

Where does this document live?

- Digital location:** [Enter the on-line location]
- Physical location:** [Enter the location of a printout of this document, often in the Emergency Operations Plan]
- Companion Document:** [insert district document here] Template: [\[Quick Reference Document\]](#)
- Companion Document:** [insert district document here] Template: [\[Worksheet Reference Document\]](#)

Version	Date	Author	Description of Changes	Comments
1.0	10/17/2024	CSTF Taskforce 2024	Completed initial document	


Purpose

The purpose of this document is to provide guidance to educational entities toward the development of their own Incident Response Plan (“IRP”). This document should be used as a framework to establish a consistent, complete, comprehensive organizational **Incident Response Plan**. The incident response process follows six stages:



Each of these stages will be addressed individually with considerations provided for a district to develop their own, localized plan for each stage.

Purpose	1
Stage 1 - Preparation	2
Stage 2 - Identification	5
Stage 3 - Containment	8
Stage 4 - Eradication	11
Stage 5 - Recovery	12
Stage 6 - Lessons Learned	14
REFERENCES:	15

<h1>Stage 1</h1>		<p>Description: Organizations exist in Stage 1 until an incident occurs. This section should be reviewed regularly to ensure that the organization is fully prepared to respond to any cybersecurity event or incident.</p>
------------------	---	--

Description	
<p>1.1 Define a Cyber Incident</p>	<p>How does your organization define a cyber security incident? Is there a policy defined (Board, Insurance Policy, Emergency Operations Plan, other plans)?</p> <hr/> <hr/> <p>EXAMPLE: NIST defines a Computer Security Incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.</p> <p>The district should consider how the board and/or its cybersecurity insurer defines a Cyber Incident/Event. For example, NEOLA's definition of a Cybersecurity Event:</p> <p><i>An unexpected, observable action or change that leads to an investigation. Includes any event that is known or has the potential to negatively impact the confidentiality, integrity, or availability of District information/data. This can range from the loss of a laptop, tablet, or other mobile/portable storage device, virus infection of an end-user workstation, or breach of a District system by a hacker</i></p>
<p>1.2 Define and Identify Cyber Incident Response (IR) Team Roles & Identify Contacts and Key Resources</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Complete, print, and share your completed Incident Response Worksheet <input type="checkbox"/> Define Incident Response Team Members <input type="checkbox"/> Define Incident Response Team Extended Resources <ul style="list-style-type: none"> <input type="checkbox"/> Meet as a Incident Response Team to define/clarify roles <input type="checkbox"/> Meet as an Extended Team to define/clarify roles

Description	
1.3 Assemble Existing Plans and Tools	<p>What relevant formal policies, plans, and procedures does your organization already have in place?</p> <p>Review documents and ensure up-to-date printed copies are available. These may include:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Board Policy & Administrative Guidelines <input type="checkbox"/> Emergency Operations Plan (EOP) <input type="checkbox"/> Business Continuity Plan & Continuity of Operations Plan (COOP) <input type="checkbox"/> IT network, asset, and emergency plans <input type="checkbox"/> Crisis/Emergency Management Plan <input type="checkbox"/> Communications Plan <input type="checkbox"/> Disaster Recovery Plan (DRP) <input type="checkbox"/> Training or Phishing Mitigation Plan <input type="checkbox"/> Risk Management Plan <input type="checkbox"/> Cybersecurity Insurance Documentation <input type="checkbox"/> Other: _____
1.4 Prepare for Stakeholder Communications	<p>Prompt, clear, and consistent communication is vital in any crisis. Prepare your communications/PR team (internal and/or external) for cyber incident communications, including via tabletop exercises.</p> <p>The Incident Response Worksheet provides several considerations. They should include::</p> <ul style="list-style-type: none"> ● What are the requirements of your cybersecurity insurance? <ul style="list-style-type: none"> ○ Do they provide consulting? ● How will you communicate if normal communications are locked out? ● What involvement does cabinet require? <ul style="list-style-type: none"> ○ What involvement does the Board of Education require? ● Advising staff to not share unauthorized incident-related communications/post on social media ● Pre-writing and vetting sample notifications to staff, families, and the media for common K-12 cyber incidents
1.5 Conduct Review and Training Exercises	<ul style="list-style-type: none"> <input type="checkbox"/> Regular reviews of plan with Incident Response Team members <input type="checkbox"/> Conduct tabletop exercises to maintain familiarity with IRP
1.6 Conduct Cybersecurity Assessments	<ul style="list-style-type: none"> <input type="checkbox"/> Complete the MiSecure Quick-Self Assessment or another tool <input type="checkbox"/> Conduct a cybersecurity assessment using a comprehensive tool such as the CIS CSAT or with a third party. Based on results, establish and address remediation priorities with staff. <input type="checkbox"/> Conduct a third party penetration test regularly in order to identify and address weaknesses.

