Incident Response Plan

Introduction

In the dynamic landscape of modern cybersecurity, the inevitability of encountering threats to our digital infrastructure underscores the critical importance of preparedness and swift response. This Incident Response Plan (IRP) serves as a cornerstone in our organization's commitment to proactive risk management and resilient operations. By formalizing our approach to incident response, we not only enhance our ability to minimize the impact of cyber incidents but also reinforce our commitment to safeguarding the confidentiality, integrity, and availability of our organization's assets and information.

Purpose

This document describes the Organization or agency's overall plan for preparing and responding to both physical and electronic information security incidents. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of this Security Incident Response Plan is to prepare for, detect, and respond to security incidents. It provides a framework by which the Incident Response Team (IRT) shall determine the scope and risk of an incident, respond appropriately to that incident, communicate the results and risks to all stakeholders, and reduce the likelihood of an incident from occurring or reoccurring.

Scope

This plan applies to the physical location, the information systems, all Criminal Justice Information (CJI) data, and networks of the MNC's and any person or device that gains access to these systems or data.

Definitions

Event

An event is an exception to the normal operation of infrastructure, systems, or services. Not all events become incidents.

Incident

An incident is an event that, as assessed by the staff, violates the policies of the MNC 's related to Information Security, Physical Security, or Acceptable Use; other MNC 's Incident policy, standard, or code of conduct; or threatens the confidentiality, integrity, or availability of information systems or CJI. Incidents will be categorized according to their potential for the exposure of protected data or the criticality of the resource, using a four (4) level system of: 0 – Low; 1 – Medium; 2 – High; 3 – Extreme.

Incidents can include:

- Data Breaching
- Malware/viruses/Trojans.
- Ransomware.
- Phishing.
- Unauthorized electronic access.
- Breach of information.
- Unusual, unexplained or repeated loss of connectivity.

• Unauthorized physical access.

• Loss or destruction of physical files, etc.

Criminal Justice Information

CJI is as defined in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and the Michigan Administrative Rules.

Evidence Preservation

The goal of any incident response is to reduce and contain the impact of an incident and ensure that information security related assets are returned to service in the timeliest manner possible. The need for a rapid response is balanced by the need to collect and preserve evidence in a manner consistent with state and federal laws, and to abide by legal and administrative requirements for documentation and chain-of-custody.

Incident Response

In accordance with the FBI CJIS Security Policy, based off the National Institute of Standards and Technology (NIST) Special Publication 800-61 rev. 2, the Incident Response Life Cycle consists of a series of phases—distinct sets of activities that will assist in the handling of a security incident, from start to finish.

Preparation

Preparation includes those activities that enable the organization to respond to an incident. These include a variety of policies, procedures, tools, as well as governance and communications plans.

• Security Awareness Training: All personnel are required to take FBI CJIS Security Policy compliant Security Awareness Training. This training must be updated at a minimum of every two years. Additionally, [agency name] requires [monthly, quarterly, biannual, annual] security awareness training provided through [provider]. This training covers additional ongoing threats to systems such as malware, phishing, social engineering, ransomware, and other threats as they become known.

• **Malware/Antivirus/Spyware Protections:** All information system terminals, as well as key information flow points on the network are protected by continuous defense against malware/antivirus/spyware and other known malicious attacks. These defense mechanisms are kept up to date without the need for end user intervention, and end users are restricted from accessing, modifying, disabling, or making other changes to the defense mechanisms.

• Firewalls and Intrusion Prevention Devices (IPD): Multiple firewalls and IPD are in place within the network to provide the necessary depth of defense. keeps all firewalls and IPD up to date with the latest security patches and other relevant upgrades, as well as maintaining an active backup of the latest security configuration.

• Personnel Security Measures: All MNC's personnel with access to CJI or those areas in which CJI is accessed, stored, modified, transmitted, or maintained have been cleared to the required Personnel Security standards set forth in FBI CJIS Security Policy section 5.12.1 and the Michigan Addendum.

• P**hysical Security Measures:** All locations within the [agency name] that house CJI or CJI-related information systems are secured to the required criteria set forth in FBI CJIS Security Policy section 5.9. Access to these secured areas and information systems are a need-to-know/need to-share basis and required agency authorized credentials for access and are under the direct control and management of the Company

• E**vent Logs:** Event logging is maintained at all applicable levels, capturing all the required events and content specified for CJI through FBI CJIS Security Policy sections 5.4.1.1 and 5.4.1.1.1, retained for the specified period, and reviewed weekly. • Patching/Updating: Systems shall be patched and updated as new security patches and hot fixes are released. Any software or hardware product that reaches the end of the manufacturer's service and support life for patching will be deemed out-of-compliance and replaced.

