Guide for Cyber Security Incident Response

ABSTRACT

This document assists University personnel in establishing incident response standards and guidelines for handling cyber incidents efficiently and effectively. It provides tools and guidance for cyber incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

IMPORTANT: If an incident is deemed to be illegal or life threatening, contact the University of Miami Police, or Emergency: 911

The Information Security Office can be reached by emailing ciso@miami.edu or (305) 284-1526.

Table of Contents

Section 1: Introduction

Purpose and Scope

The intended purpose is to provide standards and guidance to address cyber security incidents, which may have impacts that affect the University's operational, financial, or reputational standing, and/or the ability to comply with regulatory and legal requirements.

This resource guide:

- Does not replace Continuity or Disaster Recovery Planning; rather, it augments the standard operating procedure, SOP-UMIT-CSIH-140-01, Cyber Security Incident Handling, which provides a framework and processes by which consistent approaches can be developed and resource allocations can be made for a given scenario to facilitate the detection, identification, containment, eradication, and recovery from specific cyber security incidents.
- Applies to all university-owned computers, servers, technology devices, systems, services, applications connected, and/or used by the University of Miami employees, students, affiliates, guests, and all University locations.
- Serves as a practical guide for responding to incidents effectively and efficiently. The primary focus of is to provide assistance with detecting, analyzing, prioritizing and handling incidents through guidelines, standards, and procedures to establish an effective cyber security incident response program.
- Addresses only incidents that are computer and cyber security-related, not those caused by natural disasters, power failures, etc. Incidents can be unique and unusual and the guide will address basic steps to take for incident response. The Cyber Incident Response Team and the Cyber Incident Response Governance Board will address and recommend appropriate steps as related to the incident.
- Is not a detailed list to accomplish every task associated with cyber incident handling and response.

Mission and Vision

Part of the overall mission for UMIT is to provide, secure, protect, maintain and manage information systems and services, allowing the University to achieve its mission. This is in scope with UMIT's vision: "*To be the best information technology organization in higher education and healthcare; recognized for strategic leadership, innovation, and collaborative partnerships in achieving the University of Miami's academic, clinical, and research goals.*"

To support the University's mission and UMIT's mission, it was instrumental to create and develop a guide for incident response. The Cyber Incident Response Team (CIRT) facilitates the incident response process. The CIRT mission is to:

1. Limit the impact of incidents in a way that safeguards the well-being of the University community.
2. Protect the information technology infrastructure of the University.
3. Protect confidential and sensitive University data from disclosure, modification, loss and exfiltration.
4. Collect the information necessary to pursue investigation(s) at the request of the appropriate university authority.

Authority

The Vice President and CIO for Information Technology by the Vice President for Business and Finance/Chief Financial Officer and the University of Miami Board of Trustees will provide authority and oversight for the security of university information technology resources.

The Vice President and CIO for Information technology has delegated the Information Security Office the authority to act in a diligent manner to protect the integrity, confidentiality, and availability of the University's information technology resources including, but not limited, to infrastructure and information.

University policies and procedures provide the Chief Information Security Officer (CISO) and the Information Security Office (ISO) the authority to respond to threats and vulnerabilities to the University networks, systems, and services. This guide supplements and provides resources and guidance for these polices. For further review of these policies, please visit: http://it.miami.edu/policies.

The detection, identification, containment, eradication, recovery and reporting of cyber security incidents ensures that information security events, vulnerabilities, threats, and weaknesses associated with information systems are communicated and addressed in a manner that will for allow timely corrective action to be taken. The University of Miami Information Technology (UMIT) is responsible for:

- Maintaining incident response procedures, standards, and guidelines;
- Maintaining the Computer Incident Response Team (CIRT) to carry out these procedures; and for
- Arranging for the intake and investigation of reports of suspected and/or potential IT security exposures of university data and other suspected cyber incidents.

The CISO manages and coordinates detection, identification, containment, eradication, and recovery efforts of reported cyber security incidents within the University. The CISO has the authority to classify threats as a risk to the University and to activate the Computer Incident Response Team (CIRT) when necessary. Activation of the CIRT team will occur when a cyber security incident is identified as affecting University IT systems/services at an enterprise or a multi-level department.

Audience

The guide serves faculty, staff, students, and others such as affiliates and vendors who have a relationship with the University of Miami.