Description	
1.7 Build Incident Response Professional Community	<p>When preparing for a potential incident, it's recommended that you become familiar with the various organizations that can support you during an incident. Get to know the community before an incident.</p> <ul style="list-style-type: none"><input type="checkbox"/> Join Cyber Partners<input type="checkbox"/> Join the Michigan State Police Cyber Command mailing list<input type="checkbox"/> Join MS-ISAC<input type="checkbox"/> Join engin-I email list (contact your ISD Technology Director)<input type="checkbox"/> Participate and communicate with MiSecure (MiSecure.org)<input type="checkbox"/> Meet and maintain relationships with the local FBI field office.

Stage 2



Description: Determining the potential scope and impact of a cyber incident helps prioritize response and recovery efforts—including stakeholder communications.

Description													
2.1 Adopt a Cybersecurity scale	<p>A cybersecurity incident can be classified into various levels based on its severity, impact, and scope. These levels help organizations respond appropriately and allocate resources effectively.</p> <p>Organizations should customize the following table to align with their operations:</p> <table border="1"> <thead> <tr> <th>Severity Level</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>False positive</td> <td> <p>Description: Events determined to be the result of normal, if unexpected, user or automated activity.</p> <p>Example: A user mistakenly believes that they've exposed their credentials in response to a suspicious email.</p> <p>Potential Response: none</p> </td> </tr> <tr> <td>Low level Simple event</td> <td> <p>Description: Incidents that have minimal impact on the organization.</p> <p>Example: Detection of malware that has been quarantined, phishing emails that have been blocked, unsuccessful attempts to gain unauthorized access.</p> <p>Potential Response: Handled by routine operational processes, no significant disruption, limited to specific users or systems.</p> </td> </tr> <tr> <td>Medium level Significant event</td> <td> <p>Description: Incidents that have a moderate impact and may require some intervention.</p> <p>Example: A compromise of a single user's credentials, malware infection on a few systems, unauthorized access to non-sensitive data.</p> <p>Potential Response: Requires IT/security team intervention, may involve resetting passwords, cleaning infected systems, monitoring for further issues.</p> </td> </tr> <tr> <td>High level incident</td> <td> <p>Description: Incidents that significantly impact business operations or sensitive data.</p> <p>Example: Data breach involving sensitive information, widespread malware/ransomware attack, significant unauthorized access to critical systems.</p> <p>Potential Response: Response: Requires immediate and coordinated response from the incident response team, may involve shutting down systems, notifying affected parties, and implementing containment measures.</p> </td> </tr> <tr> <td>Critical level Serious incident</td> <td> <p>Description: Incidents that pose an extreme threat to the organization's operations, data, or reputation.</p> <p>Example: Advanced persistent threats (APTs), major data breach affecting large volumes of sensitive data, coordinated cyberattacks causing substantial operational disruption.</p> <p>Potential Response: A full activation of the incident response plan, potential involvement of external agencies (e.g., law enforcement, cybersecurity</p> </td> </tr> </tbody> </table>	Severity Level	Description	False positive	<p>Description: Events determined to be the result of normal, if unexpected, user or automated activity.</p> <p>Example: A user mistakenly believes that they've exposed their credentials in response to a suspicious email.</p> <p>Potential Response: none</p>	Low level Simple event	<p>Description: Incidents that have minimal impact on the organization.</p> <p>Example: Detection of malware that has been quarantined, phishing emails that have been blocked, unsuccessful attempts to gain unauthorized access.</p> <p>Potential Response: Handled by routine operational processes, no significant disruption, limited to specific users or systems.</p>	Medium level Significant event	<p>Description: Incidents that have a moderate impact and may require some intervention.</p> <p>Example: A compromise of a single user's credentials, malware infection on a few systems, unauthorized access to non-sensitive data.</p> <p>Potential Response: Requires IT/security team intervention, may involve resetting passwords, cleaning infected systems, monitoring for further issues.</p>	High level incident	<p>Description: Incidents that significantly impact business operations or sensitive data.