Mississippi State University Cybersecurity Incident Response Plan (CIRP)

Version	Date	Purpose of Revision
Original (V1.0)		Initial document
V2.0 DRAFT	April 2024	Added playbooks, modified previous content, added RACI matrix and escalation path, added overall response plan, updated classification, updated contacts

Table of Contents

1.0 Introduction

Information security/cybersecurity incidents are a major concern for various institutions and organizations, especially as new types of security-related incidents continually emerge into the threat landscape. Major universities, such as Mississippi State University, are in a unique position with large amounts of educational, medical, financial, and other critical information. Mississippi State University (MSU, also referred to as "the

University" throughout the document) is also subject to numerous federal and state laws and regulations regarding the protection of data.

The effective resolution of cybersecurity incidents is critical to the usability of the campus information technology infrastructure. Security incidents that involve sensitive information add layers of complexity and importance to those security incidents as well. Having a clear and successful incident response plan (IRP) is essential to resolve cybersecurity incidents in an efficient and effective manner to reduce costs and damages that can incur from a cybersecurity incident.

This document provides requirements, essential information, and procedures for effectively resolving cybersecurity incidents so that the University can achieve its goal of providing education and support to further the land-grant mission of Mississippi State University.

2.0 Purpose

This CIRP provides the plan for Mississippi State University's incident response team and other stakeholders for responding to cybersecurity incidents.

This plan is designed to:

- Describe the requirements and expectations of cybersecurity incident responses.
- Establish the roles and responsibilities of those involved with incident responses.
- Define the parameters for declaring, categorizing, and triaging incidents.
- Establish the incident response lifecycle and process specific to the University.
- Define and create clear communication channels used during a security incident.

An effective, efficient, and well-designed plan greatly improves the quality of response to cybersecurity incidents that will greatly benefit the University. The goal of this plan is to:

- Reduce costs associated with cybersecurity incidents (such as reducing fines associated with information lost by reducing/minimizing the amount of information lost, reducing the amount of work needed by outside consultants by being more self-sufficient at responding to incidents and limiting damage done by an incident, reduce the amount of equipment needing replacement from a compromise by limiting the damage of an incident, etc.)
- Improve productivity for employees and students across the University (such as reducing the time to repair critical infrastructure and perform productive work in a shorter time)
- Avoid reputational harm associated with cybersecurity incidents by reducing the amount of information lost from an incident to maintain capability and competitive edge to house sensitive information (such as student health data, government program information, etc.)
- Limit theft of sensitive information and reduce the impact of a cybersecurity incident (such as limiting the number of students impacted by a security incident, etc.).

- Improve information security defenses from lessons learned in response to past incidents and close potential threats (such as reducing time to remedy an incident by increasing efficiency in communication channels that came to light during an incident).

The goals and objectives specified above are to align with the goals and objectives within the University's Information Security Plan (ISP).

3.0 Scope

Mississippi State University's IRP applies to those entities within the scope of the University's Information Security Plan (ISP). Units may adopt and tailor this IRP to fit their unique requirements but shall have their IRP approved by the same governing body that approves Units' ISPs (as described in the University's ISP).

Incidents that involve threats to personal safety, physical property or other illegal activities should be immediately reported to the University Police department.

Per Mississippi Code Annotated § 75-24-29, that the University is required to follow, includes the terms that provide the basis of scoping information for this document:

- "Breach of security" means the unauthorized acquisition of electronic files, media, databases or computerized data containing personal information that has not been secured via encryption or any other method or technology that renders the personal information unreadable or unusable.
- "Personal information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements:
    - Social security number;
    - Driver's license number or state identification card number;
    - An account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; "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.
- "Affected individual" means any individual who is a resident of this state whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security.

4.0 Incident Classification

The incidents at the University will be classified based on a variety of factors and characteristics of the incident. The following table will serve as a guide in classifying incidents and their required response as described throughout the rest of the document.

To use the table, an incident will be given a severity tier based on its "Data Class" as priority, but then evaluated and assigned a tier based on the majority of its characteristics within the "Business Impact" and "Technical Attributes" that align with that tier.

Table 1. Incident Severity Tiers for Mississippi State University.

Severity	Business Impact			Technical Attributes	
Tier	Prevalence	Scope	Reputation	Data Class	Disruption
Emergency	University-wide	Critical enterprise system (e.g., Banner)	Global or National Media	High Risk (e.g.,CUI, PII, or PHI)	>48 hrs of down-time
High	Multiple departments	Shared system (e.g., department server)	Regional Media	Moderate Risk	Between 4 hrs and 48 hrs of down-time
Low	Fewer than 10 users/systems	Limited user system (e.g., staff laptop)	No to Low Local Media	Low Risk	Less than 4 hrs of down-time

Note: CUI – Controlled Unclassified Information
PII – Personally Identifiable Information
PHI – Protected Health Information

5.0 Procedure

The University's overall incident response procedure consists of three phases:

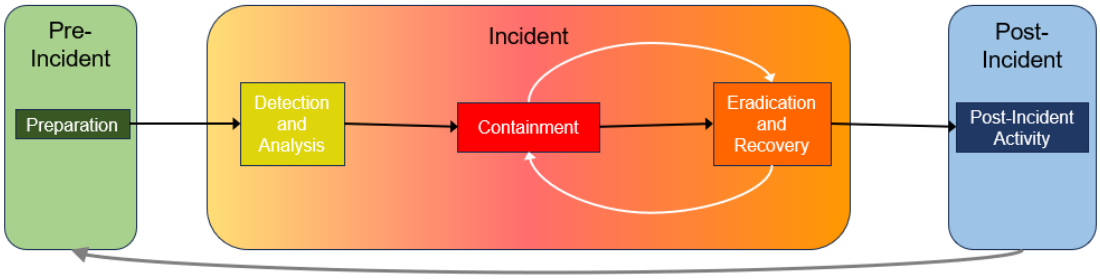
- Pre-incident
- Incident
- Post-incident

The three phases map to the steps of the NIST SP 800-61 Rev2 and the Cybersecurity Incident and Vulnerability Response Playbooks by the Cybersecurity and Infrastructure Security Agency (CISA) incident response process that make up the more detailed steps of the University incident response:

- Preparation
- Detection and Analysis
- Containment
- Eradication and Recovery
- Post-incident Activity

The figure below provides how the steps fit within the three phases of the incident response procedure.

Figure 1. Three phases and five steps of Mississippi State University's incident response plan.



5.1 Pre-incident

The “Pre-incident” phase focuses on preparing for an incident by establishing an incident response plan that provides the capability of the University to respond to incidents and prevent incidents by securing systems, networks, and applications.

5.1.1 Preparation

The preparation of an incident should include various planning activities and gathering resources. One of the main focuses of this step is to establish multiple (separate and different) communication and coordination mechanisms in case of the failure of one mechanism during an incident. Another focus would be gathering incident analysis resources and mitigation software and hardware. Training the incident responders is also a major focus for the preparation step.

5.1.1.1 Facilities

There are various types of facilities that the response team can use but will use their designated workstation and/or building for meetings and conducting work for non-Emergency level incidents (as defined later in this document), unless otherwise specified by the Incident Manager (as defined later in this document) or through the guidance of law enforcement. Secure storage facilities for securing evidence and sensitive materials relating to the incident will be made available for the incident response team. These storage facilities include:

- MSU Microsoft M365 tenant (Teams)
- MSU ITS Local Storage
- MSU Team Dynamics IT Service Management (ITSM)

For Emergency level incidents, the University has a dedicated Emergency Operation Center (EOC) for central communication and coordination with enhanced features and capabilities, which include:

- Maroon Alert - Everbridge Mass notification environment for when on-campus resources are unavailable.

- The University has designated a primary EOC on campus, a secondary operations center on campus, and a second off-site alternate operations center.
- Further information about the EOC would be available from the University Emergency Manager at 662-325-4521 during a declared Emergency level incident.

5.1.1.2 Incident Resources

Incident responders would have available forensic tools and analysis from ITS. Incidents classified as High or Emergency could require third party vendor support. Mississippi State University has SpearTip on retainer for incident response (see Appendix D for contact information). Engaging a company for external forensic investigation may be preferred or required in some circumstances such as Payment Card Industry incidents.

5.1.1.3 Reporting Mechanisms

These reporting mechanisms are how users can submit/report a suspected incident (at least one mechanism should permit people to report incidents anonymously) for the University:

- Phone or email or visit ITS Service Desk: Service Desk Home (msstate.edu)
- Anonymous reporting: EthicsPoint - Mississippi State University

5.1.1.4 Cybersecurity Incident Response Team (CIRT) Roles and Responsibilities.

The CIRT is comprised of various individuals and departments that bring their own specialties and strengths to resolve cyber security incidents. These members of the incident response team have specific roles and responsibilities during incident response activities, and are described as the following:

- Incident Response Handler – employees within ITS, other Mississippi State University staff, or outside contractors who gather, preserve, and analyze evidence so that incident can be resolved. These individuals usually detect the first signs of an incident and initiate the incident response plan.
- Incident Manager – assigned to every incident; manages all aspects of the response, coordinates communication, and ensures escalations are properly made as appropriate; primary and centralized point-of-contact during the response; responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.
- Chief Information Security Officer (CISO) – holds ultimate responsibility for the execution of the technical aspects of incident response; oversees the CIRT, managing staff, and making high-level decisions throughout the response as needed; escalates incidents to stakeholders outside security,

communicating with and briefing leadership, and coordinating management-level decisions and actions.

- Office of General Counsel (OGC) (also called “Legal” throughout the document) – acts as liaison between the CISO and external law enforcement; provides guidance on the extent and form of all responses and disclosures to law enforcement and the public.
- Chief Information Officer (CIO) – focal point and responsible for campus-wide information technology organization (Information Technology Services (ITS)) and any issues; serves as liaison between the University and outside entities for information technology.
- Office of Research Compliance & Security (ORC&S) – provides support and training in the regulatory requirements for the conduct of scientific research for University faculty members, researchers, and students. ORC&S contains the research security officer that is the point of contact for Research Security issues in each department in the University, implement the University’s Research Security Program and policies, assist with export compliance, conduct security screenings, identify foreign travel concerns, identify malign foreign influence, identify insider risk concerns.
- Chief Technology Transformation Officer (CTTO) – provides leadership development and implementation for ITS’s technology improvement initiatives, while advising University leadership on plans and directions for these projects; serves as liaison with ITS and University leadership.
- Office of Strategic Communications – part of the Office of Public Affairs to provide leadership for strategic and crisis communications, news and media relations, and digital and social media content development including the University’s website.
- Executive Council – comprised of the University’s senior leadership and meet monthly to advise the president on official policies and procedures.
- Office of the Provost and Executive Vice President – oversee and coordinate the learning enterprise of the University; includes coordination of the delivery of quality undergraduate and graduate instruction, oversight of the faculty, and coordination of the academic programs in the various colleges and departments.
- President – head of the University, oversees all departments, and provides overall vision/guidance for the University; ultimately represents the University.

