University of Oklahoma

Security Incident Management Policy

Policy ID:	009
Version:	1.0
Policy Owner:	Chief Information Officer (CIO)
Policy Approver:	President, University of Oklahoma

PURPOSE

The University must ensure cybersecurity incidents are handled in a consistent manner to protect the confidentiality, integrity, and availability of University data and systems. Security incidents must be reported promptly through the proper University and/or Department Information Technology channels and resolved by designated professionals in a manner that is consistent with University policies, applicable laws, and this plan.

The handling of a security incident must protect the University, the data, the system and any persons affected by the incident. Security incident management must:

1. Identify the incident.
2. Contain the incident.
3. Eradicate the incident.
4. Recover from the incident.

This Security Incident Management Policy establishes the standardized process for identifying, containing, eradicating, and recovering from security incident. It establishes the basic language to discuss such incidents, identifies roles and responsibilities involved in responding to and recovering from these incidents, and provides a playbook for handling these events from the time an event is detected to the post incident report and event closing.

SCOPE

This policy applies to all University of Oklahoma Staff or Faculty, University of Oklahoma contractors, and their associated contractors, as well as temporary workers and those given access to IT systems and/or services. All access locations, including on-site and remote/off-site locations. Exclusions – None.

DEFINITIONS

Cybersecurity Incident is a violation or Imminent Threat of violation of computer security policies, standard security practices, confidentiality, integrity, availability, possession or control, authenticity, utility, or safety of information systems. It may also mean the loss of data through theft or device misplacement or loss, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction. A Cybersecurity Incident that compromises the privacy or security of Protected Health Information (PHI) or Personally Identifiable Information (PII) is treated as a possible Breach.

The University of Oklahoma has named and defined the following types of cybersecurity incidents:

> **Phishing** is a type of cyberattack that uses email, phone or text to entice individuals into providing personal or sensitive information, ranging from passwords, credit card information

and social security numbers to details about a person or organization. Attackers pose as legitimate representatives to gain this information, which is then used to access accounts or systems, often leading to identity theft or significant financial loss. MITRE ATT&CK further categorizes three subtechniques of targeted phishing attacks: spearphishing attachment, spearphishing link, or spearphishing via service.

Malware/Ransomware is an umbrella term for various types of malicious programs that are delivered and installed on end-user systems and servers. These types of malware programs fall into commonly referred to categories such as Backdoors, Banking Trojans, Keyloggers, Stealers, remote access tools, and downloaders. More sophisticated types of malware will combine the capabilities of more than one of the above, and we frequently see malware employing evasion tactics to avoid detection. Ransomware is a type of malware that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever.

Account Compromise incidents occur when an individual gains logical or physical access without permission to an OU network, system, application, data or other resource.

External Threat Actor incidents are typically conducted by individuals without a relationship to OU (Student, Faculty, Staff, Vendor, Affiliate, etc.) and employ various methods including phishing attacks, ransomware, malware and other tactics to identify points of entry into OU networks, systems, data and resources.

Data Loss Prevention incidents occur through data breaches, exfiltration, or unwanted destruction of sensitive data activities.

Lost or Stolen Device incidents occur when information goes missing, whether through misplacement or malice. must be reported to ensure OU is meeting its obligations to report security incidents in a timely manner to prevent unauthorized access, disclosure, or modification of OU records lost or stolen.

Internal Threat Actor incidents include any unapproved or malicious use of University resources occur. Internal Threat Actors may include, but are not limited to: employees, vendors or contractors, students, staff, faculty, affiliates or other users with a legitimate association to OU.

Imminent Threat is a situation in which there is a factual basis for believing that a specific incident is about to occur; for example, when a warning is issued of an exploit that is rapidly spreading across the Internet and the University determines that its information or systems are vulnerable to the exploit.

Breach is any accidental or intentional disclosure of regulated or otherwise confidential data. A breach is the acquisition, access, use, or disclosure of confidential data in a manner not permitted by law or obligations that compromises the security or privacy of the data.

ROLES & RESPONSIBILITIES

Everyone is responsible for security.