</p> <p>Example: Data breach involving sensitive information, widespread malware/ransomware attack, significant unauthorized access to critical systems.</p> <p>Potential Response: Response: Requires immediate and coordinated response from the incident response team, may involve shutting down systems, notifying affected parties, and implementing containment measures.</p>	Critical level Serious incident	<p>Description: Incidents that pose an extreme threat to the organization's operations, data, or reputation.</p> <p>Example: Advanced persistent threats (APTs), major data breach affecting large volumes of sensitive data, coordinated cyberattacks causing substantial operational disruption.</p> <p>Potential Response: A full activation of the incident response plan, potential involvement of external agencies (e.g., law enforcement, cybersecurity</p>
Severity Level	Description												
False positive	<p>Description: Events determined to be the result of normal, if unexpected, user or automated activity.</p> <p>Example: A user mistakenly believes that they've exposed their credentials in response to a suspicious email.</p> <p>Potential Response: none</p>												
Low level Simple event	<p>Description: Incidents that have minimal impact on the organization.</p> <p>Example: Detection of malware that has been quarantined, phishing emails that have been blocked, unsuccessful attempts to gain unauthorized access.</p> <p>Potential Response: Handled by routine operational processes, no significant disruption, limited to specific users or systems.</p>												
Medium level Significant event	<p>Description: Incidents that have a moderate impact and may require some intervention.</p> <p>Example: A compromise of a single user's credentials, malware infection on a few systems, unauthorized access to non-sensitive data.</p> <p>Potential Response: Requires IT/security team intervention, may involve resetting passwords, cleaning infected systems, monitoring for further issues.</p>												
High level incident	<p>Description: Incidents that significantly impact business operations or sensitive data.</p> <p>Example: Data breach involving sensitive information, widespread malware/ransomware attack, significant unauthorized access to critical systems.</p> <p>Potential Response: Response: Requires immediate and coordinated response from the incident response team, may involve shutting down systems, notifying affected parties, and implementing containment measures.</p>												
Critical level Serious incident	<p>Description: Incidents that pose an extreme threat to the organization's operations, data, or reputation.</p> <p>Example: Advanced persistent threats (APTs), major data breach affecting large volumes of sensitive data, coordinated cyberattacks causing substantial operational disruption.</p> <p>Potential Response: A full activation of the incident response plan, potential involvement of external agencies (e.g., law enforcement, cybersecurity</p>												

Description	
	experts), comprehensive containment, eradication, and recovery efforts.
Catastrophic	<p><u>Description</u>: Incidents that threaten the survival of the organization.</p> <p><u>Example</u>: Nation-state sponsored attacks causing massive data loss, critical infrastructure attacks leading to extended downtime, cyberattacks causing significant financial loss or legal ramifications.</p> <p><u>Potential Response</u>: Crisis management, involvement of executive leadership, public communication strategies, extensive recovery and continuity plans, potential long-term impact assessment and remediation. Possible execution of your Emergency Management Plan.</p>
2.2 Communication and Team Resources	<p>Whom should be communicate with?</p> <hr/> <p>Link to your Incident Response Worksheet (based on the MiSecure Incident Response Worksheet or other resource)</p> <p>If this is a High Level Incident or greater:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Pull together your Cyber Incident Response Team (CIRT) <input type="checkbox"/> You may need to contact cybersecurity insurance if PII has been released, systems require remediation, there is a threat to the organization's operations and/or reputation <input type="checkbox"/> You should work with your cybersecurity insurance provider to determine when this is appropriate <ul style="list-style-type: none"> o You may need to contact MC3 if there is evidence of a crime. o You may need to contact FBI if there is a cyber incident (particularly ransomware) <input type="checkbox"/> You should contact MiSecure to report any indicators of compromise (IOCs) to assist other districts in identifying if they are experiencing a similar incident. You should also report on tactics, techniques and procedures (TTPs) that the bad actor used to create the incident so districts can strengthen their defenses.