Contact information for the incident response team members and others within and outside of the University can be found in Appendix B for more information.

5.1.1.5 Escalation Path

Once Information Technology Services (ITS) is made aware of a potential incident, the Chief Information Security Officer (CISO) or designee will direct an initial investigation to collect and understand the basic facts of the incident. Based upon the investigation, the

incident will be classified, the appropriate members of the CIRT notified, and the CISO will assign an Incident Manager to the incident response.

The RACI (Responsible, Accountable, Consulted, Informed) matrix in Appendix I summarizes the involvement of the core incident response team members for incidents including a data breach.

Certain individuals and teams shall be notified of incidents based on incident severity. The escalation path table below (Table 2) defines who shall be notified at each severity tier. These escalations are cumulative so all individuals/teams at and below the severity tier level shall be notified of the incident. In the case where an incident evolves and the severity tier is updated as the investigation unfolds, all of the appropriate individuals/teams shall be notified as soon as possible.

To use the Escalation Path table, the individual/team will notify the individual/team directly to the right of themselves for that level of severity tier as the incident progresses and the severity tier potentially increases. For example, an "Emergency" severity incident will first be handled by the Service Desk, then be in communication with the Incident Manager (once one is assigned by the CISO). The Incident Manager will then inform the CISO of the escalation, then the CISO will notify the CIO, and then the CIO will notify Legal of the escalation. The Incident Manager will then notify the CTTO of the escalation of the incident and the CTTO will notify the Office of Strategic Communications if they deem it necessary.

Table 2. Escalation Path for Incident Response at Mississippi State University.

Severity Tier	**Low**	**High**					**Emergency**			
CIRT Member	Service Desk	Incident Manager	CISO	CIO	Legal	Additional Contacts Based on Incident Type (if required)	CTTO	Office of Strategic Communications	Provost	President

In addition to the notification path above, certain individuals/teams shall be notified based on certain attributes outside of the severity tier, as shown in the following table (Table 3). The procedure for notifying the individual/team will follow the same procedure for the escalation path table, but the type of incident is labeled to the left of the corresponding notification/escalation path.

Table 3. Additional Notification Requirements for Incidents.

Type of Incident	Escalation Path		
Breach of PII	Mississippi Department of Information Technology Services (MDITS)	Office of Compliance & Risk Management	Appropriate Executive Leadership
Breach of FERPA Information	University Registrar		
Breach of Payment and Credit Card Information	Office of Controller and Treasurer	Mississippi State University Acquiring Bank(s)	
Ransom Demand	Mississippi Department of Information Technology Services (MDITS)	Office of Compliance & Risk Management	Appropriate Executive Leadership
Breach of CUI/Research	Office of Research Compliance and Security	Appropriate Executive Leadership	
Breach of PHI	HIPAA Security Officer	Office of Compliance & Risk Management	Appropriate Executive Leadership

Depending on the severity and context of the incident, federal agencies (such as Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), etc.) and local law enforcement agencies (such as Mississippi State University Campus Police, Starkville Police, Mississippi Bureau of Investigation (MBI), etc.) will also be notified as determined by laws, regulations, and guidance from Legal and Incident Manager.

5.1.1.6 Training

Exercises involving simulated incidents are required to be conducted at least annually for each component of the incident response team. Combined exercises involving different levels and combinations of components of the incident response team shall be conducted at least every two years. Testing backups shall be conducted in accordance with the University's ISP.

Additional information on exercises can be found in NIST SP 800-84 and NIST SP 800-61 Rev2.

5.2 Incident

The "Incident" phase focuses on the activities that are performed during the active handling of the incident.

5.2.1 Detection and Analysis

Determining if an incident has occurred and, if so, assigning an appropriate type, scope, and magnitude of compromise within the affected environment. This activity also identifies what data, devices, and/or systems were damaged, accessed, and/or exposed as part of the incident. If the determination has concluded that an incident has occurred, the collection of logs, system images, and other artifacts occur during this activity along with notifying/mobilizing the incident response team.

5.2.1.1 Declare Incident

Incident response can be initiated by several types of events, including but not limited to:

- Automated detection systems or sensor alerts
- ITS Service Desk ticket submission
- Vendor report
- Internal or external organizational component incident report or situational awareness update
- Third-party reporting of network activity to known compromised infrastructure, detection of malicious code, loss of services, etc.
- Analytics or hunt teams that identify potentially malicious or otherwise unauthorized activity

Any of the previous events can initiate the incident response process (as described previously) through the declaration of the incident, where “declaration” refers to the identification of an incident and communications to ITS Security rather than formal declaration of a major incident as defined in applicable law and policy.

A copy of the CIRP Response Checklist Template will be initiated to provide a timeline and details of the steps taken of the response to the incident.

5.2.1.2 Determine Scope

A key component for incident response is determining the scope of the incident and the corresponding scope of the response/investigation to the incident. The main focus of this phase is to understand what has happened, what assets are affected, and the overall impact to classify the data and criticality of impacted assets. Check various assets (including devices and networks) for signs of compromise (analysis of the signs of compromise will occur in later steps, but the focus on this step is to identify which and how many assets are affected). These assets include, but are not limited to:

- Mapped or shared drives
- Cloud-based storage (OneDrive, O365, DropBox, Google Drive, etc.)
- Network storage devices of any kind
- External hard drives
- USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras, lab equipment, etc.)
- Mapped or shared folders from other computers (e.g., J: drive)

A major outcome of this phase is to determine the severity of the incident and assign the incident a classification (as described previously in this document) to set the appropriate response that corresponds to the severity of the incident through its classification.

5.2.1.3 Collect and Preserve Data

Collect and preserve (including for potential law enforcement investigation) data for incident verification, categorization, prioritization, mitigation, reporting, and ascribing. Data and logs should be collected from as many of the affected devices as possible, including, but not limited to, data from the perimeter, internal network, endpoint (server and host), audit logs, connection logs, system performance logs, and user activity logs. Collection of evidence, including forensic data, happens during this component of the incident response with meeting all applicable polices and standards that include a detailed log that is kept for all evidence (refer to NIST Computer Security Incident Handling Guide, SP 800-61 r2).

5.2.1.4 Perform Technical Analysis

Develop a technical and contextual understanding of the incident. The goal of the analysis within this phase is to examine the breadth of data sources throughout the environment to find at least some part of the attack chain (if not all of the elements of the attack chain) of the incident. The scope is updated as information is collected and the investigation evolves. The following activities can be used for conducting the technical analysis of the incident:

- Correlate events and document timeline: acquire, store, and analyze logs to correlate adversarial activity. Documentation and timeline of relevant findings are established.
- Identify anomalous activity: assess and profile affected systems and networks for subtle activity that could be adversary behavior. This process allows for the finding of deviations from established baseline activity that could be adversarial behavior.
- Identify root cause and enabling conditions: attempt to identify the root cause of the incident and collect corresponding threat information that can be used in further searches and to inform subsequent response efforts. Identifying the conditions that enabled the adversary to carry out the incident within the environment, along with assessing networks and systems for changes that may have been made to either evade defenses or facilitate persistent access is also conducted.
- Gather incident indicators: identify and document indicators of compromise that can be used for correlative analysis on the network.
- Analyze for common adversary Tactics, Techniques, and Procedures (TTP): compare TTPs to adversary TTPs documented in the MITRE Att&CK and analyze how the incident TTPs fit into the attack lifecycle/chain.

- Validate and refine investigation scope: using the data and information collected from the investigation, identify any additional potentially impacted systems, devices, and associated accounts. New indicators of compromise (IOCs) and TTPs might be identified and used for further/refined investigation and the incident can be scoped over time. Communication with stakeholders on the scope of the incident is essential while the incident investigation evolves.

5.2.2 Containment

Implement initial short-term mechanisms that prevent further damage and reduce the immediate impact of the incident (usually by removing the adversary's access). The type of incident will drive the type of containment strategy used due to the unique nature of every incident and system affected. However, the following will provide a baseline set of activities that are common containment strategies/activities for a wide variety of incidents and can be used with tailoring to specific incidents.

- Isolating impacted systems and network segments from each other and/or from non-impacted systems and networks.
- Capturing forensic images to preserve evidence for legal use and future investigation of the incident.
- Updating firewall filtering.
- Blocking (and logging) of unauthorized accesses; blocking malware sources.
- Closing specific ports and mail servers or other relevant servers/services.
- Changing system admin passwords, rotating private keys, and service/application account secrets where compromise is suspected and revocation of privileged access.

Ensure that the containment scope includes all related incidents and activity (especially adversary activity). If new signs of compromise are found, return to the Technical Analysis step to rescope the incident. Once no new signs of compromise are found and successful containment is achieved (which can also include hardening or modifying the environment to protect targeted systems if the root cause of the incident is known), preserve evidence for reference or law enforcement investigation, adjust detection tools, and move to Eradication and Recovery activities.

5.2.3 Eradication and Recovery

Eliminate artifacts of the incident and mitigate vulnerabilities or other conditions that were exploited. It is possible to perform eradication and recovery activities simultaneously.

5.2.3.1 Eradication

Take actions to remove all evidence of compromise and prevent the threat actor from maintaining persistence presence in the environment. The type of incident will drive the

type of eradication activities used due to the unique nature of every incident and system affected. However, the following will provide a baseline set of activities that are common eradication strategies/activities for a wide variety of incidents and can be used with tailoring to specific incidents. All eradication activities and plans must consider all the scenarios that a threat actor could use for alternative attack vectors and multiple persistence mechanisms.

- Remediating all infected IT environments (e.g., cloud, OT, hybrid, host, and network systems).
- Reimaging affected systems (often from golden image sources), rebuilding systems from scratch.
- Rebuilding hardware (required when incident involves rootkits).
- Replacing compromised files with clean versions.
- Installing patches.
- Resetting passwords on compromised accounts.
- Monitoring for any signs of adversary response to containment activities.
- Developing response scenarios for threat actor use of alternative attack vectors.
- Allowing adequate time to ensure all systems are clear of all possible threat actor persistence mechanisms (such as backdoors, etc.) as adversaries often use more than one mechanism.

If new adversary activity is discovered during or at the end of the Eradication activity, contain the new activity and return to Technical Analysis for rescoping of the incident with the additional information found. Once eradication is successful, the incident response can move into Recovery.

5.2.3.2 Recovery

Restore systems to normal operations and confirm that they are functioning normally/baseline levels. A key component in Recovery is to have the mechanisms and controls in place to validate that the recovery plan has been successfully executed and no signs of adversary exist in the environment. The type of incident will drive the type of recovery activities used due to the unique nature of every incident and system affected. However, the following will provide a baseline set of activities that are common recovery strategies/activities for a wide variety of incidents and can be used with tailoring to specific incidents.

- Reconnecting rebuilt/new systems to networks.
- Tightening perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.
- Testing systems (including security controls) thoroughly.
- Monitoring operations for additional abnormal behaviors.

