ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security Incident Response

Purpose

A continual threat environment necessitates our preparedness to respond to information security incidents of various types and severity. Loss of compliant or business sensitive data has serious consequences to the University as well as a possible widespread impact on others. An immediate and thorough response to an Information Security incident is required by legislation and by the UMS Information Security Policy and Standards (Section 10). This plan describes the overall UMS approach to responding to incidents, outlines procedures to be followed when an incident is discovered, and provides a foundation for campuses to build local plans.
The primary purpose of incident response is to reduce the impact of the incident through protecting the information resources from further unauthorized access, mitigating the effects of the incident, and fulfilling legal and regulatory obligations. Our goals for effective incident response include maintaining and restoring business continuity; determining how the incident happened; supporting law enforcement; learning how to better protect resources and respond to events; and timely and appropriately notifying management, stakeholders, and those affected.

To meet the purpose and goals, response to information security incidents must follow prescribed steps for initial assessment, investigation, reporting, and follow-up. The specific procedures within these steps need to be tailored to the type and severity of the incident.

Phase 1 [Detection and Analysis]

During the Detection and Analysis Phase, an initial incident assessment is carried out by performing the functions of Discovery, Categorization, Initial Notification and Triage.

Discovery

An information security incident is an adverse event that affects the availability, confidentiality or integrity of information resources.
An incident may be electronic or non-electronic. Electronic events relate to the security of computer systems, networks, or electronic data and may involve unauthorized computer access to a single or multi-user computer system. Non-electronic events involve activities such as inappropriate access to classified (business sensitive or compliant) information which is spoken or printed. Types of incidents include:

- Unauthorized access to information
- Unauthorized disclosure
- Network attacks or unwanted disruption(denial of service, scanning, sniffing)
- Malware (viruses, worms, trojans)
- Theft or loss of equipment
- Physical intrusion or break-in
- Social engineering (e.g. phishing)
- Policy violations such as unauthorized use of user credentials

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security Incident Response

Categorization

If an incident involves a campus computer and a breach of compliant data can be ruled out, the campus will take actions in accordance with their local plan. If an incident involves a System Office computer, the System Office will take the necessary actions to respond in accordance with this plan. If a breach of compliant data cannot be ruled out, the Office of Information Security and the campus will work together to take the necessary actions to respond in accordance with this plan.

Initial Notification

Upon discovering an incident, prompt actions must be taken to involve the right people in the incident response. The first step in notification is to complete a Security Incident Report (**APPENDIX B**) which must include enough information to determine proper actions and required reporting.

- Date and time of the incident discovery, and date incident occurred, if known.
- General description of the incident to include nature of the incident, the system that is affected and the organization that is involved
- Scope of the incident to include systems and/or data at possible risk
- Actions taken since incident discovery
- Contact information of individual reporting incident to include phone number and email address.

The flow chart **(APPENDIX A)** depicts the actions to be taken. First, notify appropriate supervisor, manager or department lead. In accordance with the Information Policy and Standards, electronic incidents shall be escalated to the campus IT help desk. Non-electronic events shall be escalated to the appropriate campus office (Information owner or applicable FERPA, HIPAA, or GLBA officer). Local staff should immediately review the situation to determine whether or not an event is actually an incident, whether or not the incident involves a potential breach of University data, and whether or not the presence of Compliant Data or Business Sensitive Data can be ruled out. Notifications for incidents which involve a potential breach will be made to the System CISO or the CISO's office (Office of Information Security) within the following timeframes:

- Immediately – upon confirmation of a breach of compliant data
- 1 hour – potential breach of compliant data if involvement of compliant data cannot be ruled out
- 2 hours – potential breach of compliant data multi-user systems if involvement of compliant data cannot be ruled out
- 4 hours – potential breach of compliant data on single user system if involvement of compliant data cannot be ruled out
- 24 hours – potential breach of business sensitive data or unclassified system if involvement of business sensitive or unclassified data cannot be ruled out.

Those incidents which involve potential breaches may include a larger scope than originally perceived. For that reason, all potential breaches shall be identified to the Office of Information Security. Upon notification that an event is an information security incident, the Chief Information Security Officer will classify the system according the type and severity considering the following factors for evaluation, to determine the appropriate management staff to contact and for the formation of the Computer Security Incident Response Team appropriate team.