Staffing

The Organization will strive to maintain adequate staff levels and third-party support to investigate each incident to completion and communicate its status to other parties while it continues to monitor the tools that detect new events.

Training

No incident response capability can be effectively maintained over time without proper and ongoing training. The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested, and translated into recommendations for enhancements. All MNC staff will be trained on a periodic basis in security awareness, procedures for reporting and handling incidents to ensure a consistent and appropriate response to an incident, and that post incident findings are incorporated into policy and procedure.

Detection and Analysis

Detection: is the discovery of an event with security tools or through notification by an inside or outside party about a suspected incident. The detection of an

incident requires the immediate activation of the IRT as listed in Appendix A. The determination of a security incident can arise from one or several circumstances simultaneously. Means by which detection can occur include:

• Trained personnel reviewing collected event data for evidence of compromise.

• Software applications analyzing events, trends, and patterns of behavior.

• Intrusion Protection/Intrusion Detection devices alerting to unusual network or port traffic.

• The observation of suspicious or anomalous activity within a company facility or on a computer system. It is critical in this phase:

• To detect whether a security incident has occurred.

• To determine the method of attack.

• To determine the impact of the incident to the mission, systems, and personnel involved in

Analysis

Analysis of the incident indicators will be performed in a manner consistent with the type of incident. In the event of a physical incident, appropriate steps will be taken to determine weaknesses in either the physical security of the facility, its monitoring tools, or its training programs to assess areas for process improvement or change. For an electronic incident, will utilize [to perform static and dynamic analysis of malicious code, a review of information system boundary protections, determination of source code if applicable, the depth and breadth of the attack, if the attack has migrated to other systems on or off the network, and any other tasks appropriate to the type of incident experienced. These analyses can be performed either manually or utilizing automated tools dependent upon the situation, timeliness, and availability of resources'

Incident Categories

An incident will be categorized as one of four severity levels. These severity levels are based on the impact to [agency name] and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to company image, or impact to trust by customers and citizens, etc. The below table provides a listing of the severity levels and a definition of each severity level.

Severity Level	Description
0 (Low)	Incident where the impact is minimal. Examples may be e-mailing SPAM, isolated virus infections, etc.
1 (Medium)	Incident where the impact is significant. Examples may be a delayed or limited ability to provide services, meet **[municipality or county name]'s** mission, delayed delivery of critical electronic mail or data transfers, etc.
2 (High)	Incident where the impact is severe. Examples may be a disruption to the services and/or performance of our mission functions. proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting over 1 percent of employees, Public Safety systems are unavailable, or
3 (Extreme)	Incident where the impact is catastrophic. Examples may be a shutdown of all network services. proprietary or confidential information has been compromised and published in/on a public venue or site. Public safety systems are unavailable. Executive management must make a public statement.

Incident Reporting

If an incident involves or is suspected of involving criminal justice information, the MSP Information Security Officer (ISO) will be contacted and provided a CJIS-016 "Information

Security Officer (ISO) Security Incident Report". The CJIS-016 is available under the Manuals, Policies, & Laws link at www.michigan.gov/lein

Containment, Eradication, and Recovery

Containment

Containment is responsible for containment and will document all containment activities during an incident. Containment activities for security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. This requires intelligence gathered by the detection and analysis phases of t he incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication

Eradication efforts for a security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery

Recovery efforts for incidents will involve the restoration of affected systems to normal operation. This is dependent upon the type of incident experienced but may include actions such as restoring systems from backups, rebuilding systems from an agency approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Post-Incident Activity

Post-incident activities will occur after the detection, analysis, containment, eradication, and recovery from a security incident. One of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Important items to be reviewed and considered for documentation are:

• Exactly what happened, and at what times?

• How well did staff and management perform in dealing with the incident?

• What information was needed sooner?

• Were any steps or actions taken that might have inhibited the recovery?

• What should be done differently the next time a similar incident occurs?

• How could information sharing with other organizations have been improved?
•What corrective actions can prevent similar actions 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?