5.3 Post-incident

The goal of this phase is to document the incident, inform leadership, harden the environment to prevent similar incidents, and develop then apply lessons learned to

improve incident handling in the future. Unless otherwise required by law enforcement or federal agency policy, incident documentation should be kept for at least three years (NIST SP 800-61r2).

5.3.1 Adjust sensors, alerts, and log collection

Add/modify/update enterprise-wide detections to mitigate against adversary TTPs that were successfully used during the incident. Identify and address gaps in security and notifications ("blind spots") to ensure adequate coverage in the future. Monitor the environment for evidence of adversarial persistence.

5.3.2 Finalize reports

Provide post-incident updates as required by law and policy. This activity includes working with the appropriate law enforcement or agency to provide required artifacts and/or take additional response actions.

Provide a completed version of the CIRP Response Checklist Template and the Incident Response Report in Appendix E.

5.3.3 Perform lessons learned activities

Conduct lessons learned activities/analysis to review the effectiveness and efficiency of the incident response. The lessons learned meeting should be held within seven days of the end of the incident. Questions to be answered in the meeting include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps/actions taken that might have inhibited the recovery?
- What would the people involved in the incident response do differently the next time a similar incident occurs?
- How could communication between the CIRT team members and other organizations be improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Capture the lessons learned, initial root cause, problems executing courses of action, and any missing policies and procedures. Additional information on these activities can be found in CISA's Cybersecurity Incident & Vulnerability Response Playbooks and NIST SP 800-61r2.

6.0 Playbooks

The following playbooks provide detailed information on actions that the University's incident response team will follow. These playbooks are based on CISA's Cybersecurity Incident & Vulnerability Response Playbooks and Educause playbooks. The playbooks are tailored to fit the needs/requirements of the University and the incident.

These playbooks describe the various processes that the incident response team should follow for a confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.

The following playbooks and steps within those playbooks describe each step in more detail. Many activities are iterative and may continuously occur and/or evolve until the incident is closed out.

6.1 Personally Identifiable Information (PII) Exposed Through Fraud/Impersonation or System Vulnerability

This playbook is a reference process for handling fraud/impersonation incidents. One example of this type of attack would be a threat actor sending false multi-factor authorization (MFA) login request push notifications to the victim until the victim accepts the false MFA request. The attacker can then use the accepted login request to log into the victim's University account and redirect their paycheck from the victim's bank account to the attacker's bank account.

The University contains information that meets the requirements to comply with HIPAA and protect PHI. An attacker can use fraud/impersonation or a vulnerability on a system (system vulnerability) to gain access to PHI of the victim(s).

6.1.1 Detection and Analysis

- Begin documentation within TeamDynamics: incident timeline, any initial actions taken, artifacts collected.
- Begin a copy of the CIRP Response Checklist Template
- Classify data and criticality of impacted assets.
- Determine severity of incident based on severity levels and current information on the incident.
    - Low: mitigate locally with service desk and document mitigation within TeamDynamics. Incident response can end after documentation.
    - High/Emergency: notify CISO, CISO notifies/activates CIRT, declares incident, Incident Manager assigned.
- Activate communication channels needed for the appropriate CIRT members needed for the incident and others that must be notified, including:
    - If health information, see Appendix F for further details.
    - If PCI/DSS (credit card) information, see Appendix G for further details.
    - MDITS

        - By the end of the next business day following discovery of incident if there is any impact to the University (including Low severity incidents).
    - Local/federal law enforcement
    - Federal agency/agencies (such as CISA or Department of Defense (DoD))
- Determine initial investigation scope.
- Perform technical analysis (step is complete when incident has been verified, scope determined, method(s) of persistent access to the network has/have been identified, impact has been assessed, hypothesis for the narrative of exploitation has been created (TTPs and IOCs), and all stakeholders are proceeding with a common operating picture)
    - Collect logs related to the event. These include, but are not limited to:
        - Network devices
        - Centralized logging (SIEM, syslog servers)
        - Authentication sources (LDAP, Active Directory, RADIUS, etc.)
    - Identify anomalous activity.
        - Assess affected systems and networks for adversary behavior.
        - Identify deviations from established baseline activity.
    - Identify root cause and enabling conditions.
        - Attempt to identify root cause of the incident and collect threat information for further searches.
        - Identify and document conditions that enabled adversary to access and operate within the environment (including system(s) affected, changes to networks/systems, etc.)
        - Identify attack vector (how adversary accessed the environment of the incident) and assess access of the adversary (depth and breadth of access of the affected system(s))
    - Analyze for common adversary TTPs.
        - Identify initial access techniques.
            - Identify associated command and control information if initial access is done by malware.
                - Port number
                - Protocol
                - Profile
                - Domain
                - IP address
        - Identify techniques used by adversary to achieve code execution.
        - Identify persistence mechanisms by assessing compromised hosts.
        - Identify lateral movement by determining techniques used by adversary to access remote hosts.
        - Identify method of remote access, credentials used to authenticate, and level of privilege.
            - Identify adversary’s level of credential access and/or privilege escalation.

    - Identify mechanism used for data exfiltration.
- Continue to update scope and communicate updated scope to all stakeholders to ensure common operating picture.

6.1.2 Containment, Eradication, and Recovery

6.1.2.1 Containment

- Isolate affected systems – disconnect from the network but DO NOT POWER OFF
- Assess risk to other systems.
    - Apply additional interim mitigations, additions to monitoring, etc.
- Determine appropriate containment strategy based on:
    - Requirement to preserve evidence
    - Accountability of services (e.g., network connectivity, services availability)
    - Resource constraints
    - Time required to perform containment steps
- Collect evidence for additional review and legal proceedings.
- Create forensics images of hard drives and memory.
- Take snapshots of virtual machines to preserve the current state.
- Retrieve hard copies of any disclosed program information.
- Isolate affected systems and networks, including, but not limited to:
    - Perimeter containment
    - Internal network containment
    - Host-based/Endpoint containment
    - Temporarily disconnect public-facing systems from the internet, etc.
- Close specific ports and mail servers. Update firewall filtering
- Change system admin passwords, rotate private keys, and revoke privileged access for service/application account secrets where compromise is suspected.
- Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.
- Prevent Domain Name Server (DNS) resolution of known attacker domain names.
- Prevent compromised system(s) from connecting to other systems on the network.
- Monitor systems for signs of threat actor response to containment activities.
- If new signs of compromise are found, return to technical analysis to re-scope the incident.
- Continue documentation of findings and communications with any necessary external contacts (MDITS, etc.)

- Once containment is successful (i.e., no new signs of compromise), preserve evidence for reference and law enforcement (if applicable), adjust detection tools, and move to eradication.

6.1.2.2 Eradication

- Develop an eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanisms.
- Remove artifacts of the incident from affected systems, networks, etc.
- Reimage affected systems from clean backups (i.e., golden images/sources).
- Rebuild hardware if rootkits were involved or suspected.
- Scan for malware to ensure removal of malicious code.
- Monitor for signs of threat actor response to eradication activities.
    - Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism).
- Update the timeline and documentation to incorporate all pertinent events from this step.
- Complete any remaining actions of the eradication plan.
- Continue detection and analysis activities after executing the eradication plan for any signs of adversary re-entry or use of new access methods.
- If new adversary activity is discovered, contain the new activity and return to Technical Analysis until the true scope of the compromise and infection vectors are identified.
- If eradication is successful, move to Recovery.

6.1.2.3 Recovery

- Restore systems to operational use (recovering data).
- Fully patch and install updates on all systems before reconnecting to the network.
- Change all local system and user passwords (including any centralized accounts that used the system) on affected systems before redeployment.
- Change all passwords and private keys stored on the system used to access other systems.
- Harden the system to a well-documented standard (such as CIS Benchmarks).
- Scan for and remediate discovered vulnerabilities before deployment.
    - Document any exceptions for vulnerabilities that cannot be mitigated, including compensating controls that will be used instead.
- Improve/modify monitoring to help stop any recurrence of the incident.
    - Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.

- Test systems thoroughly (including security controls assessment) to validate systems are operating normally before bringing back online in production networks.
- Review all relevant TTPs to ensure situational awareness of the threat actor activity.
- Update incident timeline to incorporate all pertinent events from Recovery step.
- Complete any additional/outstanding specific recovery activities.

6.1.3 Post-incident Activities

6.1.3.1 Adjust sensors, alerts, and log collection

- Add enterprise-wide detections to mitigate against adversary TTPs that were executed to cause the incident.
- Identify and mitigate operational "blind spots" to complete coverage moving forward.
- Continue to monitor the University environment for evidence of persistent presence.

6.1.3.2 Finalize reports

- Provide post-incident updates as required by law and policy.
- Publish post-incident report. Provide a step-by-step review of the entire incident and answer the "Who", "What", "Where", "Why", and "How" questions. Provide a completed version of the CIRP Response Checklist Template and the Incident Response Report in Appendix E.
- Work with MDITS and any other agencies and law enforcement to provide any additional information/evidence/actions required.

6.1.3.3 Perform lessons learned

- Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.
- Identify if University incident response processes were followed and if the processes were sufficient.
- Identify any policies and procedures in need of modification/creation to prevent similar incidents from occurring.
- Identify how information sharing with stakeholders (MDITS, law enforcement, etc.) can be improved during incident response.
- Identify any gaps in incident responder training.
- Identify any unclear/undefined roles, responsibilities, interfaces, and authorities.
- Identify precursors/indicators that should be monitored to detect similar incidents.

        - Identify if University infrastructure for defense was sufficient and identify the gaps if the defense was not sufficient.
        - Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.
        - Identify any deficiencies in the University incident response planning process. If no deficiencies identified, identify how the agency intends to implement more rigor in its incident response planning.
        - Create a plan to implement any recommended changes and improvements with target dates for completion.
- Complete the hardening of the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.
- Finalize the documentation of the incident, inform the Information Technology Council, University leadership, and any stakeholders.

6.2 External Attack/Distributed Denial of Service

This playbook is a reference process for handling Distributed Denial of Service (DDoS) incidents. A DDoS attack is an attempt to make an online service unavailable to legitimate users by overwhelming the service with traffic from multiple sources. Examples of this type of attack include an overwhelming number of UDP datagrams being sent to a targeted host (UDP Flood), overwhelming number of ICMP echo requests to a victim (Ping Flood), or overwhelming number of HTTP GET or POST requests to a targeted host (HTTP Flood Attack).

