University of Mary
IT Security Incident Response

November 13, 2018

Purpose and Scope

This policy defines how the University of Mary (UMary) responds to a security incident. It applies to the entire UMary organization, all UMary systems, and all third-party systems carrying UMary data. UMary 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. 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

This policy applies to all students and employees at the University of Mary under authority of National Institute of Standards and Technology, Special Publication 800-171r1.

Responsibilities

Chief Information Officer	Maintains and enforces this policy
Technical Director	Acts as the primary head of the Incident Response Team
OIT Staff	Monitors systems and activity; responds to potential security events and incidents. Forms the core of the incident response team.

Legal Counsel	Legal counsel should review incident response plans, policies, and procedures to ensure their compliance with law, including the right to privacy. Counsel will provide guidance 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. Counsel also assists in the proper communication to external Law Enforcement agencies as required. Acts as an integral component of the incident response team.
Public Affairs	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 is 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.

Safety & Security	Coordinates with the incident response team for incidents that may affect the physical safety of UMary 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.
Third-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
End Users	Report potential adverse events, cooperate with the incident response team as they prioritize and remediate any incidents.
Council	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 UMary network or systems. Security incidents can be intentional (e.g. an outside agent attacking UMary systems, or an employee misusing confidential data) or accidental (e.g. unintentionally publishing employee personal information to the public or other employees who do not 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, including:
  - Determination if a specific adverse event may be a security incident, including intrusion detection
  - Collection of data and evidence surrounding the incident
  - Remediation of the vulnerability
  - Attempt to determine the scope of impact including duration, what data was potentially accessed or altered, or what systems and networks are unavailable
  - Communicate and coordinate with Executive Leadership, Legal Counsel, Public Affairs, and Safety and Security
- Provide advisories to the rest of the UMary organization about new vulnerabilities as appropriate
- Provide training and awareness on incident response policy and procedures to the rest of the UMary organization
- 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 Incident Response Team Composition

The exact composition of the incident response team for a specific incident will vary depending on the circumstances. The table below shows the standing and optional members of the UMary incident response team, their roles, 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
Incident Response Team Leader	Chief Information Officer (Technical Director or Director of Enterprise Applications 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 Members	Director of Enterprise Applications, Technical Director, Systems Administrator, Network Administrator, other members of OIT as required	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 Counsel	Legal Counsel	Always – an integral part of the team, advising on legal issues arising from an incident and/or the response to it. Legal counsel assists with proper communication to Law Enforcement.

Public Affairs	Designated member of Public Affairs who can make decisions – e.g., Vice President or Director	Always – engaged when the incident either affects the public (e.g. compromise of student credit card information), or could cause damage to the UMary brand or reputation.
Human Resources	Designated member of HR department who can make decisions – e.g. Director	Always – engaged either when the incident involves employee misbehavior or a compromise to employee personal information
Safety & Security	Designated member of the Safety & Security team who can make decisions – e.g. Director, Safety & Security	Always – engaged if the attack could have physical security ramifications, or if required for access during the incident response.

Attack Vectors 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

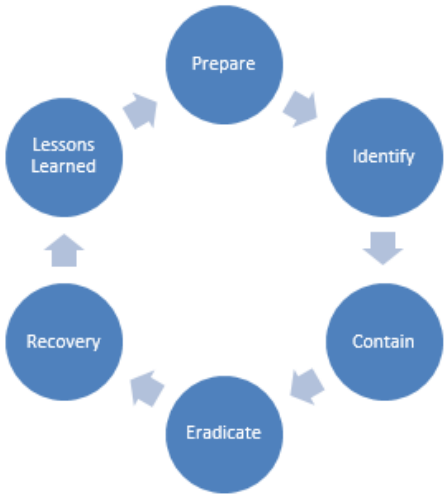
- External/Removable Media: An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive
- Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., 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

- Antivirus software alerts when it detects that a host is infected with malware
- An email recipient receives a phishing email
- 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

Incident Response Stages



Prepare

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

1. Select and keep updated tools used for investigating an event
2. Participate in training on different types of incidents and appropriate responses and remediation
3. Identify ownership and responsibility for all systems (including data) in the enterprise
4. Define alternate communication channels:
    a. Alternate email service
    b. Chat messaging
    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
    b. Disconnect

Identify

Notification of potential security threats and events may come from multiple sources, including end users, automated monitoring services that do passive detection, active detection (such as detecting an unusual service with a port scan), monitoring external sources of information about new vulnerabilities or exploits, or observation by third parties or IT professionals. All potential security incidents shall be reported to the Office of Information Technology (OIT) Help Desk at helpdesk@umary.edu or 701.355.3711, and a ticket opened in the IT Request system. As soon as a potential security incident is 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 (Attachment 1). 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 affecting 10 people or less.
High	Preventing system operations for a medium or high availability system, or a breach of confidential data affecting 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 5 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, the event 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 General Counsel to confirm. The head of the incident response team will also work with executive management and Public Affairs to determine if the media should 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

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 counsel, and public affairs 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

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. Depending on the event, containment actions may include blocking traffic from certain addresses or on certain ports, changing DNS entries, 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 Counsel 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, performing antivirus, 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.

Lessons Learned

A key component to evolving the security posture of the organization is incorporating 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.
- 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

Attachment 1

Information Security Incident Response Form

Who identified the incident?

Name & Title:

Telephone Number:

Email Address:

OIT Ticket Number (if applicable):

How was the incident detected?

Type of Incident (check all that apply)

_____ Phishing

_____ Unauthorized Use

_____ Unauthorized Access

_____ Malicious Code

_____ Denial of Service

_____ Probe

_____ Other (Describe)

Incident Details:

Prioritization:

_____ Low _____ High

Contact Law Enforcement?

____ Yes _____ No

If yes, provide details (date/time, person contacted, LE instructions, etc.):

Communicate to Media?

____ Yes _____ No

If yes, provide details (date/time, person contacted, message, etc.):

Department of Education notified?

____ Yes _____ No _____ N/A

Containment Actions

Person(s) performing containment (name(s) & contact information):

1.
2.
3.
4.

Were any affected systems removed from the network?

____ Yes _____ No _____ N/A

If yes, provide details (list systems, date/time the systems were removed if applicable, and rationale):

Were affected systems backed up?

_____ Yes _____ No _____ N/A

Details: List system(s), date and time the system(s) last backed up, or reasons why not. (N/A if there was nothing to backup)

Eradication Actions

Person(s) performing forensics and eradication (name(s) & contact information):

1.
2.
3.
4.

Was the vulnerability identified and corrected?

____ Yes _____ No

(Details)

How did the Incident Response Team confirm the incident was fully eradicated?

Recovery Actions

(Briefly describe what steps the Incident Response Team took to restore the affected networks or systems to normal performance. Also include here if there were any other remediation actions taken.)

Incident Response Team Findings & Recommendations

(List any recommendations related to the incident)

Lessons Learned

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

Exhibits

(List and attach any exhibits relevant to the security incident.)

Report Preparer