Description	
2.3 Identify Compromise	<p>What tools are available to help identify a compromise?</p> <hr/> <p>How do you identify compromised accounts?</p> <hr/> <p>Consider:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Alerts <ul style="list-style-type: none"> <input type="checkbox"/> Antivirus and antispam software <input type="checkbox"/> Endpoint Detection and Response Software (EDR) <input type="checkbox"/> SIEMs <input type="checkbox"/> Intrusion Detection and Prevention Systems (IDPS) <input type="checkbox"/> Third party monitoring <input type="checkbox"/> Logs <ul style="list-style-type: none"> <input type="checkbox"/> Operating Systems <input type="checkbox"/> Service and Application logs <input type="checkbox"/> Network device / Network Flow logs <input type="checkbox"/> Publicly Available Information <ul style="list-style-type: none"> <input type="checkbox"/> MS-ISAC Alerts <input type="checkbox"/> People <ul style="list-style-type: none"> <input type="checkbox"/> Reports of incidents
2.4 Monitor for Anomalous Activity	<p>Consider:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Instituting more robust system logging and network monitoring <input type="checkbox"/> Increase monitoring of systems and network activity for anomalous activity, remote access, new/changed privileged accounts, or other signs of intrusion

Stage 3



Description: Once a cyber event or incident has been identified, it is critical that the attack and/or attacker is contained.

Description

Contain the incident

3.1 Blocking Communication with other Devices

Block compromised systems from communicating with other devices or with attackers.

Specific containment responses depend on the scale/scope of the actual incident.

Some reasonable responses are:

- Isolate a local individual machine
- Isolate a remote individual machine
- Isolating several remote machines
- Isolate a subnet
- Isolate the entire network
- Disconnect from the Internet
- Isolate a cloud-based server(s)
- Restrict authentication methods such as SSO, Cloud
- Disabling services, especially any that are being targeted (e.g. web server, student information systems, financial systems)
- Disabling compromised accounts (revoke tokens and delete active connections)
- Disable/restrict remote access methods such as VPNs
- Review usage and confirm integrity of Administrative level accounts

Caution should be taken before taking steps to contain the incident. For instance:

- Incident responders/law enforcement may wish to monitor an attacker or gather additional evidence before beginning containment activities.
- Once containment and eradication efforts begin, attackers may change tactics, targets, or intensity of malicious activity. Continue to monitor systems closely and be prepared to move quickly in response.

Powering off systems prematurely may delete in-memory evidence of compromise. Containment tools, which may be at your disposal, include:

- Endpoint configuration management tools (via Intune/SCCM and/or via AppLocker, JAMF, Google Chrome Device Management, etc.)
- EDR/Antivirus global controls
- Host-based firewall controls
- Switch ports, uplinks, and network segments (which can be disabled)
- Network firewall (for both inbound and outbound traffic)
- Content/DNS web filters