1. Anyone suspecting or discovering a security incident related to the University of Oklahoma, must notify the University of Oklahoma IT Security team as soon as possible or within one business day. The University of Oklahoma IT Security team will be responsible for notifying the appropriate people and investigating the incident.
2. The person reporting the incident should document and report any available relevant

information about the incident, including but not limited to dates, times, person/assets involved, serial numbers, MAC Address, and IP Addresses.

3. Situations which are suspected to be crimes must be reported immediately to the appropriate law enforcement agencies by the person who possesses first-hand knowledge of the facts or circumstances related to a suspected crime. OU students, faculty, and staff on campus must report crimes to the University Policy Department.
4. The University of Oklahoma Chief Information Officer (CIO), the Chief Information Security Officer (CISO), and the IT Security teams act as the Cybersecurity Incident Response Team (CSIRT) for all security-related functions.
5. The CSIRT will be responsible for assigning resources to work on specific tasks of the incident response process and will coordinate the overall response. All people involved in the incident response and recovery are responsible for providing required information to CSIRT.

IT Security Operations Responsibilities

The functions performed by Security Operations are essential to the CSIRT and include:

- Designate an Incident Commander upon activation of the Plan
- Maintenance of the Cybersecurity Incident Response Playbook
- Identification and Reporting of New Threats

IT Governance, Risk, and Compliance (OU IT GRC) Responsibilities

The functions performed by Governance, Risk and Compliance are essential to maintaining the Plan in a consistent state of readiness and include:

- Distribution and maintenance of the Cybersecurity Incident Response Plan
- Maintenance of the Cybersecurity Incident Response Playbook
- Exercising the Cybersecurity Incident Response Plan
- Working with the Office of Risk Management in reporting Cybersecurity Incidents to cybersecurity insurance broker
- Facilitating Post Incident Reviews

IT Training, Education, and Awareness (TEA) Responsibilities

The functions performed by the Director, System Security Awareness and Training are essential to ensuring the University community is aware of their roles and responsibilities as it pertains Cybersecurity Incidents and include:

- Provide Cybersecurity Incident Reporting procedure training to University Personnel through in-person training, learning management system content, and periodic security reminders
- Provide role-based training to those with a defined role or responsibility in the Cybersecurity Incident Response Plan

Information System Owner Responsibilities

Information System Owners are senior university administrators accountable for the creation and maintenance of information systems relied upon for key university operations. This individual(s) is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario. The functions performed by an Information System Owner include:

- Respond immediately to reports of cybersecurity incidents
- Provide support to Department and Central IT personnel to ensure containment occurs as needed

Information System Administrator Responsibilities

The individual(s) responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. The functions performed by the Department IT Personnel include:

- Respond immediately to reports of cybersecurity incidents
- Provide swift action to notify users and IT Owners of planned containment activities
- Participate in and accept, respond, and complete tasks assigned by the Incident Commander
- Serve as the system Subject Matter Expert to the Incident Commander and provide system-level support to the Incident Commander for the duration of the incident.
- Facilitate conversations with Information System Owners and/or vendors to complete assigned incident response tasks, as assigned by the Incident Commander

POLICY STATEMENTS

PR.IP-9 INCIDENT RESPONSE PLAN

The Chief Information Security Officer has responsibility for documenting the incident response plan. The Cybersecurity Incident Response Plan is confidential. Any distribution of the Plan must be approved by the Chief Information Security Officer.

The Plan contains detailed information about the University of Oklahoma's cybersecurity incident response strategy, personnel, locations, and inventories which are not for general publication to those outside of the response team.

The Plan must be reviewed and revised by the Chief Information Security Officer, at least annually, and more often as necessary.

PR.IP-9 INCIDENT REPORTING

Once a cybersecurity event has been reported to IT, the IT reporting party must create an incident record is created in the IT System of Record, and assigned to OU IT Security Operations. IT should gather as much information and evidence as possible when reporting 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.
- The name of the reporting person(s)
- Date/time of the report
- Contact information for the reporting person(s)
- The nature of the cybersecurity incident
- Unique identifiers for the Information Systems involved in the cybersecurity incident
- Location or source of cybersecurity incident

Reported incidents become security incidents only after they have been received and evaluated by the CSIRT.