6.2.1 Detection and Analysis

- Begin documentation within TeamDynamics: incident timeline, any initial actions taken, artifacts collected.
- Begin a copy of the CIRP Response Checklist Template
- Classify data and criticality of impacted assets.
- Determine severity of incident based on severity levels and current information on the incident.
    - Low: mitigate locally with service desk and document mitigation within TDnext. Incident response can end after documentation.
    - High/Emergency: notify CISO, CISO notifies/activates CIRT, declares incident, Incident Manager assigned.
    - Update Umbrella if DNS related.
    - Update firewall (if required).
    - Communicate with MissiON and Internet Service Provider.
    - PCAP Analysis (if required).
- Activate communication channels needed for the appropriate CIRT members needed for the incident and others that must be notified, including:
    - Local law enforcement
    - Infrastructure

- Internet Service Provider (ISP) - CSPIRE
    - Requests assistance to filter IP
- MDITS
    - By the end of the next business day following discovery of incident if there is any impact to the University (including Low severity incidents).
- Federal agency/agencies (such as CISA or DoD).

- Determine initial investigation scope.
- Perform technical analysis (step is complete when incident has been verified, scope determined, method(s) of persistent access to the network has/have been identified, impact has been assessed, hypothesis for the narrative of exploitation has been created (TTPs and IOCs), and all stakeholders are proceeding with a common operating picture)
    - Collect logs related to the event. These include, but are not limited to:
        - Network devices
        - Centralized logging (SIEM, syslog servers)
        - Authentication sources (LDAP, Active Directory, RADIUS, etc.)
        - Infrastructure
            - Fortinet Firewalls
            - F5 Load Balancer
        - Infrastructure Monitoring
            - Check external latency
            - Check latency of websites outbound/in.
            - Check outages.
            - Check degradation of services/systems.
            - Contact Monitoring Service/NOC to check logs.
        - All Departments
            - Check for unknown or unexpected incoming traffic.
            - Detection of unknown/unidentified packets from unknown senders.
            - Check IT Services to see impact.
            - Check Critical Systems referenced in Business Continuity Plan (BCP)/Business Impact Assessment (BIA).
    - Identify anomalous activity.
        - Assess affected systems and networks for adversary behavior.
        - Identify deviations from established baseline activity.
        - Communicate with 3rd party organizations to check scope of incident.
            - Cyber Security
                - Check with REN-ISAC.
                - Check with Cloud Hosting Service Providers.
                - If DNS related, contact Cisco (Umbrella) or DNS service provider.
            - Office of Strategic Communications Team

        - Check with Cloud Service Provider hosting their materials.
        - Check social media (Facebook, Instagram, X, etc.).
- Check global reports of similar incidents to help determine scope.
    - Are there reports of global issues where the institution would be collateral damage?
        - Check internet health and traffic reports to rule out global issues.
        - Check Content Delivery Network (CDN).
    - Validate organization communication.
        - Email
        - VOIP infrastructure
- Identify root cause and enabling conditions.
    - Attempt to identify root cause of the incident and collect threat information for further searches.
    - Identify and document conditions that enabled adversary to access and operate within the environment (including system(s) affected, changes to networks/systems, etc.)
    - Identify attack vector (how adversary accessed the environment of the incident) and assess access of the adversary (depth and breadth of access of the affected system(s))
- Analyze for common adversary TTPs.
- Continue to update scope and communicate updated scope to all stakeholders to ensure common operating picture.
    - Activate additional communication channels if needed.

6.2.2 Containment, Eradication, and Recovery

6.2.2.1 Containment

- Isolate affected assets.
    - Perimeter containment
    - Internal network containment
    - Host-based/endpoint containment
    - Temporarily disconnect public-facing systems from the internet, etc.
- Assess risk to other systems.
    - Apply additional interim mitigations, additions to monitoring, etc.
- Determine appropriate containment strategy based on:
    - Requirement to preserve evidence
    - Accountability of services (e.g., network connectivity, services availability)
    - Resource constraints
    - Time required to perform containment steps

- If applicable/available, temporarily redirect legitimate traffic to backup resources.
- Close specific ports and mail servers. Update firewall filtering.
- Prevent compromised/affected system(s) from connecting to other systems on the network.
- Monitor for other areas of compromise (to prevent the attack from distracting from another attack, like an adversary gaining persistence on a system while the DDoS attack occurring).
- Constrain resources.
    - If previous steps fail, simply constraining resources, like rate and connection limit is a last resort – it can turn away both good and bad traffic. Instead, you may want to disable or blackhole an application.
    - If there are too many attackers to make blocking by IP address or region feasible, you may have to develop a plan to unwind the attack by mitigating "backwards"— that is, defending the site from the database tier to the application tier, and then to the web servers, load balancers, and finally the firewalls.
- Collect evidence for additional review and legal proceedings.
- Create forensics images of hard drives and memory.
- Take snapshots of virtual machines to preserve the current state.
- Retrieve hard copies of any disclosed program information.
- Monitor systems for signs of threat actor response to containment activities.
- If new signs of compromise are found, return to technical analysis to re-scope the incident.
- Continue documentation of findings/update timeline and communications with any necessary external contacts (MDITS, etc.).
- Once containment is successful (i.e., no new signs of compromise), preserve evidence for reference and law enforcement (if applicable), adjust detection tools, and move to eradication.

6.2.2.2 Eradication

- Develop an eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanisms.
    - Is attack Host Based or IP Based?
        - IP Based Attack
            - Change Public IP address
            - Consider failing over to DR site.
        - Host Based
            - Continue pursuing ISP assistance.
    - Evaluate mitigation options for Source Address.
        - Can Source Address be blocked at Firewall?

        - Can source address or addresses be GeoBlocked by Firewall?
            - Consider business impact of GeoBlocking.
    - Is attack targeting a specific application?
        - Can Patching mitigate (as some DDOS exploits a missing patch or vulnerability)?
    - As the identification of the different mix of attack vectors becomes apparent, the following techniques can be used as remediation specific to individual attacks.
        - Null Routing/Blackhole Routing - a network route (routing table entry) that goes nowhere. Matching packets are dropped/ignored rather than forwarded, acting as a kind of very limited firewall.
        - DNS Sinkhole - a standard DNS server that has been configured to hand out non-routable addresses for all domains in the sinkhole, so that every computer that uses it will fail to get access to the real website. The higher up the DNS resolution chain the sinkhole is, the more requests it will block as it will supply answers to a greater number of lower NS servers that in turn will serve a greater number of clients.
        - Scrubbing Center - a centralized data cleansing station where traffic to the affected website is analyzed, and malicious traffic (SQL injection, XSS, DDoS and other known exploits) is removed. Scrubbing centers are often used by ISPs and cloud providers because they prefer to route potential malicious traffic to an out of path data cleansing station rather than keeping it in network and bogging down the legitimate traffic. With an on-demand scrubbing center, when an attack is detected, the traffic is redirected (typically using DNS or BGP (Border Gateway Protocol)) to a local scrubbing center where the traffic is analyzed (usually using deep packet inspection) and the attack traffic is filtered out while the clean traffic passes back to the network for delivery.
- Execute eradication plan.
- Reimage affected systems from clean backups (i.e., golden images/sources).
- Rebuild hardware if rootkits were involved or suspected.
- Scan for malware to ensure removal of malicious code.
- Monitor for signs of threat actor response to eradication activities.
    - Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism).
- Update the timeline and documentation to incorporate all pertinent events from this step.

- Complete any remaining actions of the eradication plan.
- Continue detection and analysis activities after executing the eradication plan for any signs of adversary re-entry or use of new access methods.
- If new adversary activity is discovered, contain the new activity and return to Technical Analysis until the true scope of the compromise and infection vectors are identified.
- If eradication is successful, move to Recovery.

6.2.2.3 Recovery

- Restore systems to operational use (recovering data).
- Fully patch and install updates on all systems before reconnecting to the network.
- Change all local system passwords and user passwords (including any centralized accounts that used the system) on affected systems before redeployment.
- Change all passwords and private keys stored on the system used to access other systems.
- Harden the system to a well-documented standard (such as CIS Benchmarks).
- Scan for and remediate discovered vulnerabilities before deployment.
    - Document any exceptions for vulnerabilities that cannot be mitigated, including compensating controls that will be used instead.
- Improve/modify monitoring to help stop any recurrence of the incident.
    - Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.
- Test systems thoroughly (including security controls assessment) to validate systems are operating normally before bringing back online in production networks.
- Review all relevant TTPs to ensure situational awareness of the threat actor activity.
- Update incident timeline to incorporate all pertinent events from Recovery step.
- Complete any additional/outstanding specific recovery activities.

6.2.3 Post-incident Activities

6.2.3.1 Adjust Sensors, Alerts, and Log Collection

- Add enterprise-wide detections to mitigate against adversary TTPs that were executed to cause the incident.
- Identify and mitigate operational “blind spots” to complete coverage moving forward.
- Continue to monitor the University environment for evidence of persistent presence.

6.2.3.2 Finalize Reports

- Provide post-incident updates as required by law and policy.
- Publish post-incident report. Provide a step-by-step review of the entire incident and answer the “Who”, “What”, “Where”, “Why”, and “How” questions. Provide a completed version of the CIRP Response Checklist Template and the Incident Response Report in Appendix E.
- Work with MDITS or any other agencies and law enforcement to provide any additional information/evidence/actions required.

6.2.3.3 Perform Lessons Learned

- Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.
- Identify if University incident response processes were followed and if the processes were sufficient.
- Identify any policies and procedures in need of modification/creation to prevent similar incidents from occurring.
- Identify how information sharing with stakeholders (MDITS, law enforcement, etc.) can be improved during incident response.
- Identify any gaps in incident responder training.
- Identify any unclear/undefined roles, responsibilities, interfaces, and authorities.
- Identify precursors/indicators that should be monitored to detect similar incidents.
- Identify if University infrastructure for defense was sufficient and identify the gaps if the defense was not sufficient.
- Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.
- Identify any deficiencies in the University incident response planning process. If no deficiencies identified, identify how the agency intends to implement more rigor in its incident response planning.
- Create a plan to implement any recommended changes and improvements with target dates for completion.

- Complete the hardening of the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.
- Finalize the documentation of the incident, inform Information Technology Council, University leadership, and any stakeholders.

6.3 Research Data/Proprietary Information Exposed

This playbook is in reference to incidents that include research data or University proprietary information that is exposed to unauthorized parties. The information that is exposed could have significant consequences if disclosed to threat actors. (See university's ISP for definitions and classification guides for the data included in this playbook) An example of this kind of incident includes a researcher clicking on malicious link and opens back door to computer and attacker able to copy research files.