- Criticality of systems
- Value of information compromised
- Number of people or functions impacted
- Business considerations
- Public relations
- Impact to the University

The Chief Information Security Officer (CISO) will rely on individuals with the right expertise to assist in his/her specific area to work collaboratively in limiting the impact of the incident and to increase the speed at which the University can recognize, analyze and respond to the incident. Depending on the nature of the incident, the CISO may form a CSIRT **(APPENDIX C).**

Priorities in incident handling:

It is important to prioritize the CSIRT actions to be taken during an incident before an actual incident occurs. In certain situations, an incident may be so complex and have so many moving parts that it is impossible to respond to everything at once; priorities are essential.

PRIORITY	Task
1	Protect human life and people's safety
2	Protect compliant or sensitive information from discloser, abuse or misuse.
3	Protect regulated information to ensure no criminal/civil administrative action occurred
4	Protect critical information, systems, and networks from compromise, damage, alteration or corruption.
5	Minimize business disruption.
6	Certify that the integrity and availability of the areas affected have been restored to a Production Ready and Active Environment.

Triage

The objective of the triage process is to gather information, assess the nature of an incident and begin making decisions about how to respond to it. The following factors need to be considered during triage. One important condition to make the process both efficient and effective is determining who has responsibility and or authority over the suspected compromised system.

- What type of incident has occurred?
- Network (campus) affected?
- Who is involved?
- What are the effects of the incident
- What is the scope?
- Are there other vulnerable or affected systems?
- What is the impact thus far?
- What is the projected impact?
- What can be done to contain the incident?
- Analysis to identify the root cause of the incident?
- Recommendations for proceeding?

Preventing the situation from becoming more severe is critical, so actions to contain are critical. Deep analyses such as identifying the root cause of the incident should be continued but delayed until after the incident is contained.

Special consideration should be made to preserve evidence as part of incident response. Gathering evidence and preserving it are essential for proper assessment of an incident, and for recovery. In accordance with the UMS Information Security Policy (Section 10.2), where evidence is required, it shall be collected to ensure compliance with legal requirements. Keeping good records and maintaining a chain of custody are essential to follow-up activities, such as criminal investigations. In accordance with the Information Security Policy and Standards (Section 10.2.3), the campus police department, or local law enforcement where sworn campus police are not available, shall be utilized to ensure proper procedures in evidence collection, chain of custody, storage, and delivery whenever an incident may involve a violation of law such as illegal entry. In some instances the equipment, images of the equipment or other records may be seized to be used for possible forensic analysis.

Chain of Custody pertains to the documentation and securing of evidence items recovered during an incident. Each item is assigned a unique identifying number or name, initialed by the team member recovering the item and documented in a format listing each item, where it was located, the date and time of recovery, and the team member involved. Items are then secured in a controlled environment under limited access. A record is kept documenting each person who comes into contact with the evidence item and the purpose for that persons possession of the item. Accountability for ensuring this process is adhered to lies with the CISO, with responsibility for following this procedure residing with each team member encountering items of an evidentiary nature.

In general, the following concepts should be applied:

- Actions taken to secure and collect electronic evidence should not change the evidence.
- Activity relating to the seizure, examination, storage, or transfer of electronic evidence should be fully documented, preserved, and available for review.

Many incident investigations, especially those expected to result in criminal or civil legal action will include a forensic analysis component. The CSIRT members will frequently serve dual roles as investigators and forensic analysts. Each role has distinct areas of responsibility.

NOTE: *Incident responders should use caution when seizing electronic evidence devices. The improper access of data stored in electronic devices may violate provisions of Federal Law such as the Electronic Communications Privacy Act (ECPA). Additional legal process or policy may be necessary.*

PHASE 2 [Containment/Eradication/Recovery]

Containment Actions necessary to prevent further damage or exposure must be performed expeditiously. Computer systems that are engaged in active attacks against other computer systems (such as denial of service attacks) must be contained immediately. The CISO or the CSIRT may coordinate with Networkmaine to block compromised services and/or hosts that present a definitive danger to the rest of the network. Unless further investigation requires unrestricted access, all other compromises must be contained as soon as possible, but no later than the same business day. Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, changing passwords on compromised systems as well as any systems that regularly interact with the compromised systems, or other means as appropriate.

Eradication Normal operations must be resumed with confidence that the initial problem has been fixed. Eradication efforts will focus on identifying, removing and repairing the vulnerability that led to the incident and ensuring the system is 100% free from the problem. To do this, the vulnerability needs to be clearly identified so the incident isn't repeated. In addition to this vulnerability analysis, actions may include implementing protection techniques such as firewalls, moving the system to a new name/IP address, or in extreme cases, porting the machine's function to a more secure operating system. After removal or elimination of the cause of an incident, and the system has been restored, efforts shall be made to confirm the mitigation of all threats and vulnerabilities and to verify new threats have not emerged.