PR.IP-9 INCIDENT RESPONSE

In order to facilitate the accurate and productive response, all security incidents must be assessed and prioritized by the CSIRT at their onset. As the security incident progresses, its classification may be reevaluated and changed as necessary to ensure proper handling. If a security incident falls under multiple priorities, the highest priority will generally dictate the course of the incident response efforts.

Incidents will be prioritized in accordance with the Security Incident Prioritization Standard.

PR.IP-9 INCIDENT NOTIFICATION

The CSIRT reviews the known details of the incident and determines the incident's initial risk classification according to the Impact Matrix below, and has the responsibility to inform other departments about an incident may have an effect on the on their systems.

Incidents classified as Significant, Serious, or Severe require notification to parties outside of OU IT and warrant activation of Cybersecurity Incident Response Plan. In the event of plan activation, the Incident Commander must activate the CISO and Director for OU IT GRC. The CISO will coordinate and facilitate notifications, if necessary, to the CIO.

OU IT GRC is responsible for communication information about the Incident to appropriate personnel and for maintaining contact with key stakeholders, for the purpose of update and coordination, for the duration of the Incident.

All incidents involving Protected Health Information must be communicated to the OU HIPAA Security Officer immediately. The HIPAA Security Officer will determine if communication/notification to the Office for Civil Rights is appropriate.

All incidents involving OU Health Information must be communicated to the OU Health Chief Information Security Officer and the Director for IT Security.

At any point in the investigation, the CSIRT may determine, based on the type and classification of the incident and the specific details of the impact, that it is necessary to involve other OU departments to participate or assist in the investigation and subsequent remediation of the incident. The OU IT GRC, if necessary, will coordinate and facilitate notifications to other departments.

PRIORITY	EXAMPLES	NOTIFICATION
Low	• May cause minor financial loss (< $5,000) • Risk impacts a single user. • Requires only minimal effort to complete corrective actions and continue or resume operations (less than 2 hours to complete). • Results in non-compliance with a University Policy, Standard, or Procedure.	• Communicate with user and Mission Support or department IT contacts via email of phone call.
Moderate	• May cause moderate financial loss (>$25,000). • Risk impacts a single department. • Requires a moderate effort to complete corrective actions and continue to resume operations (less than 4 hours to complete). • Results in non-compliance with a State of Oklahoma Policy, Standard, or Procedure.	• Communicate with impacted users, department IT or Mission Support contacts via phone or email. • Send Post Incident Summary Report to Dean, Director, or Department Head.
Significant	• May cause significant financial loss (>$50,000). • Requires a significant effort to complete corrective actions and continue or resume operations (less than 6 hours to complete).	• Communicate with impacted users, department IT or Mission Support contacts via phone or email.

	• Risk impacts multiple departments or entire campus. • May require recovery in an alternate site environment. • Will result in a cybersecurity insurance policy claim.	• Send Post Incident Summary Report to Dean, Director, or Department Head. • Optional campus-wide email alert.
Serious	• Requires a serious effort to complete corrective actions and conintue or resume operations (greater than 6 hours to complet) or may require recovery in an alternate site environment. • May cause serious financial loss (>$100,000). • Risk impacts more than one campus. • May require recovery in an alternate site environment. • Will result in a cybersecurity insurance policy claim. • Will result in a reportable breach or incident to a regulatory body.	• Communicate with department IT or Mission Support contacts via Slack and email. • Send campus-wide email outlining how to avoid the risk and what corrective actions to take if necessary. • Send Post Incident Summary Report to Dean, Director, or Department Head. • Notify appropriate compliance offices.
Severe	• Requires a serious effort to complete correction actions and continue or resume operations (greater than 8 hours to complete) or will require recovery in an alternate site environment. • May cause serious financial loss (>$150,000). • Risk impacts all campuses. • May require recovery in an alternate site environment. • Will result in a cybersecurity insurance policy claim. • Will result in a reportable breach or incident to a regulatory body.	• Communicate with department IT or Mission Support contacts via Slack and email. • Send system-wide email outlining how to avoid the risk and what corrective actions to take if necessary. • Send Post Incident Summary Report to Dean, Director, or Department Head. • Notify appropriate compliance offices.

PR.IP-9 RELEASE OF INFORMATION

All releases of information about a security incident must be authorized by CSIRT or designated by the University of Oklahoma CIO and the Office of Legal Counsel. All requests for press releases must be forwarded to the Office of Legal Counsel.