6.3.1 Detection and Analysis

- Begin documentation within TeamDynamics: incident timeline, any initial actions taken, artifacts collected.
- Begin a copy of the CIRP Response Checklist Template
- Classify data and criticality of impacted assets.
- Determine severity of incident based on severity levels and current information on the incident.
    - Low: mitigate locally with service desk and document mitigation within TDnext. Incident response can end after documentation.
    - High/Emergency: notify CISO, CISO notifies/activates CIRT, declares incident, Incident Manager assigned.
- Activate communication channels needed for the appropriate CIRT members needed for the incident and others that must be notified, including:
    - ORED Office of Research Compliance and Security and Export Control Officers
    - External researchers/External shareholders/Security or program point person for research program
    - MDITS
        - By the end of the next business day following discovery of incident if there is any impact to the University (including Low severity incidents).
    - Local/federal law enforcement.
    - Federal agency/agencies (such as CISA or DoD).
- Determine initial investigation scope.
- Perform technical analysis (step is complete when incident has been verified, scope determined, method(s) of persistent access to the network has/have been identified, impact has been assessed, hypothesis for the narrative of exploitation has been created (TTPs and IOCs), and all stakeholders are proceeding with a common operating picture)
    - Collect logs related to the event. These include, but are not limited to:
        - Network devices
        - Centralized logging (SIEM, syslog servers)
        - Authentication sources (LDAP, Active Directory, RADIUS, etc.)
    - Identify anomalous activity.
        - Assess affected systems and networks for adversary behavior.
        - Identify deviations from established baseline activity.
    - Identify root cause and enabling conditions.

- Attempt to identify root cause of the incident and collect threat information for further searches.
- Identify and document conditions that enabled adversary to access and operate within the environment (including system(s) affected, changes to networks/systems, etc.)
- Identify attack vector (how adversary accessed the environment of the incident) and assess access of the adversary (depth and breadth of access of the affected system(s))

- Analyze for common adversary TTPs.
  - Identify initial access techniques.
    - Identify associated command and control information if initial access is done by malware.
      a. Port number
      b. Protocol
      c. Profile
      d. Domain
      e. IP address
  - Identify techniques used by adversary to achieve code execution.
  - Identify persistence mechanisms by assessing compromised hosts.
  - Identify lateral movement by determining techniques used by adversary to access remote hosts.
  - Identify method of remote access, credentials used to authenticate, and level of privilege.
    - Identify adversary's level of credential access and/or privilege escalation.
  - Identify mechanism used for data exfiltration.
- Continue to update scope and communicate updated scope to all stakeholders to ensure common operating picture.

6.3.2 Containment, Eradication, and Recovery

6.3.2.1 Containment

- Isolate affected systems – disconnect from the network but DO NOT POWER OFF
- Assess risk to other systems.
  - Apply additional interim mitigations, additions to monitoring, etc.
- Determine appropriate containment strategy based on:
  - Requirement to preserve evidence
  - Accountability of services (e.g., network connectivity, services availability)
  - Resource constraints
  - Time required to perform containment steps

- Collect evidence for additional review and legal proceedings.
- Create forensics images of hard drives and memory.
- Take snapshots of virtual machines to preserve the current state.
- Retrieve hard copies of any disclosed program information.
- Isolate affected systems and networks, including, but not limited to:
    - Perimeter containment
    - Internal network containment
    - Host-based/Endpoint containment
    - Temporarily disconnect public-facing systems from the internet, etc.
- Close specific ports and mail servers. Update firewall filtering
- Change system admin passwords, rotate private keys, and revoke privileged access for service/application account secrets where compromise is suspected.
- Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.
- Prevent Domain Name Server (DNS) resolution of known attacker domain names.
- Prevent compromised system(s) from connecting to other systems on the network.
- Monitor systems for signs of threat actor response to containment activities.
- If new signs of compromise are found, return to technical analysis to re-scope the incident.
- Continue documentation of findings and communications with any necessary external contacts (MDITS, etc.)
- Once containment is successful (i.e., no new signs of compromise), preserve evidence for reference and law enforcement (if applicable), adjust detection tools, and move to eradication.

6.3.2.2 Eradication

- Develop an eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanisms.
- Remove artifacts of the incident from affected systems, networks, etc.
- Reimage affected systems from clean backups (i.e., golden images/sources).
- Rebuild hardware if rootkits were involved or suspected.
- Scan for malware to ensure removal of malicious code.
- Monitor for signs of threat actor response to eradication activities.
    - Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism).

- Update the timeline and documentation to incorporate all pertinent events from this step.
- Complete any remaining actions of the eradication plan.
- Continue detection and analysis activities after executing the eradication plan for any signs of adversary re-entry or use of new access methods.
- If new adversary activity is discovered, contain the new activity and return to Technical Analysis until the true scope of the compromise and infection vectors are identified.
- If eradication is successful, move to Recovery.

6.3.2.3 Recovery

- Restore systems to operational use (recovering data).
- Fully patch and install updates on all systems before reconnecting to the network.
- Change all local system and user passwords (including any centralized accounts that used the system) on affected systems before redeployment.
- Change all passwords and private keys stored on the system used to access other systems.
- Harden the system to a well-documented standard (such as CIS Benchmarks).
- Scan for and remediate discovered vulnerabilities before deployment.
    - Document any exceptions for vulnerabilities that cannot be mitigated, including compensating controls that will be used instead.
- Improve/modify monitoring to help stop any recurrence of the incident.
    - Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.
- Test systems thoroughly (including security controls assessment) to validate systems are operating normally before bringing back online in production networks.
- Review all relevant TTPs to ensure situational awareness of the threat actor activity.
- Update incident timeline to incorporate all pertinent events from Recovery step.
- Complete any additional/outstanding specific recovery activities.

6.3.3 Post-incident Activities

6.3.3.1 Adjust Sensors, Alerts, and Log Collection

- Add enterprise-wide detections to mitigate against adversary TTPs that were executed to cause the incident.
- Identify and mitigate operational “blind spots” to complete coverage moving forward.

- Continue to monitor the University environment for evidence of persistent presence.

6.3.3.2 Finalize Reports

- Provide post-incident updates as required by law and policy.
- Publish post-incident report. Provide a step-by-step review of the entire incident and answer the “Who”, “What”, “Where”, “Why”, and “How” questions. Provide a completed version of the CIRP Response Checklist Template and the Incident Response Report in Appendix E.
- Work with MDITS and any other agencies and law enforcement to provide any additional information/evidence/actions required.

6.3.3.3 Perform Lessons Learned

- Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.
- Identify if University incident response processes were followed and if the processes were sufficient.
- Identify any policies and procedures in need of modification/creation to prevent similar incidents from occurring.
- Identify how information sharing with stakeholders (MDITS, law enforcement, etc.) can be improved during incident response.
- Identify any gaps in incident responder training.
- Identify any unclear/undefined roles, responsibilities, interfaces, and authorities.
- Identify precursors/indicators that should be monitored to detect similar incidents.
- Identify if University infrastructure for defense was sufficient and identify the gaps if the defense was not sufficient.
- Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.
- Identify any deficiencies in the University incident response planning process. If no deficiencies identified, identify how the agency intends to implement more rigor in its incident response planning.
- Create a plan to implement any recommended changes and improvements with target dates for completion.

- Complete the hardening of the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.
- Finalize the documentation of the incident, inform the Information Technology Council, University leadership, and any stakeholders.

6.4 Ransomware

This playbook is a reference process for handling ransomware incidents. Examples of this type of attack include Petya (encrypts entire computer systems and overwrites the master book record, which makes the operating system unbootable) and TorrentLocker/CryptoLocker (typically distributed through spam email campaigns and is geographically targeted with email messages delivered to specific regions; uses AES algorithm to encrypt file types; also collects email addresses from the victim's address book to spread malware beyond the initial infected computer).

The University's policy on paying ransomware is not paying the requested ransom since that money would go towards further attacks by the hackers and the University is dedicated to fighting for the greater good to the best of its abilities. However, in extreme circumstances (such as massive/catastrophic failures and life/death situations), payment may be considered and will be approved on a case-by-case basis at the discretion of the OCRM, the President of the University, MDITS, and federal law enforcement.

6.4.1 Detection and Analysis

- Begin documentation within TeamDynamics: incident timeline, any initial actions taken, artifacts collected.
- Begin a copy of the CIRP Response Checklist Template
- Classify data and criticality of impacted assets.
- Determine severity of incident based on severity levels and current information on the incident.
    - Low: mitigate locally with service desk and document mitigation within TeamDynamics. Incident response can end after documentation.
    - High/Emergency: notify CISO, CISO notifies/activates CIRT, declares incident, Incident Manager assigned.
- Activate communication channels needed for the appropriate CIRT members needed for the incident and others that must be notified, including:
    - If health information, see Appendix C for further details.
    - MDITS
        - By the end of the next business day following discovery of incident if there is any impact to the University (including Low severity incidents).
    - Local/federal law enforcement.
    - Federal agency/agencies (such as CISA or DoD).
- Determine initial investigation scope.
    - Internal
        - How many endpoints were affected?
        - How many servers were affected?
        - Were backups affected?
        - Was Shared folder location affected?
    - External

        - Have there been any threats/comments made on Social Media? (Facebook, Twitter, Reddit, etc.)
        - Communicate with 3rd party organizations.
            - DHS NCCIC
            - REN-ISAC
            - US-CERT
    - Are there reports of global issues where the university would be collateral damage?
        - Is this a targeted attack of the university or across the education sector? Or many sectors?
- Perform technical analysis (step is complete when incident has been verified, scope determined, method(s) of persistent access to the network has/have been identified, impact has been assessed, hypothesis for the narrative of exploitation has been created (TTPs and IOCs), and all stakeholders are proceeding with a common operating picture)
    - Collect logs related to the event. These include, but are not limited to:
        - Network devices
        - Centralized logging (SIEM, syslog servers)
        - Authentication sources (LDAP, Active Directory, RADIUS, etc.)
    - Identify anomalous activity.
        - Assess affected systems and networks for adversary behavior.
        - Identify deviations from established baseline activity.
    - Identify root cause and enabling conditions.
        - Attempt to identify root cause of the incident and collect threat information for further searches.
        - Identify and document conditions that enabled adversary to access and operate within the environment (including system(s) affected, changes to networks/systems, etc.)
        - Identify attack vector (how adversary accessed the environment of the incident) and assess access of the adversary (depth and breadth of access of the affected system(s))
    - Analyze for common adversary TTPs (tactics, techniques, and procedures).
        - Identify initial access techniques.
            - Has a Ransomware message appeared on the screen?
                - Yes: take a picture and then remove from network and proceed to Section 2. of this playbook.
                - No: If in the process of encrypting and the message has not appeared, immediately remove from the network
                - Unsure: if there is evidence that system(s) have been compromised, remove from the network.
            - Did EDR (Endpoint Detection and Response) detect Ransomware?
                - Yes: Investigate Ransomware in Cisco Secure Endpoint Console

        - No: Notify vendor that EDR failed to detect Ransomware.
    - Has malicious code been found on systems?
        - Yes: use that code and all tools possible to see if it exists anywhere else on the network.
        - No: Proceed to following question.
    - Is the code a potential unwanted application, remote access, or hacker tool?
        - Yes: use the info provided to see if other devices on the network have been exposed.
        - No: Proceed to next step
    - EPP (Endpoint Protection) detect Ransomware?
        - Yes: Was it stopped? Investigate further to gather more details.
        - No: Why was it not detected? Contact vendor to notify them EPP did not detect Ransomware. If further investigation provides hashes or Indicators of Compromise (IOC's), enter into EPP immediately to stop further propagation.
    - Did EDR detect Ransomware?
        - Yes: EDR filters data into Enterprise EDR, follow process found above.
        - No: Contact EDR provider and inform them there was no detection.
    - Are Shared File Location(s) affected?
        - Check for encrypted files.
        - Disconnect from the backups and the disaster response sites until Ransomware is contained.
- Identify associated command and control information if initial access is done by malware.
    a. Port number
    b. Protocol
    c. Profile
    d. Domain
    e. IP address
- Identify techniques used by adversary to achieve code execution.
- Identify persistence mechanisms by assessing compromised hosts.
- Identify lateral movement by determining techniques used by adversary to access remote hosts.
- Identify method of remote access, credentials used to authenticate, and level of privilege.
    - Identify adversary's level of credential access and/or privilege escalation.
- Identify mechanism used for data encryption.

