

**Miami Valley Risk Management Association Incident Response Plan**

This document discusses the steps taken during an incident response plan for MVRMA

## **1.   Overview**

Information security incidents represent a significant risk to the organization.  MVRMA must take appropriate steps in the event of an information security incident to minimize the impact and scope of the incident.

## **2.   Purpose**

This procedure outlines the escalation process for information security incidents related to MVRMA information.

## **3.   Scope**

This procedure applies to any system, service, device, process, or media that is used to access, store, or transmit institutional data in electronic, audible, or physical formats.  This procedure applies to personally owned systems, devices, and media; MVRMA owned systems, services, devices, and media; and third-party service providers.

## **4.   Definitions**

* **Information Security Incident** – Any attempt or act toward unauthorized access, use, disclosure, modification, or destruction of information including, but not limited to, interference with information technology operation and violation of MVRMA Rules, IT policies and standards, and applicable laws and regulations.
	+ Examples of Information Security Incidents include, but are not limited to:
		- Computer system breaches
		- Theft or loss of systems, devices, or media
		- Unauthorized access to, or use of, systems, software, or data
		- Unauthorized changes to systems, software, or data
		- Website defacement
		- Denial of service attacks
		- Impersonation of systems or people
		- Interference with the intended use of IT resources
		- Compromised user accounts
		- Presence of an unauthorized application, such as malware.
* **Incident Response Team** – The individual responsible for investigating data breaches and other information security incidents.  These individuals may include, but are not limited to MVRMA Staff, MVRMA 3rd party IT Consultant, Cyber Insurance provider and local, state, and federal law enforcement agencies.
* **MVRMA Incident Handler** – The Loss Control Manager is the staff lead of incident response efforts, unless otherwise designated by the Executive Director.
* **Institutional Data** – Any information or data that is gathered, analyzed, or published by any department of MVRMA in support of its mission(s).

## **5.   Reporting**

It is important that actual or suspected information security incidents are reported as early as possible to limit the damage and cost of recovery.

* **IMMEDIATELY** report any suspected or suspicious activity to HCST, MVRMA IT Service Provider
	+ **Barry D. Hassler** / President
	barry.hassler@hcst.com
	support@hcst.com
	**HCST** Office: (937) 427-9000 (main) (937) 688-3833 (Springfield)
	1430 Oak Court, Suite 312 / Beavercreek, OH USA
	[https://hcst.com](https://hcst.com?utm_source=email&utm_name=barry.hassler)
* **IMMEDIATE NOTICE** must be made to Beazley Group of all potential claims and circumstances (assistance, and cooperation clause applies)
* Cyber Liability Carrier Beazley NY needs to also be provided with Notice of Claim immediately:

Beth Diamond

Beazley Group

Address: 1270 Avenue of the America’s, Suite 1200

New York, NY 10020

Fax: (546) 378-4039

Email: tmbclaims@beazley.com

Elaine G. Tizon, CISR

Assistant Vice President, Claims Advocate

Address: 100 Pine Street, 11th Floor

San Francisco, CA 94111-5101

Voice: (415) 403-1458 Fax: (415) 403-1466

Email: elaine.tizon@alliant.com

Attn: TMB Claims Group

1270 Avenue of the Americas

New York, NY 10020

866-567-8570

bbr.claims@beazley.com

[**Link to Beazley Online Reporting**](https://www.beazleybreachsolutions.com/usa/report_an_incident.html)

## **6.   Response**

* The MVRMA Incident Handler for the suspected information security incident will manage the response at the MVRMA organization level.
* The incident response effort is comprised of six prioritized remediation activities:

1.  Containment
2.  Data Collection/Recovery
3.  Analysis
4.  Notification
5.  Reporting
6.  Data Retention

* Containment
	+ Whenever possible, the Incident Handler/designated 3rd party IT specialist will perform a network quarantine at the time of a reported/suspected incident and/or instruct the system administrator to unplug the network cable of the suspected machine.
	+ The Incident Handler/ designated 3rd party IT will quarantine potentially compromised host(s) at the time of containment and promptly reach out to the system administrator or system owner to create a plan to contain the incident. Note that the Incident Handler may quarantine/notify additional hosts based on suspicious behavior pending verification. In cases where the impact of system downtime is very high, the Incident Handler will work with system administrators to determine the level of account privilege and eliminate their access safely.
	+ All user privileges will be suspended immediately after the originating UID is determined until such a time that future risks are non- existent.
	+ Once a threat is verified, the Incident Handler will notify the Executive Director and staff and continue to remediation priority 2 (Data Collection/Recovery) and proceed sequentially through all remaining priorities.
	+ Once a threat is ruled non-existent, the Incident Handler will reinstate user privileges and continue to remediation priority 5 (Reporting) and proceed sequentially through all remaining priorities.
* Data Collection/Recovery
	+ The Incident Handler will collect data from the third-party service providers to quickly assess the scope of the incident, including:
		- Preliminary list of compromised systems and/or services
		- Preliminary list of storage media that may contain evidence and/or compromised data
		- Preliminary incident timeline based on initially available evidence
		- Examination of logs should begin
		- Modes of data recovery, if needed, should begin being examined after the scope of the incident is realized with the goal being a return to departmental productivity with minimal data loss
		- Data recovery should begin once the threat is quarantined and deemed to be non-threatening
* Analysis
	+ The Incident Handler will establish whether there is reasonable belief that an attacker(s) successfully accessed Protected Institutional Data.
	+ The Incident Handler will generate an incident timeline and ascertain the impacts and/or actions of all parties to identify the details of the compromise.  When possible, a full back-up or system image may be necessary for analysis.
	+ The Incident Handler will coordinate the communication between stakeholders including data owners, data stewards, data custodians, and any relevant compliance officers.
* Notification
	+ The Incident Handler will provide the Executive Director with the following information:
		- Complete list of compromised systems and/or services and associated UIDs
		- Complete list of storage media that may contain evidence and/or compromised data
		- Incident timeline based on initially available evidence
		- All results of the analysis
* Reporting
	+ The incident handler/ designated 3rd party IT specialist will draft the final incident report after the analysis and notification priorities are complete and submit it to Information Security for discussion. Preliminary reports should be avoided whenever possible since working conclusions can change substantially through the course of an investigation.
	+ Technical personnel participating in the containment, data collection/recovery, or analysis can offer incident reports for their participation to be included within the final incident report, but typically technical issues should be resolved by this stage.
	+ For critical incidents involving HIPAA related data, HIPAA Breach Notification Rule requirements for notifying appropriate parties of the incident shall be used.
	+ **It is the data and/or application owner’s responsibility for breach notification when no established regulatory notification requirements exist.**
* Data Retention
	+ Information Security will archive the final report in case it is needed for reference in the future; reports must be retained for twelve (12) months.
	+ Incident notes should be retained by the incident handler for twelve (12) months from the date that the report is issued.
	+ Raw incident data should be retained by the incident handler for thirty (30) days from the date that the report is issued. This includes disk- images, unfiltered netflow-content, raw file-timelines, and other data that was collected but deemed not relevant to the investigation.

## **7.   Related Documents**

 [Cyber Coverage Evidence Attachment](https://storage.googleapis.com/proudcity/mvrmaoh/uploads/2021/07/Cyber-Program-Summary.pdf)

 [APIP Cyber Excess Evidence of Coverage](https://storage.googleapis.com/proudcity/mvrmaoh/uploads/2022/01/20-21-APIP-Cyber-Excess-EOC_MVRMA.pdf)

[Beazley First Responder Guide](https://www.beazleybreachsolutions.com/usa/first_responder_guide.html)