Incident specific information, such as accounts involved, programs or system names, must not be provided to any callers claiming to be a security officer from another site. All suspicious requests for information must be forwarded to the CSIRT. If there is any doubt about whether you can release a specific piece of information, contact the CSIRT.

PR.IP-9 INCIDENT CONTAINMENT

The goal of Cybersecurity Incident containment is to reduce and contain the scope of an incident and

ensure that Information Systems are returned to service as quickly as possible. Rapid response and containment is balanced by the requirement to collect and preserve evidence in a manner consistent with the requirements of rules 26-34 of the Federal Rules of Civil Discovery, and to abide by legal and Administrative requirements for documentation and chain of custody.

In support of the OU Acceptable Use and Cybersecurity Policies, OU IT reserves the right to network contain systems or disable compromised accounts, including essential or critical service accounts, to contain an incident. The CSIRT, CISO, and CIO, if necessary, will make every reasonable effort to contact IT Administrators and Owners prior to containment activities.

In carrying out this responsibility, the CSIRT will ensure that important operational decisions are elevated to the appropriate levels to protect the fundamental interests of the University and others impacted by the incident.

PR.IP-9 INCIDENT REMEDIATION AND RECOVERY

Remediation is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained. Post-Incident Reports will be completed at this stage by OU IT GRC and reviewed with the department or unit incident response contacts.

The Cybersecurity Incident Response Playbook provides a checklist of major steps to be performed during a cybersecurity incident. The Playbook does not dictate the exact sequence of steps that should always be followed and should be used as a guide for those involved.

The CSIRT will provide a resolution alert once incidents are confirmed to be remediated and/or recovered and facilitate a final incident summary and briefing.

PR.IP-9 INCIDENT DOCUMENTATION AND CLOSURE

A log must be kept for all security incidents under investigation. The information must be logged in an approved location or tool that cannot be altered by unauthorized personnel. The following information must be recorded:

1. Dates and times when incident-related events were discovered or occurred
2. Security incident contact information
3. All assets that have been affected
4. Evidence related to the incident

A security incident report should be written by CSIRT and distributed to all appropriate personnel, and should consider the following, but not limited to:

- Challenges encountered during incident response activities
- Lessons learned during the incident
- Outstanding risks identified during the course of the incident and recommend risk mitigation strategies to be presented to the department or unit contacts.
- Missing policy, standard, or procedure documentation needed to respond to future incidents

All on-line copies of infected files, worm code, etc., should be removed from the system(s). A set of recommendations must be presented to the appropriate management levels.

Upon completion of the incident documentation, the CSIRT will provide authorization to close a security incident. Security incident documentation must be retained for a minimum of one (1) year. Security incident documentation, when involving Category A – Healthcare Information, must be

retained for a minimum of six (6) years.

REFERENCES

- National Institute of Standards and Technology Cybersecurity Framework (CSF), PR.IP-9
- National Institute of Standards and Technology Special Publication 800-171, Controlled Unclassified Information, 3.6.1, 3.6.2, 3.6.3
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Security Rule, §164.308(a)(6), §164.308(a)(7), §164.308(a)(7)(ii)(D), §164.310(a)(2)(i), §164.312(a)(2)(ii)
- General Data Protection Regulation (GDPR)
- Payment Card Industry (PCI) Data Security Standards
- Gramm-Leach-Bliley Act (GLBA)
- Family Education Rights and Protection Act (FERPA)
- National Institute of Standards and Technology Special Publication 800-61, Computer Security Incident Handling Guide

ENFORCEMENT AND COMPLIANCE

Failure to comply with this Policy or other applicable laws, policies, and regulations may result in the limitation, suspension, or revocation of user privileges and may further subject the user to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, and applicable laws. This Policy is approved and enforced by the OU Chief Information Officer (CIO). Internal Audit, or other departments, may periodically assess compliance with this policy and may report violations to the Board of Regents.

IT EXCEPTIONS

The CIO acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this Policy. Such instances must be documented following the IT Policy and Standards exception process, and may require the approval of the Chief Information Officer, Chief Information Security Officer, and/or the Data Owner depending upon the level or risk introduced with the exception.