- Continue to update scope and communicate updated scope to all stakeholders to ensure common operating picture.

6.4.2 Containment, Eradication, and Recovery

6.4.2.1 Containment

- Isolate affected systems – disconnect from the network but DO NOT POWER OFF
- Assess risk to other systems.
    - VPN Users
        - Disable through Cisco Secure Endpoint
        - If EDR has been disabled, work with Network Team to terminate VPN session. Then work with Service Desk team to prevent further sessions. Must occur within first 5-10 minutes or else endpoint has been lost.
    - Apply appropriate additional interim mitigations, additions to monitoring, etc.
- Determine appropriate containment strategy based on:
    - Requirement to preserve evidence
    - Accountability of services (e.g., network connectivity, services availability)
    - Resource constraints
    - Time required to perform containment steps
- Collect evidence for additional review and legal proceedings.
- Create forensics images of hard drives and memory.
- Take snapshots of virtual machines to preserve the current state.
- Retrieve hard copies of any disclosed program information.
- Isolate affected systems and networks, including, but not limited to:
    - Perimeter containment
    - Internal network containment
    - Host-based/Endpoint containment
    - Temporarily disconnect public-facing systems from the internet, etc.
- Close specific ports and mail servers. Update firewall filtering
- Change system admin passwords, rotate private keys, and revoke privileged access for service/application account secrets where compromise is suspected.
- Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.
- Prevent Domain Name Server (DNS) resolution of known attacker domain names.
- Prevent compromised system(s) from connecting to other systems on the network.

- Monitor systems for signs of threat actor response to containment activities.
- If new signs of compromise are found, return to technical analysis to re-scope the incident.
- Continue documentation of findings and communications with any necessary external contacts (MDITS, etc.)
- Once containment is successful (i.e., no new signs of compromise), preserve evidence for reference and law enforcement (if applicable), adjust detection tools, and move to eradication.

6.4.2.2 Eradication

- Develop an eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanisms.
- Remove artifacts of the incident from affected systems, networks, etc.
- Reimage affected systems from clean backups (i.e., golden images/sources).
- Rebuild hardware if rootkits were involved or suspected.
- Scan for malware to ensure removal of malicious code.
- Monitor for signs of threat actor response to eradication activities.
    - Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism).
- Update the timeline and documentation to incorporate all pertinent events from this step.
- Complete any remaining actions of the eradication plan.
- Continue detection and analysis activities after executing the eradication plan for any signs of adversary re-entry or use of new access methods.
- If new adversary activity is discovered, contain the new activity and return to Technical Analysis until the true scope of the compromise and infection vectors are identified.
- If eradication is successful, move to Recovery.

6.4.2.3 Recovery

- Restore systems to operational use (recovering data).
- Fully patch and install updates on all systems before reconnecting to the network.
- Change all local system and user passwords (including any centralized accounts that used the system) on affected systems before redeployment.
- Change all passwords and private keys stored on the system used to access other systems.
- Harden the system to a well-documented standard (such as CIS Benchmarks).
- Scan for and remediate discovered vulnerabilities before deployment.

- Document any exceptions for vulnerabilities that cannot be mitigated, including compensating controls that will be used instead.
- Improve/modify monitoring to help stop any recurrence of the incident.
- Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.
- Test systems thoroughly (including security controls assessment) to validate systems are operating normally before bringing back online in production networks.
- Review all relevant TTPs to ensure situational awareness of the threat actor activity.
- Update incident timeline to incorporate all pertinent events from Recovery step.
- Complete any additional/outstanding specific recovery activities.

6.4.3 Post-incident Activities

6.4.3.1 Adjust Sensors, Alerts, and Log Collection

- Add enterprise-wide detections to mitigate against adversary TTPs that were executed to cause the incident.
- Identify and mitigate operational “blind spots” to complete coverage moving forward.
- Continue to monitor the University environment for evidence of persistent presence.

6.4.3.2 Finalize Reports

- Provide post-incident updates as required by law and policy.
- Publish post-incident report. Provide a step-by-step review of the entire incident and answer the “Who”, “What”, “Where”, “Why”, and “How” questions. Provide a completed version of the CIRP Response Checklist Template and the Incident Response Report in Appendix E.
- Work with MDITS and any other agencies and law enforcement to provide any additional information/evidence/actions required.

6.4.3.3 Perform Lessons Learned

- Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.
- Identify if University incident response processes were followed and if the processes were sufficient.
- Identify any policies and procedures in need of modification/creation to prevent similar incidents from occurring.

    - Identify how information sharing with stakeholders (MDITS, law enforcement, etc.) can be improved during incident response.
    - Identify any gaps in incident responder training.
    - Identify any unclear/undefined roles, responsibilities, interfaces, and authorities.
    - Identify precursors/indicators that should be monitored to detect similar incidents.
    - Identify if University infrastructure for defense was sufficient and identify the gaps if the defense was not sufficient.
    - Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.
    - Identify any deficiencies in the University incident response planning process. If no deficiencies identified, identify how the agency intends to implement more rigor in its incident response planning.
    - Create a plan to implement any recommended changes and improvements with target dates for completion.
- Complete the hardening of the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.
- Finalize the documentation of the incident, inform the Information Technology Council, University leadership, and any stakeholders.

Appendix A: Definitions

This appendix defines selected terms used in this document.

Availability – The ability to ensure the timely and reliable access and use of MSU Information.

Compromise (also seen as "data compromise") – Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of any object may have occurred.

Confidentiality – The preservation of authorized restrictions on access to and disclosure of MSU Information.

Controlled Unclassified Information (CUI) - Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls (such as information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls). This information cannot, however, be classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended (such as classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency).

Impersonation - The "practice of pretexting as another person with the goal of obtaining information or access to a person, company, or computer system."

Incident (also seen as "cybersecurity incident" or "security incident") – an occurrence that (1) actually or immediately jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Integrity – Guarding against improper modification or destruction of MSU information and ensuring non-repudiation and authenticity.

Malware - a piece of malicious software that has been successfully executed on a system.

Personally Identifiable Information (PII) - Information that can be used to distinguish or trace an individual's identity (including, but not limited to, name, social security number, date of birth, mother's maiden name, etc.)

Pretexting - A form of social engineering where the attacker creates a fictional backstory to manipulate someone into providing information or to influence the victim's behavior

Protected Health Information (PHI) - A subset of PII and is defined as individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except otherwise contained in employment records held by a HIPAA covered entity in its role as an employer.

RACI (Responsible, Accountable, Consulted, Informed) matrix – A type of responsibility assignment matrix in project management that lists all the stakeholders of a project and their level of involvement within those tasks indicated in a table by R, A, C, and I.

- Responsible – is the one who does the work to complete the task or create the deliverable; every task should have at least one responsible person and could have several.
- Accountable – is the one who delegates and reviews the work involved; they make sure the responsible person or team knows the expectations and completes work on time; every task should have only one accountable person.
- Consulted – provide input and feedback on the work being done; may be individuals who aren't working on a given task but whose work will be affected by the outcome; also, sometimes teammates outside of the team whose work will be affected by the outcomes; one consulted party per affected team is considered best practice.
- Informed – need to be looped into the progress but not consulted or overwhelmed with the details of every task; need to know what's going on because it could affect their work, but they're not decision makers in the process; usually outside of the team and in different departments; usually upper-leadership of affected teams (Unit heads, etc.) and/or senior leadership (Vice Presidents, President, etc.)

Ransomware - An attack that is a subset of malware that is designed to block access to a system or data on a system until a sum of money is paid.

Threat Actor – An individual or a group posing a threat; source of risk that can result in harmful impact.

Vulnerability - A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

PCI DSS Definitions

The following definitions are key terms that are used in the PCI DSS response plan.

Cardholder - Customer to which a payment card is issued to or any individual authorized to use the payment card.

Cardholder Data (CHD) - At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Cardholder Name - The name of the Cardholder to whom the card has been issued.

Card Verification Code (CAV2, CVC2, CID, or CVV2 data) - Also known as "Card Validation Code" or "Card Validation Value", or "Card Security Code". Refers to either: (1) magnetic-stripe data, or (2) printed security features.

(1) Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:

- CAV – Card Authentication Value (JCB payment cards)
- PAN CVC – Card Validation Code (MasterCard payment cards)
- CVV – Card Verification Value (Visa and Discover payment cards)
- CSC – Card Security Code (American Express)

(2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand:

- CID – Card Identification Number (American Express and Discover payment cards)
- CAV2 – Card Authentication Value 2 (JCB payment cards)
- PAN CVC2 – Card Validation Code 2 (MasterCard payment cards)
- CVV2 – Card Verification Value 2 (Visa payment cards)

Disposal – (1) CHD on/in hard-copy materials when no longer needed for business or legal reasons that are destroyed/pending destruction to the point where CHD cannot be reconstructed from media. Hard-copy materials are stored in secure storage containers prior to destruction and may be destroyed by:
cross-cut shredding, incineration, pulped, or approved destruction methods as specified within the University's Information Security Plan.

(2) Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.

Expiration Date - The date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.

Magnetic-Stripe Data – Also known as "Track Data" or "full track data". Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.

Merchant - For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

Merchant Department - Any University department or Unit (can be a group of departments or a subset of a department) which has been approved by the University to accept credit cards and has been assigned a Merchant identification number.

Merchant Department Responsible Person (MDRP) - An individual within the University department or Unit who has primary authority and responsibility within that department for credit card transactions.

Payment Card Industry Data Security Standards (PCI DSS) - PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices. The goal of the PCI Data Security Standard (PCI DSS) is to protect cardholder data and sensitive authentication data wherever it is processed, stored, or transmitted. The security requirements are set and managed by the Payment Card Industry Security Standards Council (PCI SSC), while compliance of these requirements is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB, MasterCard, and Visa Inc.

Personal Identification Number (PIN) - Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.

PIN block - A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN.

Primary Account Number (PAN) - Also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Sensitive Authentication Data - Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Service Code - Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

Appendix B – Main CIRT Contact Information

This appendix provides the contact information of the main CIRT members that will be notified for incidents that correspond to the incident classification that is assigned.