Section 2: Cyber Incident Response Capabilities

A cyber security incident is defined by the Department of Homeland Security as an occurrence that:

1. Actually or imminently jeopardizes – without lawful authority – the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores or transmits;
2. Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies; and/or
3. An incident can be either intentional or accidental in nature.[1]

Establishing incident response capabilities at the University:

1. Ensures a systematic, consistent incident handling methodology and coordinated actions for responding to incidents;
2. Helps personnel to minimize loss or theft of information and disruption of services caused by incidents; and
3. Builds institutional resilience.

Information gained and lessons learned during incident handling will help better prepare for dealing with future incidents, and limits the impact of incidents in a way that safeguards the well-being of the university community.

University of Miami's Approach to Cyber Incident Response

The University's approach is to provide policy, standards, and documentation for establishing incident response capabilities, recommendations, and advice on maintaining and enhancing existing capabilities in the event of an incident.

Strategy and Goals for Cyber Incident Response

Timely and thorough action to manage the impact of incidents is a critical to limit the potential for damage by ensuring that actions identified and taken are well known and coordinated. Incident response goals include:

- To protect the well-being of the University community.
- To protect the confidentiality, integrity, and availability of University system, networks, and data.
- To help University personnel recover their business processes after computer or network incidents.
- To provide a consistent response strategy to system and network threats that put University data, systems, and services at risk.
- To develop and activate a communications plan including initial reporting of the incident as well as ongoing communications as necessary.
- To address any legal issues.
- To coordinate efforts with external incident response teams.
- To minimize the University's reputational risk by notifying appropriate University officials of incidents that have the potential to become high profile events and implementing timely and appropriate corrective actions.

To achieve these goals, UMIT has adopted security best practices from standardized incident response processes such as those published by the National Institute of Standards (NIST), Special Publication 800-61 and other subject matter experts such as SANS and OWASP.

The specific process elements that comprise the UMIT Cyber Incident Response Plan include:

- Preparation: Maintaining and improving incident response capabilities and preventing incidents by ensuring the systems, networks, services, and applications are secure;
- Identification: Confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents;
- Containment: Minimizing loss, theft/misuse of information, or service disruption;
- Eradication: Eliminating the threat;
- Recovery: Restoring computing services quickly and securely; and
- Post-incident activities: Assessing response for more effective handling of future incidents through utilization of reports such as "Lessons Learned," and after-action activities or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future. Perform cost analysis for an incident as requested and determined by the CIRT Governance Advisory Board.

Primary functions present throughout incident response handling include:

- Communication: Notifying appropriate internal and external parties and maintaining situational awareness;
- Analysis: Examining available data to support decision-making throughout the incident management lifecycle; and
- Documentation: Recording and time stamping all evidence discovered, information collected, and actions taken from identification through post-incident activities.

University Authority for Cyber Incident Response –

Cyber Incident Response Governance Team

The Cyber Incident Response Governance Team is responsible for providing oversight, direction, and guidance for cyber incident response. The team is composed of the following University stakeholders:

- Vice President and CIO for Information Technology or their designee
- Chief Information Security Officer
- University General Counsel
- University Internal Audit
- UHealth IT (where needed and appropriate)
- HIPAA Privacy and Security (where needed and appropriate)
- UHealth Compliance (where needed and appropriate)
- University Compliance
- University General Counsel
- University Police
- University Communications/Relations

Other groups such as those listed below are included in an advisory capacity to provide feedback and guidance during the incident procedure. These departments/individuals include:

- Vice President for Business and Finance/Chief Operating Officer – Potential financial impact to the University and personnel actions for staff
- Vice President and Provost – Personnel actions for faculty.
- University Internal Audit – Data integrity of critical University data, compliance with University procedures and fraud investigations
- Student Affairs/Student Conduct – Offenses by University of Miami students
- Data Custodians/Trustees/Stewards/Owners – sensitive or non-public data access

NOTE: Requests from local, state, federal, private legal, or other entities do not necessarily constitute proper authority. Submit all external requests for approval and authorization to University Counsel for their review. Upon their review and approval, the requests will be routed to the appropriate department. These requests include, but are not limited to, the requests for information below.