Post-incident activities will be incorporated into future training opportunities for all parties involved in the incident, from victims' system administration personnel to incident responders.

Escalation

The escalation process will be initiated to involve other appropriate resources as the incident increases in scope and impact. Incidents should be handled at the lowest escalation level that can respond to the incident with as few resources as

possible to reduce the total impact and maintain limits on cyber-incident knowledge

Severity Level	Response Team Member Involvement	Description
0 (Low)	• IT Technical Support Staff or vendor. • Local Agency Security Officer (LASO).	Normal operations.
1 (Medium)	• IT technical support staff or vendor. • LASO. • IT Director.	is aware of a potential or actual threat and is responding to that threat.
2 (High)	• IT technical support staff or vendor. • LASO. • IT Director. • County Administrator/Controller.	An obvious threat has impacted business operations. Determine course of action for containment and eradication. Message staff of required actions and operational impacts if necessary.
3 (Extreme)	• IT technical support staff or vendor. • LASO. • IT Director. • County Administrator/Controller. • Finance Director. • Legal Contact. • **[Spokesperson title]**	Threat is widespread with significant impact. Determine course of action for containment, mitigation, and eradication. Message staff and officials. Prepare for legal action. Prepare for a public statement.

Incident Response Team

1) The person who discovers the incident will [enter action to be performed]. List possible sources of those who may discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:

a) Helpdesk.

b) IT Manager.

Usually, each source would contact one reachable entity 24/7 such as a grounds security office. Those in the IT department may have different contact procedures than those outside the IT department.

2) If the person discovering the incident is a member of the IT department or affected department, they will proceed to step four (4).

3) The Helpdesk/manager/IT Staff will refer to the IT emergency contact list or effected department contact list and call the designated numbers in order on the list. The Helpdesk will log

a) The name of the caller.

b) Time of the call.

c) Contact information about the caller.

d) The nature of the incident.

e) When the event was first noticed, supporting the idea that the incident occurred.

4) The IT staff member or affected department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff members will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages. The staff member will log the information received in the same format as the ground's security office in the previous step. The staff member could possibly add the following:

a) Is the system affected business critical?

b) What is the severity of the potential impact?

c) Name of system being targeted, along with operating system, Internet Protocol (IP) address, and location.

d) IP address and any information about the origin of the attack.

5) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

a) Category one - A threat to public safety or life.

b) Category two - A threat to sensitive data.

c) Category three - A threat to computer systems.

d) Category four - A disruption of services.

6) Team members will establish and follow one of the following procedures basing their response on the incident assessment:

a) Worm response procedure.

b) Virus response procedure.

c) System failure procedure.

d) Active intrusion response procedure - Is critical or sensitive data (Personally Identifiable Information (PII), CJI, etc.) at risk?

e) Inactive Intrusion response procedure.

f) System abuse procedure.

g) Property theft response procedure.

h) Website denial of service response procedure. i) Database or file denial of service response procedure. j) Spyware response procedure.

The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.

8) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

9) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems. Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

a) Reinstall the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.

b) Make users change passwords if passwords may have been sniffed.

c) Be sure the system has been hardened by turning off or uninstalling unused services.

d) Be sure the system is fully patched.

e) Be sure real time virus protection and intrusion detection is running.

f) Be sure the system is logging the correct events and to the proper level.

10) Documentation—the following shall be documented:

a) How the incident was discovered.

b) The category of the incident.

c) How the incident occurred, whether through email, firewall, etc.

d) Where the attack came from, such as IP addresses and other related information about the attacker.

e) What the response plan was.

f) What was done in response?

g) Whether the response was effective.

12) Evidence Preservation: make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond, in case of an appeal.

13) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.

14) In the event of a loss or suspected loss of criminal justice information, contact the Michigan State Police Information Security Officer via the CJIS-016 Form available on the LEIN Website .

15) Review response and update policies plan and take preventative steps so the intrusion can't happen again.

a) Consider whether an additional policy could have prevented the intrusion.

b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.

c) Was the incident response appropriate? How could it be improved?

d) Was every appropriate party informed in a timely manner?

e) Were the incident response procedures detailed, and did they cover the entire situation? How can they be improved?

f) Have changes been made to prevent reinfection? Have all systems been patched, systems locked down, passwords changed, antivirus updated, email policies set, etc.?