Department/User	Contact Information
Service Desk	Phone: 662-325-0631 Toll-Free: 888-398-6394 Email: servicedesk@msstate.edu Web: servicedesk.msstate.edu
Chief Information Security Officer (CISO)	Phone: 662-325-3709 Email: security@its.msstate.edu
Chief Information Officer (CIO)	Phone: 662-325-9311
Office of the General Counsel	Phone: (662) 325-8131
Chief Technology Transformation Officer (CTTO)	Phone: (662) 325-4024
Office of Strategic Communications	Phone: (662) 325-7454
Office of the Provost and Executive Vice President	Phone: 662-325-3742 Email:provost@msstate.edu
Office of the President	Phone: 662-325-3221 Email:president@msstate.edu

Appendix C – Supplemental CIRT Contact Information

This appendix provides contact information to the additional CIRT members for their expertise to provide additional support for various incidents.

Department/User	Contact Information
Office of Compliance & Risk Management	Phone: (662) 325-4024
Mississippi Department of Information Technology Services (MDITS)	ITS Service Center (601-432-8080) ITS Main Line (601-432-8000) Reporting webpage: https://www.its.ms.gov/services/security/Enterprise-Cybersecurity-Incident-Reporting
University Registrar	Phone: (662) 325-2022
Office of Controller and Treasurer	Phone: (662) 325-2302 Email: creditcard@controller.msstate.edu
HIPAA Security Officer	Phone: 662-325-3709 Email: security@its.msstate.edu

Appendix D – Emergency Incident Response Contact Information

This appendix provides contact information to the companies or agencies that can assist in incident emergencies for their expertise in containment, law enforcement, evidence collection, etc.

Company/Agency	Contact Information
SpearTip (Third-party Emergency Incident Response Team)	Phone: 833-997-7327 Email: breachresponse@speartip.com
Cybersecurity & Infrastructure Security Agency (CISA)	Phone: 888-282-0870 Email: report@cisa.gov Reporting webpage: https://www.cisa.gov/report
University Police	Phone: 911 (or 662-325-2121 for non-emergencies)
Federal Bureau of Investigation (FBI) Jackson (Mississippi Local Office)	Phone: 601-948-5000 Email: tips.fbi.gov Reporting webpage: https://tips.fbi.gov/home

Appendix E – Emergency Incident Report Template

Departmental Security Contact Information:

Name:
Department:
Email:
Phone:
Location/Site Involved (Building/Room/Campus):

Type of Incident:

- Personally Identifiable Information (PII) Exposed Through Fraud/Impersonation or System Vulnerability
- Research Data/Proprietary Information Exposed
- External Attack/Distributed Denial of Service
- Ransomware
- Other

Classification of Incident:

Date and Time of Discovery:

Incident Details:

How was the incident detected?

How long was the compromise in place?

What measures were in place to protect the information/system? What failed and why did it fail? Why?

What employees are assigned to the security of the system or information? Any shared administration with other departments?

Please attach a copy of the completed CIRP Response Checklist Template spreadsheet corresponding to the incident and provide further details below that expand on the "Detection & Analysis", "Containment", "Eradication & Recovery", and "Post-Incident" actions taken.

For example:

- Log files maintained
- Forensics investigation
- Physically secured system
- System restored from backup
- Patches/virus updates and system verified
- Exposed information removed from web and external search engine(s) cache cleared

Appendix F – HIPAA Supplemental Incident Response Plan

F.1 Purpose

The Health Insurance Portability and Accountability Act (HIPAA) Supplemental Incident Response Plan provides the additional information needed to effectively respond to security incidents involving Personal Health Information (PHI)/electronic PHI (ePHI) and HIPAA information.

F.2 Scope

Mississippi State University is in accordance with HIPAA due to the University being designated a "hybrid entity". The University protects the confidentiality, integrity, and availability of protected health information and the University's regulations complying with this law can be found in OP 91.400: Health Insurance Portability and Accountability Act (HIPAA) and in the NIST SP 800-66r2. Any information related to HIPAA and OP 91.400 (such as ePHI) that is involved in a security incident would require this supplemental incident response plan to be executed to ensure a compliant and efficient response.

F.3 Procedure

The procedure for responding to a breach of HIPAA information begins during the "Detection and Analysis" section of the "Personally Identifiable Information (PII) Exposed Through Fraud/Impersonation or System Vulnerability" playbook.

- After determining health information/HIPAA information was exposed, activate communication channels needed for CIRT and others that must be notified, including:
    - HIPAA privacy officer. It is important to know that organizations must report the dates when the breach first occurred and when they should have known about it.
        - HIPAA determines its consequences from the date that the organization should have known about the breach, not when it was actually reported so the breach must be reported it as soon as possible.
        - The privacy officer will want specific information about the possible breach so he or she can conduct an appropriate risk assessment. The information should describe the nature of the PHI that was disclosed, how well people were identified on it, where it was exposed, who might have seen it, and whether or not it was delivered.
    - MDITS
        - By the end of the next business day following discovery of incident if there is any impact to the University (including Low severity incidents).

    - Local/federal law enforcement
    - Affected Individuals: Covered entities are required to notify affected individuals whose PHI/ePHI has been compromised as a result of the breach. Notifications should be provided in writing and include specific information about the breach, steps individuals can take to protect themselves, and resources for additional information or assistance.
    - Department of Health and Human Services (HHS): Covered entities must also notify the Secretary of HHS of breaches affecting 500 or more individuals within 60 days of discovering the breach. Breaches affecting fewer than 500 individuals can be reported annually to HHS.
- Because the extent of the information that was exposed determines the scope of the response, the HIPAA privacy officer will provide specific and additional response tasks to resolve the incident (such as notifying additional departments (such as Legal or the CIO) or hardening specific systems based on the NIST SP 800-66r2 standard) that will be integrated into the "Personally Identifiable Information (PII) Exposed Through Fraud/Impersonation or System Vulnerability" playbook. Continue through those steps starting at "Perform technical analysis" once scope has been determined.

Appendix G - Payment Card Supplemental Security Incident Response Plan

G.1 Purpose

The Payment Card Supplemental Security Incident Response Plan supplements the University Incident Response Plan. Additional elements defining those responsible, the classification and handling of, and the reporting/notification requirements for incident response plan at Mississippi State University are required to be compliant to Payment Card Industry Data Security Standard (PCI DSS).

G.2 Scope/Applicability

A list of the merchants and operations with payment card acceptance and IP addresses has been provided to the Information Technology Security Office to identify the areas for accepting payment cards.

Incidents involving PCI DSS data/information will be required to follow the additional steps within this supplemental playbook along with the University's incident response plan procedures within the playbook appropriate for the current incident. PCI DSS data/information includes, but is not limited to, Payment Card data or any material or records that contain cardholder data.

G.3 Procedures

G.3.1 PCI Incident Response Plan

The PCI Incident Response Plan's procedures begin when there is a declaration of an incident involving PCI DSS information or data (during the "Detection and Analysis" step of the CIRP). Because the extent of the information that was exposed determines the scope of the response, the PCI DSS Response Team will provide specific and additional response tasks to resolve the incident (such as notifying additional departments (such as Legal or the CIO) or hardening specific systems based on the standards put in place by the PCI Security Standards Council) that will be integrated into the "Personally Identifiable Information (PII) Exposed Through Fraud/Impersonation or System Vulnerability" playbook. Continue through those steps starting at "Perform technical analysis" once scope has been determined.

In the event of a suspected or confirmed incident:

1. Contact the PCI DSS Response Team by sending an email documenting the incident to
   creditcard@controller.msstate.edu.
2. The PCI DSS Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
3. If the incident involves a payment station (computer/system used to process credit cards):
   a. Do NOT turn off the computer/system.

b. Disconnect the network cable connecting the computer/system to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.

4. Document any steps taken until the PCI DSS Response Team has arrived. Include the date, time, person/persons involved, and action taken for each step. Start a copy of the CIRP Response Checklist Template, Appendix E for the ITS incident form, and Appendix H for the PCI DSS incident form.
5. Assist the PCI DSS Response Team as they investigate the incident.

G.3.1.1 Incident Response Team Procedures

In response to a system compromise, the PCI DSS Response Team and Information Technology Services will:

1. Ensure compromised system is isolated on/from the network.
2. Gather, review, and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs and alerts.
3. Assist department in analysis of locally maintained system and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system.
5. If an incident of unauthorized access is confirmed and card holder data was potentially compromised, the Incident Manager (at the discretion of the PCI Committee), depending on the nature of the data compromise, must notify the appropriate organizations in the "Additional Notification Requirements for Incident" table in this document. Additional communications to that table may include the following:
    a. Chief Financial Officer
    b. Internal Audit group
    c. Mississippi State University Acquiring Bank(s), the Acquiring Bank will be responsible for communicating with the card brands (VISA, MasterCard)
    d. If American Express payment cards are potentially included in the breach, the University is responsible for notifying and working with American Express
        i. For incidents involving American Express cards, contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident.
            1. Fill out the Merchant Data Incident Initial Notice Form and email to EIRP@aexp.com within 72 hours after the security incident is discovered
            2. Phone number: (888) 732-3750
    e. If Discover Network payment cards are potentially included in the breach the University is responsible for notifying and working with Discover Network.
        i. For incidents involving Discover cards, contact Discover Security within 48 hours after the reported incident.
            1. Phone Number: (800) 347-3083

f. Campus police and local law enforcement
g. Payment Card Industry Forensic Investigator (PFI) (https://listings.pcisecuritystandards.org/documents/Responding_to_a_Cardholder_Data_Breach.pdf)

6. Assist the PFI and law enforcement personnel in investigative process.

G.3.3 Bank Breach Response Plans

The credit card companies have specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. For Visa and MasterCard, it is the University's responsibility to notify their own bank (the financial institution(s) that issues merchant accounts to the university) and the University's bank will be responsible for notifying Visa and MasterCard, were applicable.

Elavon – The merchant internal security group at Elavon provides their Data Compromise Management documentation below embedded as a PDF: (Double Click to open)

Data Compromise Management

WHAT IS A DATA COMPROMISE EVENT?