- Warrant: If presented with a warrant authorized by University General Counsel, comply immediately with the request. Notify your supervisor and the campus police unless advised by law enforcement or General Counsel.
- Subpoena: If presented with a subpoena authorized by University General Counsel, comply with the request. Notify your supervisor unless advised otherwise by General Counsel.
- Freedom of Information Act: University General Counsel will advise how to honor the requests.

Cyber Incident Response Team

The UMIT CIRT, as needed and defined by the nature, scope, and type of incident, is composed of membership from the Information Security Office staff, Applications and Services, Infrastructure and Operations, Academic Technologies, and members as needed from the campus at large. See Appendix B, UM Cyber Incident Response Team Organization Chart.

Reporting a Cyber Incident

An incident is any event that poses a threat to the integrity, availability or confidentiality of the University's systems, services, and/or information. Incidents must be reported immediately to the Information Security Office or as soon as possible after discovery. The CISO, or their designee, will act as the Incident Response Manager (IRM) for all reported incidents. The CISO, with the assistance of the reporting entity, will coordinate all aspects of the incident response process. The reporting entities must coordinate with the CISO or their designee prior to initiating any actions during the incident response process. All communications regarding incidents must be conducted through channels that are known to be unaffected by the incident.

Incidents can be reported using various communication channels including email, phone, in-person, or by initiating a UService incident ticket.

The Information Security Office can be contacted at ciso@miami.edu or (305) 284-1526.

Examples of incidents that need to be reported immediately include, but are not limited to:

- A virus/worm/Trojan affecting multiple systems;
- Intrusion, loss, theft, or damage to electronic information, the network, systems, electronic devices, etc.
- Other involving the security or privacy of information resources.

Prompt and early notification allows the CISO and affected departments time to gather as much information and evidence as possible when escalating potential incidents. Information that should be gathered and shared when reporting an incident includes:

- A description of the incident, including a timeline and identification/detection details.
- Contact information of affected individuals.
- If known, the IP Address, hostname, and location of system(s).
- In the case of a Website incident, the specific URL.
- Type and classification of data (personally identifiable information, electronic personal health information, student information, financial information, etc.) that may be included on the system.
- What is the level of the system's criticality as noted on its most recent risk assessment.

Prompt reporting may help reduce risks associated with incidents, including:

- Regulatory: Compliance with federal and state legislation regarding the protection of information. This includes data and systems that fall under GLBA (Gramm-Leach-Bliley Act), HIPAA (Health Insurance Portability and Accountability Act), FERPA (Federal Education Rights and Privacy Act), ITAR (International Traffic in Arms Regulations), PCI-DSS (Payment Card Industry Data Security Standard), federal/state data breach notification laws and the Patriot Act.
- Operational: Failure to protect systems and data can cause disruptions to critical daily operations.
- Financial: There may be costs associated with lost data, restoring systems, and data breach notifications.
- Reputational: There may be a negative impact on confidence in a system or on the University's reputation.
- Physical safety: Due to the prevalence of the "Internet of Things" such as those used to monitor patient care and physical facilities, a cyberattack against networked devices could cause physical harm to individuals.

Cyber Incident Response Procedures

When an incident report is received, the CISO will confirm details surrounding the incident through the identification, detection, and analysis phases of incident handling. Different types of incidents merit different types of response strategies. Generally,

- For a confirmed incident, the CISO will coordinate actions through the Cyber Incident Response Governance Team and the CIRT Team.
- If an incident cannot be confirmed, the CISO will seek advice from subject matter experts and make mitigation recommendations to the reporting entity.

The CISO and the CIRT team shall categorize the incident according to type and potential impact(s). The incident shall be classified and addressed in order of priority.

- If immediate action is required, the CISO will begin coordinated incident response activities. NOTE: The CIRT will only be activated when an incident is affecting University IT systems/services at an enterprise or multi-department level.
- If immediate action is not required, the CISO will work with the reporting entity to determine appropriate response recommendations and actions.

In the case of multiple incidents occurring simultaneously, the CISO and CIRT Team will triage and classify the incidents according to their immediate and potential adverse effects and prioritize investigation and recovery activities according to the severity of the incident.

Communications and Information Sharing

Communication is essential for relationships between affected areas and UMIT and must be established between the CISO and other groups, both internal (e.g., human resources, legal), and external (e.g., other incident response teams, law enforcement, vendors who specialize in incident response and have a contractual relationship with the University). Communication must occur in a timely manner with clarity and accuracy. University departments should proactively develop internal incident communication guidelines.

