation by 3rd parties or IT professionals. All potential security incidents should be reported to MU and a ticket should be opened in the IT Request system. As soon as a potential security incident has been reported, the head of the incident response team should be notified, and he/she will have final say on whether a particular adverse event is to be treated as a security incident. Once declared an incident, an incident response form should be started (Exhibit A). If done electronically, the location of the form should be recorded in the ticket. The location of copies of supporting information (logs, screen shots, etc.) should be clearly identified as the investigation progresses, and ideally, copied to a common location off the network (e.g. an encrypted drive), as long as that drive is properly secured.

Initial focus should be on determining the nature and scope of a potential attack, and using that to prioritize the incident. Priority levels are defined as follows:

Priority Level	Definition
Low	Prevents system operations for a low availability system, or a data breach that does not include confidential data, a data breach of only internal data, or a confidential data breach impacting 10 people or less.
High	Preventing system operations for a medium or high availability system, or a breach of confidential data impacting more than 10 people.

The table below shows target timeframes for each stage of incident response, based on priority.

	Target Timeframes	
Incident Response Stage	Low	High
Identification	ASAP	ASAP
Containment	Within 1 business day	Within 4 hours
Eradication	Within 5 business days	Within 1 business day
Recovery	Within 5 business days	Within 2 business days
Lesson Learned	Within 5 business days	Within 2 business days

Depending on context, later stages may be accelerated in parallel with the later stage of identification. Specifically, the team may want to take certain containment actions before the scope is fully understood if it is clear this is a high priority event. The head of the incident response team will make this decision, if appropriate.

As the team prioritizes the incident, the head of the incident response team will determine what optional response team members should be contacted. If there is the potential a crime may have occurred, the head of the incident response team will contact Legal to confirm. The head of the incident response team will also work with executive management and Public Relations on whether the media needs to be notified.

Law enforcement should generally be notified if:

1. A crime may have occurred
2. There is a potential threat to student, employee or public safety
3. All phishing attempts shall be reported to the FBI

Media should generally be notified if:

1. A High-Level confidentiality breach occurred that impacted non-employees
2. If there was a potential threat to public safety

The timing and nature of these notifications will be determined by the head of the incident response team, working with executive management, Legal and Public Relations as required.

If the security incident included a data breach of Personally Identifiable Information (PII) or Protected Health Information (PHI), all individuals whose information was compromised must also be notified. This notification must be done consistent with the requirements of FERPA, PCI, HIPAA and HITECH, depending on the nature of the information compromised.

Containment

Once a security incident has been identified and prioritized, the incident response team will determine appropriate containment actions. Containment is simply defined as the actions required to stop further damage from occurring. It leverages the information gained during the identification stage to tailor the activity in the containment phase, or a lot of time can be wasted by not attacking the root cause of the incident. Depending on the event, containment actions may include blocking traffic from certain addresses or on certain ports, changing DNS entries, change the configuration of the IDS/IPS or firewalls, disabling specific accounts, up to removing individual devices or an entire system from the network, or shutting down part of the network. If the security incident is an active attack, the team should avoid actions that would unnecessarily notify the attacker. In no event should the team “hack back” – the focus should simply be to prevent further damage. Isolating the system (removing it from the network) may be the simplest initial containment step if the issue is malware.

In some cases, containment may need to be delayed to better monitor the attacker's activity and collect evidence. Due to the potential for additional liability, Legal should always be involved in any decision to delay containment.

Eradication

The goal during the eradication phase is to eliminate the threat posed to systems and information. Specific activities may include patching systems to correct a vulnerability, doing antivirus (AV), rootkit or network scans to ensure no other systems are affected, or changes to account permissions as appropriate. There may be additional evidence or information collected during this phase that will support any criminal investigation or aid in full recovery. Affected systems may still be unavailable during the eradication phase.

Recovery

The goal of recovery is to restore the affected systems and business processes to normal operations. Depending on the nature of the incident, it may involve rebuilding systems, reinstalling software, applying any system hardening guidelines, assessing the overall security of any rebuilt systems to ensure no additional vulnerabilities are inadvertently created, or restoring network access to systems that were isolated.