Table 1 - Revision History

Revision Date	Version	Revised By	Changes Made
02/04/2020	0.1	OU IT, April Dickson	Baseline Version
01/03/2022	0.2	OU IT, April Dickson	Added the following definitions: The University of Oklahoma has named and defined the following types of cybersecurity incidents: Phishing is a type of cyberattack that uses email, phone or text to entice individuals into providing personal or sensitive information, ranging from passwords, credit card information and social security numbers to details about a person or organization. Attackers pose as legitimate representatives to gain this information, which is then used to access accounts or systems, often leading to identity theft or significant financial loss. MITRE ATT&CK further categorizes three subtechniques of targeted phishing attacks: spearphishing attachment, spearphishing link, or spearphishing via service.
01/03/2022	0.2	OU IT, April Dickson	Malware/Ransomware is an umbrella term for various types of malicious programs that are delivered and installed on end-user systems and servers. These types of malware programs fall into commonly referred to categories such as Backdoors, Banking Trojans, Keyloggers, Stealers, remote access tools, and downloaders. More sophisticated types of malware will combine the capabilities of more than one of the above, and we frequently see malware employing evasion tactics to avoid detection. Ransomware is a type of malware that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever.

01/03/2022	0.2	OU IT, April Dickson	Account Compromise incidents occur when an individual gains logical or physical access without permission to an OU network, system, application, data or other resource.
01/03/2022	0.2	OU IT, April Dickson	External Threat Actor incidents are typically conducted by individuals without a relationship to OU (Student, Faculty, Staff, Vendor, Affiliate, etc.) and employ various methods including phishing attacks, ransomware, malware and other tactics to identify points of entry into OU networks, systems, data and resources.
01/03/2022	0.2	OU IT, April Dickson	Data Loss Prevention incidents occur through data breaches, exfiltration, or unwanted destruction of sensitive data activities.
01/03/2022	0.2	OU IT, April Dickson	Lost or Stolen Device incidents occur when information goes missing, whether through misplacement or malice. must be reported to ensure OU is meeting its obligations to report security incidents in a timely manner to prevent unauthorized access, disclosure, or modification of OU records lost or stolen.
01/03/2022	0.2	OU IT, April Dickson	Internal Threat Actor incidents include any unapproved or malicious use of University resources occur. Internal Threat Actors may include, but are not limited to: employees, vendors or contractors, students, staff, faculty, affiliates or other users with a legitimate association to OU.
01/03/2022	0.2	OU IT, April Dickson	Revised statement. The Plan must be reviewed and revised by the Chief Information Security Officer, at least annually, and more often as necessary.
01/03/2022	0.2	OU IT, April Dickson	Revised statement. The CSIRT reviews the known details of the incident and determines the incident's initial risk classification according to the Impact Matrix below, and has the responsibility to inform other departments about an incident may have an effect on the on their systems.
01/03/2022	0.2	OU IT, April Dickson	Removed bold font. Revised statement. In support of the OU Acceptable Use and Cybersecurity Policies, OU IT reserves the right to network contain systems or disable compromised accounts, including essential or critical service accounts, to contain an incident. The CSIRT, CISO, and CIO, if necessary, will make every reasonable effort to contact IT Administrators and Owners prior to containment activities.

01/03/2022	0.2	OU IT, April Dickson	Revised roles and responsibilities. IT Security Operations Responsibilities IT Governance, Risk, and Compliance (OU IT GRC) Responsibilities IT Training, Education, and Awareness (TEA) Responsibilities Information System Owner Responsibilities Information System Administrator Responsibilities
			Added immediate notification to HIPAA Security Officer.
			Added the following statement. Security incident documentation must be retained for a minimum of one (1) year. Security incident documentation, when involving Category A – Healthcare Information, must be retained for a minimum of six (6) years.

Figure 1 - Approval History

Version	Approval Date	Approved by:
1.0	02/08/2022	Information Security Review Board
1.0	02/08/2022	Security Governance Advisory Council
1.0	03/31/2022	University President

Figure 2 - Review History

Version	Review Date	Reviewed by:
0.1	12/12/2021	OU HIPAA Security Officer
0.1	12/12/2021	OU Internal Audit/Eminere Group