A communication plan must be activated soon as possible after an incident has been confirmed.

After the confirmation of an incident, the CISO and the CIRT Governance Team will coordinate to allow for appropriate information sharing and communication between those parties that have a definite need to know.

A communication plan is mandatory whenever there is a confirmed breach of PII and or PHI.

The communications plan should identify internal and external communication needs and describe how these needs will be addressed. Smaller events may only require internal communications, while larger events may require interaction with external stakeholders.

Section 3: The Incident Response Process

This section details the major phases of UMIT's incident response process: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

Preparation

Preparation is fundamental to the success of incident response programs. One of the recommended preparation practices for all colleges and departments within the University, including the hospital campus is to conduct an annual IT risk assessment. The benefits of conducting such an assessment include identifying applicable threats, including organization-specific threats. Each risk is categorized and prioritized to determine if the risk can be mitigated, transferred, or accepted until an overall, level of risk is reached. A second benefit includes the identification of critical resources. This allows staff members to promote, emphasize and develop monitoring and response activities for those resources.

Conducting an IT risk assessment enables departments to correlate IT resources with mission critical business processes and services. From the use of the information from the risk assessment, it becomes possible to characterize the dependencies and interdependencies along with the consequences of potential disruptions and threats and to develop and implement plans to eliminate or temper risks.

Identification, Detection, and Analysis

It is critical to enact steps as soon as possible to detect, verify, investigate, and analyze an incident. This will promote and enable an effective containment and eradication strategy. After the confirmation of an incident, resources, including vendor services if, when and where needed, to investigate the scope, impact and response will be assigned as needed. The detection and analysis phases determine the source of the incident, which provides a direction for the steps and methods needed to collect and preserve the evidence.

Coordination between the Information Security Office, identified UMIT departments and the affected college/department is imperative to ensure verification of an incident and to prevent the alteration of data needed for further investigation.

Detection and Analysis

The information security office, along with appropriate UMIT units, will work with the affected college/department to quickly analyze, validate perform an initial assessment to determine the scope of the incident. The initial assessment for determining the scope may include networks, systems, applications, data and users who/what is affected; what and how the incident originated and how it is occurring (e.g., the type and kind of tools and attack methods used and what vulnerabilities are being exploited). The analysis must provide enough information for the teams to prioritize subsequent activities, such as containment and a deeper analysis and investigation of the incident.

After confirmation and validation of the incident, the information security office and related UMIT departments will identify and assign individual(s) from various areas to lead and coordinate the investigation. The information security office and the department of infrastructure will appoint an Incident Response Manager (IRM). The IRM will lead the incident response process serving as the point of contact for all matters relating to the incident, and is responsible for coordinating the collection of the data required for documenting the investigation and gathering evidence.

In certain situations, federal, state, or local law enforcement may be involved in an incident investigation.

Interdepartmental Cooperation Guidelines

University personnel who are alerted to a threat from an internal or external source must notify the information security office.

If the threat is associated with systems and machines not managed by UMIT, the system administrator, and the business owner of record are responsible for containing and remediating the threat. The business owner and system administrator must adhere to all guidance and direction provided by the information security office.

Through various security appliances and tools, the information security office and/or the security operations center or other UMIT departments may also detect a threat. They will notify the information security office who will alert the system administration and the business owner of record.

All incidents that occur in colleges/departments who manage their own information technology must be remediated by the college's/department's IT staff with the support of the information security office, and if necessary, UMIT departments, and/or the CIRT.

Incident Categorization, Classification, and CIRT Activation

The incident type and impact will determine the level of response required. The information security office will work with colleges/departments to determine the appropriate response for each confirmed incident. The general steps required for incident categorization and classification are:

1. Type of incident, security objective (Confidentiality, Integrity, and Availability) and impact.
2. Classify the incident as a local or enterprise incident.
3. Prioritize how the incident is handled based on the UMIT Incident Response Classification Matrix.
4. When necessary, activate the CIRT.
5. Report the incident to the appropriate UM personnel and, when required, to external organizations.

After an incident is classified, it is important to categorize the incident as a local or enterprise event.

Local events are the most common type of incident observed at the University of Miami. They represent a risk to University systems, networks, and data, but are confined to a single or a small number of department systems or a small number of data records as determined by federal and state regulations and industry standards. Identified local events will be contained and eradicated through coordinated efforts between the information security office and the affected departments. Local events are the most common type of attack observed at the University of Miami.