<p>3.2 Detailed Containment Methods</p>	<p>Specific containment methods - the “how to” - vary by district. Details should be identified in this section.</p> <p>Containment of actual systems or services require additional considerations that need to be addressed prior to an actual event. While complete containment steps are outside the scope of this document, important considerations should be identified before an incident occurs in order to avoid delays. Use these questions to develop your organization’s own containment procedures.</p>
<p>3.2a Detailed Containment Methods - Network</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Network Containment <ul style="list-style-type: none"> <input type="checkbox"/> Is your patch to the upstream network labeled? <input type="checkbox"/> What levels of the Network can be isolated? <ul style="list-style-type: none"> <input type="checkbox"/> Vlans <input type="checkbox"/> Buildings <input type="checkbox"/> Network closets <input type="checkbox"/> How do you disable / disconnect from the Network/Internet? _____ <input type="checkbox"/> Do you have an isolation Network available? <input type="checkbox"/> How would you review connections to determine if the bad actor has moved to another part of the network? _____ <input type="checkbox"/> Are there any subnets/IPs to whitelist? (eg Crowdstrike or other MDR) _____
<p>3.2b Detailed Containment Methods - Service</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Service Containment <ul style="list-style-type: none"> <input type="checkbox"/> Who has the authority to make a decision to disable the service? _____ <input type="checkbox"/> Are the directions clearly outlined and hardware identified (labeled)? <input type="checkbox"/> What are the actual steps to disable the service? _____ <input type="checkbox"/> Do you need to disconnect the entire system or only a portion? _____
<p>3.2c Detailed Containment Methods - Server</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Server Containment <ul style="list-style-type: none"> <input type="checkbox"/> How might you disable the access to and from the server? _____ <input type="checkbox"/> How do you isolate a single server or machine with Crowdstrike? <ul style="list-style-type: none"> <input type="checkbox"/> Host Management and Setup > Host Management > Select the host(s) in question > Actions > Contain Host

<p>3.2d Detailed Containment Methods - User</p>	<ul style="list-style-type: none"> <input type="checkbox"/> User Containment <ul style="list-style-type: none"> <input type="checkbox"/> How do you disable a user account? _____ <input type="checkbox"/> How do you isolate a remote user device? _____
<p>3.2e Detailed Containment Methods - Cloud</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Cloud Service Containment <ul style="list-style-type: none"> <input type="checkbox"/> How do you isolate a cloud service or device? _____ <input type="checkbox"/> How do you remove malicious email messages from user mailboxes? _____

Stage 4



Description: Removing all traces of an incident and restoring systems to normal operations.

Label	Description
4.1 General	<p>After ensuring evidence has been preserved for legal and insurance purposes, eliminate all traces of the incident. This may entail:</p> <ul style="list-style-type: none"><input type="checkbox"/> Correcting any misconfigurations identified<input type="checkbox"/> Patching or upgrading all affected systems to fix exploited vulnerabilities<input type="checkbox"/> Removing any unauthorized accounts<input type="checkbox"/> Resetting passwords for compromised accounts<input type="checkbox"/> Revoke and reissue security certificates, MFA tokens, SSO/OAUTH/SAML connections to resources<input type="checkbox"/> If a domain administrator/root/SA-level account has been compromised, all account passwords may need to be reset or the account directory may need to be rebuilt.<input type="checkbox"/> Reimaging systems affected with malware <p>Caution: To preserve evidence and ensure unwanted programs/backdoors do not cause recurring issues, some devices may need to be replaced, rather than remediated.</p>
4.2 Malicious Email	<ul style="list-style-type: none"><input type="checkbox"/> How do you remove malicious email messages from user mailboxes?<input type="checkbox"/> Follow up with the source of the malicious email if appropriate
4.3 Eradication Tools	<p>Eradications tools, which may be at your disposal, include:</p> <ul style="list-style-type: none">• Endpoint configuration management tools (via Intune/SCCM and/or via AppLocker, JAMF, Google Chrome Device Management, etc.)• EDR/Antivirus controls

Stage 5



Description: Restore services and capabilities that have been impaired by a cyber security event.