Simply stated, a data compromise event is an unauthorized and illegal theft of data. A central target for a data compromise event is often credit or debit card information which a perpetrator will typically re-sell or use in the production and presenting of counterfeit cards. There are three basic types of data compromise events:

- **Physical Theft.** Stealing receipts, hardware or other documentation which contains card data
- **Skimming.** Theft of card information used in an otherwise legitimate transaction
  - Typically an "inside job" by a dishonest employee of a legitimate merchant
  - The thief can procure a victim's card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store a victim's card magnetic stripe information
- **Systemic Intrusion.** Utilizing malicious, unauthorized and illegal means to obtain electronic access to payment processing systems or storage mediums, often referred to as hacking

WHAT TO DO IF COMPROMISED

1. Immediate containment

- Do NOT access or alter compromised systems (i.e., do not log on at all to the machine and change passwords, and do not log in as ROOT)
- Isolate compromised systems(s) from the network (i.e., unplug network cable). Do not turn the compromised system(s) off.
- Preserve all merchant logs and electronic evidence
- Make a record of all action taken, who took the action and the date and time of such action
- If using a wireless network and a compromise is suspected, disable the wireless network
- Monitor all systems with cardholder data for possible threats or issues

2. Alert all necessary parties immediately

- Merchant internal security group at Elavon :
  - 865.403.7321 (Amanda Duggin)
  - 865.403.8852 (Chris Geron)
- Law enforcement
- Check applicable state laws for possible notification to cardholders

3. Follow-up with Elavon. Elavon will send you a questionnaire either by e-mail or facsimile which must be completed and returned to Elavon within 3 calendar days. This information may be forwarded by Elavon to the card brands as part of the investigation process. You will need to provide Elavon with the transaction information that was possibly involved in the data compromise within 7 calendar days so that the information can be provided to the card brands. Elavon will assist with determining what information must be reported.

4. Determination of need for independent forensic investigation. The Card Brand(s), in consultation with Elavon, will determine whether an independent forensic investigation will be required. Approved forensic investigations may be required to:

- Assess a compromised entity's computing environment to identify relevant sources of electronic evidence
- Assess all external connectivity points within each location involved
- Assess network access controls between compromised system(s) and adjacent and surrounding networks

Elavon

Appendix H - Payment Card Incident Log

In the event of a suspected or confirmed please follow the procedures below ensuring each step taken is documented using this incident log:

1. Start a new payment card incident log.

2. Contact the Response Team by sending an email documenting the incident to creditcard@controller.msstate.edu.

Action	Date/Time	Location	Person (s) performing action	Person(s) documenting action
Additional notes				

Action	Date and Time	Location	Person(s) performing action	Person(s) documenting action

3. The Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
4. If the incident involves a payment station (PC used to process credit cards):
    a. Do NOT turn off the PC.
    b. Disconnect the network cable connecting the PC to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
5. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
6. Assist the Response Team as they investigate the incident.
7. If an incident of unauthorized access is confirmed and card holder data was potentially compromised, the PCI Committee Chairperson will make the following contacts with Mississippi State University acquiring bank(s) after informing the Chief Financial Officer and the Chief Information Officer:

YES ☐ NO ☐

If YES, date and time systems were removed:

_____

Name of person(s) who disconnected the network:

_____

If NO, state reason:

_____

_____

_____

Actions Performed

Action	Date and Time	Location	Person(s) performing action	Person(s) documenting action

Appendix I – RACI Matrix

RACI Matrix of the Mississippi State University overall CIRP. This matrix provides the responsibilities of key members of the CIRT for tasks throughout the University's incident response. These tasks and responsibilities are meant to serve as a baseline for the University's incident response (such as for a large-scale breach of research data) but should be modified as needed for specific incidents' needs.

The following diagram corresponds the background colors of the cells in the matrix to the various steps in the University's incident response:

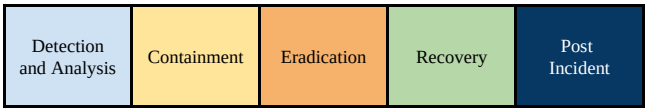


Figure 2. Background colors meaning of cells in the RACI Matrix for Mississippi State University Cyber Security Incident Response Plan.

Table 4. RACI Matrix of Mississippi State University Cyber Security Incident Response Plan.

Step	CIO	CISO	Service Desk	Incident Manager	IT Support	Data Owner	Legal	Office of Strategic Communications	Office of Compliance and Risk Mgmt	Research Compliance and Security
Register Incident		I	RA		I					
Conduct Initial Incident Analysis		I	RA		R					
Assign Severity		RA	CI		C	C	C		I	C
Determine Next Steps Based on Severity	I	RA			C					
Assign Incident Manager	I	RA		I		I	I		I	I
Mobilize CIRT	I	I	I	RA	C					
Determine Scope		I	C	RA	R	C	C			C
Collect Incident Data				A	R	C				
Perform Technical Analysis		I	I	RA	R	C				
Determine If Notification Is Required	I	C		C			RA		C	C
Notify Relevant Parties	I	I		I		I	A	RC	R	I
Communicate to Stakeholders	I	RC	I	RA		I				I
Develop Containment Plan		I	I	RA	R	C				

Execute Containment Plan		I	I	A	R					
Determine If the Incident is Contained	I	I		RA		I				
Communicate to Stakeholders	I	RC	I	RA		I				
Develop Eradication Plan			I	RA	RC	C				
Execute Eradication Plan		I	I	A	R					
Determine If the Threat Is Eradicated	I	C		RA		I				
Communicate to Stakeholders	I	RC	I	RA		I				
Develop Recovery Plan			I	RA	RC	C				
Execute Recovery Plan		I	I	RA	R					
Determine If the Systems Are Recovered	I	C		A	R	I				
Communicate to Stakeholders	I	RC	I	RA		I				
Conduct Lessons Learned Activities	I	RA	R	R	R	C			I	C
Document Findings	I	C		RA		C	C			C
Assign Action Owners		RA			I	I				
Update Controls and Policies		RA	I	I	R	I				C
Demobilize CIRT	I	C		RA		I		I		
Close Ticket	I	I		RA		I		I		

References

American Express. (2024). *U.S. Data Security*. https://www.americanexpress.com/us/merchant/us-data-security.html

American Express. (2024, April). *American Express Data Security Operating Policy (DSOP).* https://www.americanexpress.com/content/dam/amex/us/merchant/new-data-security/DSOP_United_States_EN.pdf

Carnegie Mellon University. (2020, February 20). *Social Engineering: Pretexting and Impersonation.* Information Security Office. https://www.cmu.edu/iso/news/2020/pretexting.html

Cichonski P, Millar T, Grance T, Scarfone K. (2012, August). *Computer Security Incident Handling Guide.* (National Institute of Standards and Technology, Gaithersburg, Maryland), NIST Special Publication (SP) 800-61 Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

Cybersecurity and Infrastructure Security Agency. (2021, November). *Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems.* Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Discover Global Network. (2024). *Discover Information Security & Compliance (DISC).* Discover Financial Services. https://www.discoverglobalnetwork.com/solutions/pci-compliance/discover-_information-security-compliance/?search=srch_result_txt_3&srchQ=discover%20data%20security%20team%20contact

Educause. (2019, October 4). *National Student Clearinghouse Playbooks.* https://library.educause.edu/resources/2019/10/national-student-clearinghouse-playbooks

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., Good, T. (2006, September). *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities: Recommendations of the National Institute of Standards and Technology.* (National Institute of Standards and Technology, Gaithersburg, Maryland), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L 104-191. (1996).

Health.mil. (n.d.) Personally Identifiable Information (PII). In *Health.mil Definitions.* https://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Board/Definitions

Health.mil. (n.d.) Protected Health Information (PHI). In *Health.mil Definitions.* https://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Board/Definitions

Marron, J. A. (2024, February). *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.* (National Institute of Standards and Technology, Gaithersburg, Maryland), NIST Special Publication (SP) 800-66 Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

Miranda, D., Watts, R. (2022, December 14). What is a RACI Chart? How This Project Management Tool Can Boost Your Productivity. *Forbes Advisor.* https://www.forbes.com/advisor/business/raci-chart/

Mississippi Code Annotated § 75-24-29

Mississippi State University Information Technology Services. (2023, November 07). *Mississippi State Information Security Program.* https://www.infosecurity.msstate.edu/sites/www.infosecurity.msstate.edu/files/2024-01/V2.0_Mississippi%20State%20University%20Information%20Security%20Program-Approved%202024-01-31.pdf

Mississippi State University. (2017). *Credit/Debit Card Processing*. (Mississippi State University, Starkville, Mississippi), Mississippi State Official Policy (OP) 62.08, June 2017. https://www.policies.msstate.edu/policy/6208

Mississippi State University. (2017). *Safeguarding Cardholder Data (CHD)*. (Mississippi State University, Starkville, Mississippi), Mississippi State Official Policy (OP) 62.10, June 2017. https://www.policies.msstate.edu/policy/6210

Mississippi State University. (2017). *Security of Card Payment Devices*. (Mississippi State University, Starkville, Mississippi), Mississippi State Official Policy (OP) 62.09, June 2017. https://www.policies.msstate.edu/policy/6209

Mitre. (n.d.) *Att&CK.* https://attack.mitre.org/

National Cybersecurity Center of Excellence (NCCoE). (n.d.) *Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain and Test Back Files*. National Institute of Standards and Technology (NIST). https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf

National Institute of Standards and Technology. (n.d.) Compromise. In *NIST Computer Security Resource Center Glossary of Key Information Security Terms.* https://csrc.nist.gov/glossary/term/compromise

National Institute of Standards and Technology. (n.d.) Controlled Unclassified Information (CUI). In *NIST Computer Security Resource Center Glossary of Key Information Security Terms.* https://csrc.nist.gov/glossary/term/controlled_unclassified_information

National Institute of Standards and Technology. (n.d.) Impersonation. In *NIST Computer Security Resource Center Glossary of Key Information Security Terms.* https://www.social-engineer.org/framework/attack-vectors/impersonation

National Institute of Standards and Technology. (n.d.) Incident. In *NIST Computer Security Resource Center Glossary of Key Information Security Terms.* https://csrc.nist.gov/glossary/term/cybersecurity_incident#:~:text=Definitions%3A,NIST%20Cybersecurity%20Framework%20Version%201.1

National Institute of Standards and Technology. (n.d.) Threat Actor. In *NIST Computer Security Resource Center Glossary of Key Information Security Terms.* https://csrc.nist.gov/glossary/term/threat_actor

National Institute of Standards and Technology. (n.d.) Vulnerability. In *NIST Computer Security Resource Center Glossary of Key Information Security Terms.* https://csrc.nist.gov/glossary/term/vulnerability

Payment Card Industry Security Standards Council. (2022). Cardholder. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Cardholder Data (CHD). In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Card Verification Code. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2020). *Guidance: Responding to a Cardholder Data Breach.* https://listings.pcisecuritystandards.org/documents/Responding_to_a_Cardholder_Data_Breach.pdf

Payment Card Industry Security Standards Council. (2022). *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* Document Library. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Merchant. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Payment Card Industry Data Security Standards. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Personal Identification Number. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). PIN Block. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Primary Account Number. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Sensitive Authentication Data. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Service Code. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Payment Card Industry Security Standards Council. (2022). Track Data. In *Payment Card Industry Data Security Standard: Requirements and Testing Procedures.* https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Souppaya M, Scarfone K. (2013). *Guide to Malware Incident Prevention and Handling for Desktops and Laptops.* (National Institute of Standards and Technology, Gaithersburg, Maryland), NIST Special Publication (SP) 800-83 Rev. 1, July 2013. https://doi.org/10.6028/NIST.SP.800-83r1

Standards for Safeguarding Customer Information. 16 C.F.R. Part 314. (2002).