Recovery Resuming operations to a fully operational status is needed for business continuity. However, restoring operations is a business decision that should be made only when it can be concluded that resuming operations is deemed to be sufficiently safe. Once the system has been restored, verify that the operation was successful and the system is back to its normal condition. Once the system is back on line, continue to monitor for back doors that escaped detection.

Phase 3 [Post-Incident Activity]

Reporting Requirements

The type of data that was breached in the incident, determines the law, statute or agreement which covers the situation and the reporting that is needed. Notification to any known individuals who may be harmed by this incident is likely to be required. The Maine Data Act (**APPENDIX D**) shows an example of what might be required.

In addition to notifying affected individuals, the CSIRT in conjunction with the affected Campus/department must make a determination as to what measures will be taken on behalf of the individuals. In particular identity protection and audit monitoring services can be made available. These services can be offered to the affected individuals under a specified duration with a limited sign-up window. The University is then charged only for the individuals who sign up to take advantage of the protection services.

Follow-up: Notification and Lessons Learned

After resolution of the incident, the campus or System IT organization responsible for closing the incident will prepare an after-action report **(APPENDIX E)** in accordance with the UMS Information Security Policy and Standards (Section 10.2). This report will include the cause, action taken, estimated cost to the organization, resources needed to fully recover, recommendations to improve security and prevent similar incidents and recommendations for future incident response. The report will be sent to the CISO who will forward it to senior management. Actions taken to preclude this type of incident from reoccurring will be documented and tracked. System standards and practices or campus procedures will be examined to determine if modification would preclude further incidents of this type.

Campus Plans

For local response to incidents, each campus IT organization shall develop an incident response plan. In accordance with the UMS Information Security Policy and Standards (Section 10.1.1.1), the campus plan will be approved by the CISO and the campus administration that will include conditions for escalation to the System office, and be an annex to their campus and crisis management plan. A sample plan is attached (**APPENDIX F**).

APPROVED

Signature on file in System Office of Finance and Administration

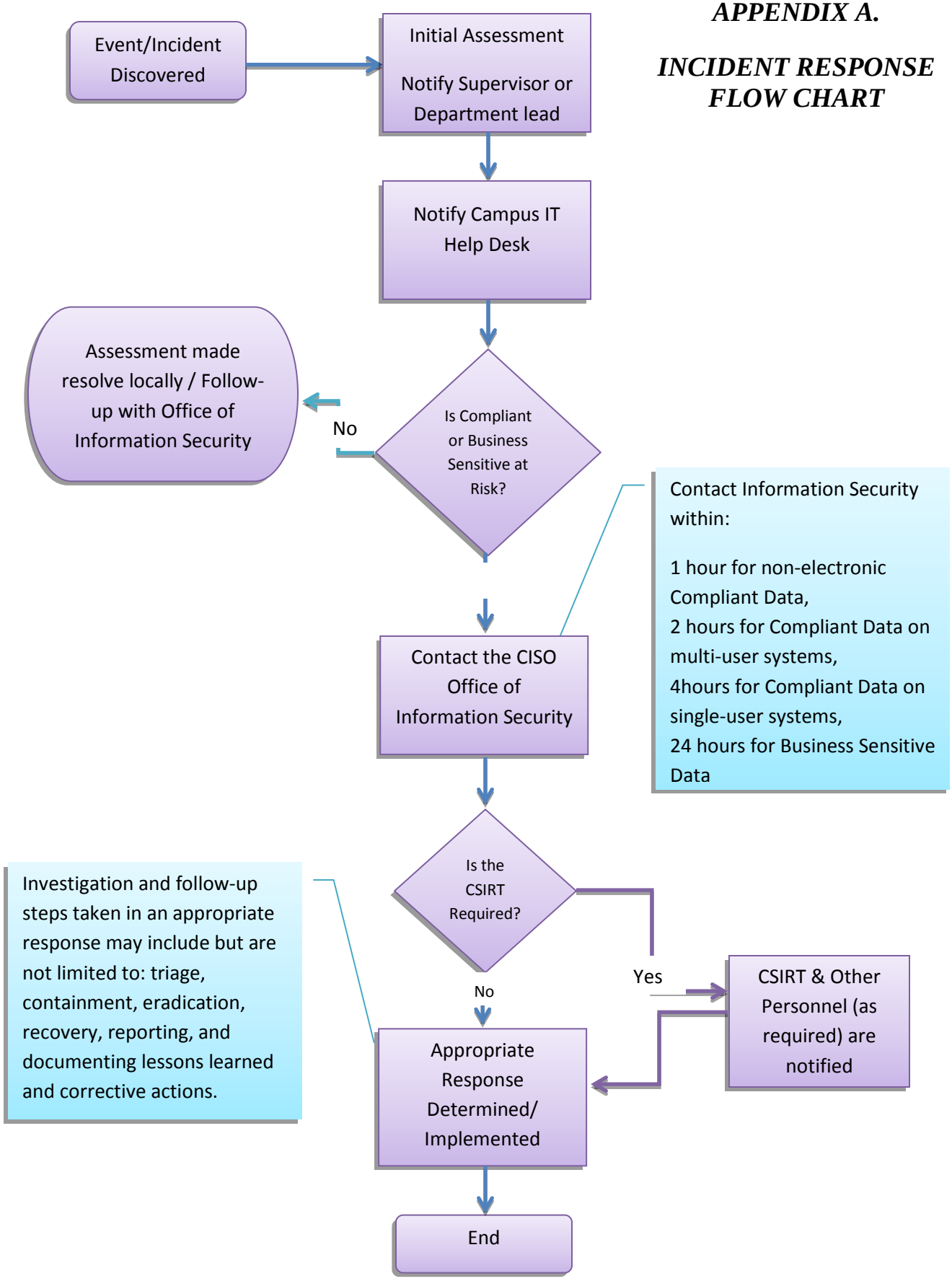
Rebecca Wyke, Vice Chancellor Finance & Administration