Description	Description
5.1 Recover and restore IT operations	<p>Based on priorities and estimated recovery timelines, repair, restore, rebuild, or replace systems that were taken offline or otherwise affected by the incident.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Reference any existing plans (such as disaster recovery, business continuity, etc) for prioritization and dependencies. <input type="checkbox"/> Replace/restore/reimage systems: <ul style="list-style-type: none"> <input type="checkbox"/> Verify backups have not been tampered with <input type="checkbox"/> Roll back to known good system state (but monitor for indications of compromise/latent malware) <input type="checkbox"/> Consider creating an isolated network or a new cloud computing instance to protect recovered systems from re-compromise. <input type="checkbox"/> Reset, restore, or recreate potentially compromised accounts
5.2 Continue to Monitor for Anomalous Activity	<p>It is critical to maintain vigilance even after IT operations have been successfully restored. Attackers often insert additional entry methods in order to regain access.</p>
5.3 Update Stakeholders on Recovery Status	<p>Providing regular, high-quality communications about incident recovery helps maintain trust in the organization and executive leadership.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Be aware of regulatory requirements for mandatory reporting of incidents like data breaches, which may require quick-turnaround notifications

Recovery

District Recovery Methods

Description: Specific restore methods—the “how to”—vary by district. Details should be identified in this section.

Restoration of actual systems or services require additional considerations that need to be addressed prior to an actual event. While complete restoration steps are outside the scope of this document, important considerations should be identified before an incident occurs in order to avoid delays. Use these questions to develop your organization’s own containment procedures.

How do you restore a server?	
How do you restore data?	
How do you restore your network infrastructure?	
How do you restore network device configuration?	
How do you reset passwords for all users?	

Stage 6



Description: Identify what worked well, areas for improvement, and strategies to enhance incident response.

Label	Description
6.1 Conduct Post-Incident Review	<p>The work of the IR team is not complete until a comprehensive assessment is prepared and shared with appropriate parties.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Identify and resolve any deficiencies in your current cybersecurity program (i.e., technologies, policies, and practices) that led to the incident. <input type="checkbox"/> Identify and resolve deficiencies in planning and execution of your incident response. <input type="checkbox"/> Assess whether additional cybersecurity risk management measures—technologies, policies, and/or practices—are needed to prevent a recurrence of the issue and strengthen the security posture of your organization. <input type="checkbox"/> Ensure the incident is sufficiently documented to meet public records, law enforcement, and/or insurance requirements. <input type="checkbox"/> Ensure information is released within the guidance provided by legal counsel.
6.2 Brief Executive Leadership	<ul style="list-style-type: none"> <input type="checkbox"/> As appropriate, prepare a final report to executive leadership on the incident and response. <input type="checkbox"/> Describe the root cause of the incident (non-technical) <input type="checkbox"/> Summarize the actions taken to respond and recover from the incident (non-technical) <input type="checkbox"/> Describe any remaining issues <input type="checkbox"/> Summarize actual recovery expenses incurred (such as labor, fees, consultants/contractors, equipment purchases, etc.) <input type="checkbox"/> Summarize recommended cybersecurity program improvements, including estimated costs
6.3 Brief other K12 Agencies	<ul style="list-style-type: none"> <input type="checkbox"/> Provide incident review to MiSecure, MiSEN or other related statewide services <input type="checkbox"/> Identify ramifications from the incident such as instruction days lost, financial impact, resources required, etc as allowed by legal
6.4 Implement Changes	<p>Implement recommended measures to strengthen the security posture of your organization.</p>

REFERENCES:

K12 Security Information eXchange: <https://www.k12six.org/>

- <https://www.k12six.org/news/k12-six-releases-essential-cyber-incident-response-runbook>

US Department of Commerce, National Institute of Standards and Technology (NIST)

- Computer Security Incident Handling Guide (800-61):
- <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>
- Guide for Cybersecurity Event Recovery (800-184):
- <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>

MiSecure.org

- [MiSecure Operations Team Incident Response template](#)

State of Michigan; Department of Technology, Management & Budget

- <https://www.michigan.gov/dtmb/services/cybersecurity/cyber-partners/cyber-incident-response>
- https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Services/Cybersecurity/MI_Sample_CyberSecurity_Incident_Response_Plan.docx?rev=b27553ead3a544818ac8eff429186013&hash=42A879C609B101CC270C077AC7780114