Enterprise events are rare, but have a large and often serious impact and often affect the campus as a whole. Enterprise issues may require the activation of the CIRT. CIRT team members who are subject matter expects will be drawn and leveraged from departments across the University to protect the University assets during the incident response process.

When multiple incidents occur simultaneously, the most serious or highest potential impact incidents must be handled first.

CIRT Activation

The CISO under the guidance of the Vice President and CIO and or the CIRT Governance Team has the authority to activate the CIRT. The CIRT (Cyber Incident Response Team) will be activated if a cyber incident has been confirmed to be affecting University IT resources at an enterprise or multi-department level, or if the data affected is governed by federal and state legislation and when the evidence warrants, departmental and individual incidents may be escalated to an enterprise level. If, when and where needed, external vendors will be used to assist the CIRT during the incident response phase.

Communications Plan
Communications processes occur throughout the incident response phases and involve the initial reporting of the incident to relevant authorities, as well as ongoing communications with those impacted.

A communications plan is required when dealing with a confirmed cyber incident. A good communications plan will help limit confusion, create focus, and increase responsiveness by sharing action plans, updating University stakeholders, and providing transparency throughout the process. The plan should identify the stakeholders, those authorized to speak about the incident, the communication channels and schedule, as well as procedures for notifying external organizations that are directly involved in the incident.

A communications plan must be developed whenever a breach of PII (Personally Identifiable Information) or ePHI (electronic Personal Health Information) has been confirmed.

Recommended elements for communications plans include:

- Identification of those authorized to speak about the incident to University stakeholders and the media.
- Clear protocols for message approval.
- Identification of channels for both internal and external stakeholders.
- Planned frequency of communications between internal and external stakeholders.
- Notification procedures for external organizations directly involved in the incident, e.g., consultants hired to assist with the investigation.

Containment, Eradication, and Recovery –

Containment

To limit the scope and magnitude of the attack, containment procedures must be implemented. A vulnerability in a particular software/computer architecture can be exploited quickly. Goals for containment include preventing data from leaving the network through the affected machines and preventing the attacker from causing further damage to UMIT assets.

All activities must be coordinated with UMIT and where needed, the business owner, and system administrator/IT technician. Recommended actions include:

- After required and appropriate containment, and only upon direction from the IRM or the CISO, the system administrator/IT technician can proceed to repair the system as needed to return to normal business operations. Failing to follow direction from the IRM or CISO can lead to corruption and/or deletion of evidence.
- Consulting, guidance, and recommendations will be provided by the CISO and UMIT (when needed) to the system administrator/IT technician during the remediation process.
- Where necessary, the CISO will deploy a small team comprised of UMIT members of the information security office, the security operations center, other UMIT departments, or an external vendor, as needed who have the appropriate expertise to the site for consultation and assistance.

- The system administrator and business owner are responsible for adhering to and following the incident procedure including all direction and guidance provided by the CISO and UMIT.

Determine risk of continued operation:

- How, why, and where is the system used? If it is a determined to be a system critical for operations, determine:
    - Does it provide a function related to student services, personnel services, health services, patient care?
    - Is it required for continued business functions of the University or U Health?
    - Is it used for PCI (payment card transactions) related functions?
- Is the system managed by UMIT, the college, department, or vendor?
- Can the system be removed from the network without affecting its operations/purpose?
    - If the compromised system threatens the integrity of the network or systems connected to the network, it must be removed from the network as quickly as possible.
    - If allowed to remain on the network, it is recommended to implement change control processes where appropriate such as changing all user and system credentials on the affected system(s) and attempting to isolate from other systems.
- After determining the severity of the incident, the purpose and criticality of the machine and the importance of restoring operations as quickly as possible, the CISO will make a recommendation to the business owner and system administrator/IT technician regarding whether the affected machine will remain online.
- Where needed and necessary, obtain a forensic image of the compromised system along with all relevant logs The CISO will determine if the forensics process needs to be implemented. All forensic processes will follow a specific procedure and can only be conducted by trained and qualified UMIT staff.

Eradication

Eradication is the removal of malicious code, accounts, or inappropriate access and includes remediating vulnerabilities that may have been the root cause of the compromise. Note: For complete remediation, a complete reinstallation of the operating system and applications is strongly recommended.