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security Incident Response

APPENDIX A.

INCIDENT RESPONSE FLOW CHART



ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security Incident Response

APPENDIX B. Security Incident Report

Security Incident Report

Contact *Information*

Name: _____ Title: _____

Email: _____ Telephone: _____

Department: _____ Date Report Submitted: _____

Incident Information

Physical Location(s) of affected computer system/network (be specific):

_____

Date/Time of incident: _____ Duration of incident: _____

Is affected system/network critical to department's mission?

How was *the* incident discovered?

☐ System Logs ☐ Performance Degradation ☐ Third Party

☐ Notified by user ☐ Other

Type of Incident:

☐ Unauthorized Access ☐ Network Attacks/Disruption ☐ Malware

☐ Theft or Loss ☐ Physical Intrusion/Break-in ☐ Social Engineering

☐ Policy Violation ☐ Other _____

What computer/Operating Systems were affected?

_____

The apparent source (IP address) of the intrusion/attack: _____

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security Incident Response

Incident Data Classification:

☐ Security Incident involving Compliant Data ☐ Security Incident involving Business Sensitive Data

☐ Security Incident involving Unclassified Data

What actions and technical mitigation have been taken?

Additional Remarks:

APPENDIX C. Computer Security Incident Response Team (CSIRT)

Criteria for determining if the CSIRT should be formed include, but are not limited to: the severity of the incident, whether a breach has occurred, legal issues surrounding the incident or information involved, and the possibility of reputation loss. The CSIRT shall consist of a management and technical component.

Representatives from the following offices may comprise the CSIRT management component on an as needed basis:

- CISO
- University Counsel
- Vice Chancellor for Finance and Administration
- Chief Information Officer
- Public Relations (System and/or Campus)
- Appropriate Information Owner/Custodian
    - Chief Human Resources and Organizational Development Officer
    - Executive Director of Student Affairs
- Campus Leadership to include the department or school directly affected
- Campus IT Leader
- Campus Security

Representative from the following offices may comprise the CSIRT technical component on an as needed basis.

- Security analyst(s) from the Office of Information Security (CISO office)
- Network Analyst/Communications Specialist(s) from Networkmaine
- System Administrator of the system affected
- Campus designated information security managers or other IT expert(s)(non-necessarily from the campus where the incident occurred
- A recorder from the local campus (This individual will not participate in the investigation, but will be charged only with documenting what was done when.)

Depending on the nature of the incident the CSIRT may call upon other personnel or organizations as needed. Those others may include but are not limited to:

- Law enforcement (local, state, and/or Federal)
- Vendors
- UMS employees/students
- Other government agencies.