If the eradication and recovery phases take more time than is acceptable to the business, other business continuity plans may need to be considered.

If there has been a confidential data breach that includes a breach of personally identifiable information, disclosure of the breach to those impacted should be done early in the recovery phase, or in parallel with the eradication phase. This stage also more generally includes any other remediation that might be required, such as processing any refunds, settling any damage claims or providing credit monitoring to employees or students.

Lessons Learned

A key component to evolving the security posture of the organization is to conduct a lessons learned session after every security incident. The depth of the lessons learned analysis should be tailored based on the priority of the event. Outcomes of lessons learned may be additional training, new security procedures, changes to existing procedures, or new or updated tools.

Incident Response Testing

The incident response plan should be tested at least annually. This can be in the form of a conference room test or a simulated exercise. The test should cover:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of payment brands in the event of a payment card data breach.
- Specific incident response procedures.
- Business recovery and continuity procedures.
- Data back-up processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands for handling a payment card data breach.

Note: addresses PCI requirement 12.10.2.

References

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

1. NIST Special Publication 800-61 R2, Computer Security Incident Handling Guide, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
2. <<University Directory>>
3. SANS Institute InfoSec Reading Room, Incident Handler's Handbook, https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
4. SANS Institute InfoSec Reaching Room, An Incident Handling Process for Small and Medium Businesses, https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791
5. SANS SCORE: Law Enforcement FAQ, https://www.sans.org/score/law-enforcement-faq/
6. NIST special publication 800-86, Guide to Integrating Forensic Techniques into Incident Response, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Exhibits

This section contains links to any documents that are required to be used by the policy. Examples would include required forms or links to internal websites or systems required to implement the policy.

Exhibit A	Incident Response Form

Exhibit A - MU IT Security Incident Response Form

How was the Incident Identified?

Name and Title:	
Phone number(s):	
E-mail:	
How was it detected:	
Ticket #	

Type of Incident (check all that apply)

☐ Denial of Service ☐ Unauthorized use ☐ Unauthorized Access ☐ Phishing ☐ Espionage
☐ Probe ☐ Malicious Code ☐ Other:

Details:

Prioritization

☐ Low ☐ High

Contact Law Enforcement?

☐ Yes ☐ No

Details:

Communicate to Media?

☐ Yes ☐ No

Details:

Containment Actions

Who performed containment? ____________________________

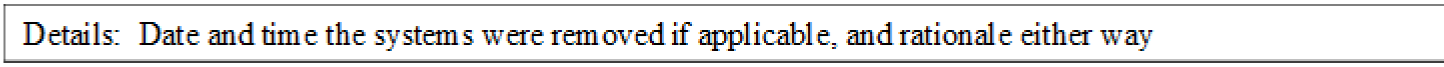
Were any affected systems removed from the network?

☐ Yes ☐ No

Who performed containment? ____________________________

Were any affected systems removed from the network?

☐ Yes ☐ No



Details: Date and time the systems were removed if applicable, and rationale either way

Were affected systems backed up?

☐ Yes ☐ No

Details: Date and time the systems were backed up, or reason they weren't. N/A if there was nothing to backup

Were the backup media sealed?

☐ Yes ☐ No

Details: When sealed and by whom, the location of backup media. N/A if there was nothing to backup

Eradication Actions

Who performed forensics and eradication? ______________________________

Was the vulnerability identified and corrected?

☐ Yes ☐ No

Details:

How did we confirm the incident was fully eradicated?

Details:

Recovery Actions

Briefly describe what steps we took to restore the affected networks and systems to normal performance. Also include here if there were any other remediation actions taken.

Details:

Lessons Learned

Briefly document any lessons learned and any long-term corrective actions taken.

Details:

Related Policies

- Acceptable Use
- Asset Management
- IT Security Framework
- End User Responsibilities

History of the Policy

2022-12-20 – The President of the University approved the establishment of this policy upon recommendation of the President’s Cabinet.

MARYWOOD UNIVERSITY
POLICIES AND PROCEDURES MANUAL