The general steps involved in the eradication phase of incident response are to:

- Identify and mitigate all exploited vulnerabilities.
- Remove the malware, inappropriate materials, and other artifacts that were cause of the incident.
- If additional hosts are discovered to be compromised/infected, repeat the detection and analysis steps to identify all affected systems then proceed with containment and eradication.
- Reinstall the operating system, apply patches and updates, reinstall applications, and apply known patches. Note: dependent on the need and criticality, of the systems, it may only be possible to clean and patch the systems. Extra care must be taken to ensure the system is clean and patched and is no longer vulnerable. If the system becomes re-infected, then the CISO or IRM will determine it is necessary to re-image the system.

Recovery

This phase allows business processes affected by the incident to recover and resume operations. Recovery can start after the incident has been contained and eradicated.

General recovery steps include:

1. Reinstall and patch the OS and applications. Change all user and system credentials. Request the ISO to run a vulnerability scan to validate the machine is compliant with policy.
2. Restore data to the system.
3. Return affected system(s) to an operationally ready state.
4. Confirm that the affected system(s) are functioning normally.
5. If necessary, implement additional monitoring to look for future related Post-Incident Activity.

Incident Closure

Documentation of a cyber incident and the steps taken to mitigate issues offers an opportunity to improve incident response processes and identify recurring issues. Most local issues can be properly documented using the University's UService Help Desk ticket system.

Certain cyber incidents, when their impact warrants, require formal, thorough documentation. The CISO will identify those incidents that need such documentation. An example would be a system that has been compromised and it was suspected that protected data was compromised. Note: A final report and documentation is required for all enterprise level incidents.

Final reports document the incident and include specific information and statistics related to the incident. The final report is intended to preserve and expand knowledge. The CISO, in partnership with the CIRT team, will produce the report.

The final report is to the VP for IT/CIO and stakeholders as appropriate. A post-incident meeting is mandatory for enterprise incidents and is recommended for other types of incidents.

Appendix A: University of Miami Incident Response Classification Matrix

Classification Level (3=Most Severe)	Typical Characteristics	Impact	Response	Activate CIRT
High	Attacks against University servers or attacks against network infrastructure. Network disruption for a large segment of the UM population	An enterprise-wide attack involving multiple departments requiring local and enterprise administrator support from the affected departments.	CIRT directs, response coordinated by the CISO. UMIT senior management, college/department system administrators/IT staff involved. If necessary, legal counsel, the HIPAA Privacy and Security Officer law enforcement involvement	Yes
High	Affects data or services for a group of individuals and threatens protected data, or involves accounts with elevated privileges with potential threat to sensitive data.	An enterprise-wide incident. CaneID (PeopleSoft), Workday, Active Directory, EPIC, LMS (learning management system), O365, Google, Box, or any other system that handles and stores protected data administrator account compromise or compromise on vendor side, or system compromise due to lack of management and maintenance.	Response coordinated with CISO, UMIT, the business owner and the local system administrators and IT staff. If necessary, legal counsel, the HIPAA Privacy and Security Officer and/or law enforcement.	Yes
Medium	Affects data or services of a single individual or group of individuals, but involves significant amounts of protected data.	Faculty or administrative desktop/electronic devices such as a tablet or cell phone, or shared folder with University defined protected data, which is compromised through misuse/ unauthorized access, and/or physical theft of computer/electronic devices.	Response coordinated with CISO, UMIT, the business owner and the local system administrators and IT staff. If necessary, legal counsel, the HIPAA Privacy and Security Officer and/or law enforcement.	Advised
Low	Affects data or services of a group of individuals with no sensitive data involved.	Compromise of an account with shared folder or shared account access.	CISO, UMIT, and – if unmanaged – business owner and local IT staff notified. Event logged and monitored. Information security office to perform forensics.	No
Low	Affects data or services of a single individual with no sensitive data beyond their own involved; focus is on correction and/or recovery and education/future prevention.	Compromised faculty/staff machine or account such as Box, Google, One Drive, O365, etc. with not University defined protected data.		No
N/A	Occurrences of minor or undetermined focus, origin and or effect for which there is no practical follow-up.			No

Appendix B: UM Cyber Incident Response Team Organization Chart

CIRT Organizational Chart