The CSIRT will ensure that actions are taken in a timely manner to include:

1. External communications, proper notifications to affected individuals, and reporting as required by law or otherwise deemed appropriate,
2. Fulfillment of the investigative actions by the technical component (triage, contain, eradicate and recover),
3. Develop a final report which will summarize the findings.

APPENDIX D. Maine Data Act

The Notice of Risk to Personal Data Act (the Act) (10 M.R.S.A. § 1346 et.seq.) creates a duty to investigate breaches in the security of an individual's computerized data and an obligation to notify such individual of the breach in specified situations.

A breach is defined as an unauthorized acquisition of data "that compromises [its] security, confidentiality or integrity," or an authorized acquisition which is then used for an unauthorized disclosure of such Personal Information.

For the purposes of the Act, the data protected is referred to as "Personal Information" stored in a University storage system. That is: An individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

1. Social security number;
2. Driver's license number or state identification card number;
3. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;
4. Account passwords or personal identification numbers or other access codes; or
   Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Personal Information does not include "publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media."

Someone "unauthorized" is a person who "does not have authority or permission to access the information… and/or obtains access by fraud, misrepresentation or similar deceptive practices."

If the University becomes aware of a breach, it must "conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information has been or will be misused."

If, after the investigation, it is determined that a breach has occurred, notice must be given to the person(s) affected. It must contain the date of the breach; the information believed to have been accessed, a summary of the University's response to the breach and a person they can contact for additional information. The notice must be given as "expediently" as possible and "without unreasonable delay," consistent with the needs of law enforcement and the need to restore the reasonable integrity, security and confidentiality of the data in the system.

Notification is required when personal information was or is reasonably believed to have been acquired by an unauthorized person…and there is likelihood that it will be misused.

Notice must be in writing (presumably given by U.S. Mail) to the person's known address unless the cost would exceed $5,000 or notification has to be given to more than 1,000 people. In these events or if there is no mailing address available "substitute notice" can be given by both e-mail and also placed conspicuously on the University's website. If substitute notice is given, the statewide media must also be notified.

If a single breach involves notification of more than 1,000 people, notice must also be given "without unreasonable delay" to consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

A report must be sent to the State of Maine Attorney General.

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Information Security Incident Response

APPENDIX E. After-Action Report

SAMPLE INCIDENT AFTER-ACTION REPORT	
Date Incident Occurred	Date:
Summary	
An overview of what occurred and who was involved in the incident.	
Root cause:	
Action taken during incident:	
Incident Outcome	
Detailed Incident Resolution:	
Estimated cost of incident: (Include expenses, labor hours, etc.)	
Additional details of the impact: (Resources needed to fully recover)	
After Actions	
Actions taken to prevent reoccurrence:	
Recommended or proposed actions:	
Recommendations to improve incident response:	

APPENDIX F. Template for Campus Computer Security Incident Response Plan

The UMS Information Security Policy and Standards requires each campus IT organization develop and implement a computer security incident response plan. This plan outlines the actions to be taken when a computer security incident is discovered.

This plan supplements the University of Maine System Information Security Incident Response Plan. For further guidance on incident response refer the UMS plan. If the incident in question is does not involve electronic storage, processing, or transmission of data (i.e. it doesn't involve a computer system) use the UMS plan and contact the University of Maine System Office of Information Security as needed.

A security incident may involve any or all of the following:
• a violation of campus computer security policies and standards,
• unauthorized computer access,
• loss of information confidentiality,
• loss of information availability,
• compromise of information integrity,
• a denial of service condition against data, network or computer,
• misuse of service, systems or information, or
• physical or logical damage to systems.

Incident response is a multi-step process from the detection to the recovery. Accomplish the following steps to ensure the process moves along and the exposure for the University is minimized.

1. **Assess the situation.** What happened? What data may be at harm? Does the situation require urgent actions to stop further spread of the problem?
2. **Notify the Campus IT Help Desk.** Many incidents cause more harm because people spend too much time trying to investigate locally. Be sure to consult with IT before destroying any forensic data. It may be necessary to take the system off the network, to contain the spread. The UMS plan calls for rapid notification the Office of Information Security if a breach of compliant or business sensitive data cannot be ruled out.
3. **Participate in Response Team.** Depending on the category of the incident, the investigation, containment, eradication, and recovery will take expertise from various functional areas at the campus and possibly at the System Office. Any required notification to individuals will be do in consultation with University Counsel and the CISO.
4. **Close the Incident.** It is important to document the incident and to determine if the incident response processes could be improved and to take remediation actions to prevent reoccurrence.