Incident Response Policy

Effective Date:	Changes:	Approved by:	Version :
12/13/23	Initial Document Creation	Board of Trustees	1.0

Contents

1. Overview

Security incidents represent a grave threat to the Microsociety Academy Charter School (MACS). Timely response to a security incident can mean the difference between a minor security incident and a major security breach with far-reaching consequences. This policy is designed to guide actions to help prevent security breaches and to mitigate the consequences of a breach quickly and efficiently if one does occur. This policy also defines roles and responsibilities for the Incident Response Team.

This policy applies to all staff, systems, and data that make up MACS' organization and its Information System.

An Incident, for the purposes of this policy is, **any potential unauthorized access to the Information System or exposure of information.**

Examples of potential incidents for this Information System include but are not limited to:

1. Lost or stolen access devices
2. Unauthorized physical access
3. Unauthorized logical access
4. Suspicious activity identified in an audit
5. Suspicious activity identified by a user
6. System alerts from security layers (firewalls, antivirus, SIEM, etc.)
7. Evidence of physical data being removed from the system

2. Policy Implementation and Updates

The MACS Executive Director is responsible for:

1. Approving of the Incident Response Policy
2. Providing management commitment to support implementation of the Incident Response Policy
3. Ensuring organizational compliance with the Incident Response Policy

The MACS Assistant Directors are responsible for:

1. Disseminating the Incident Response Policy to all team members with defined Information Technology and/or Security roles and responsibilities
2. Reviewing and updating the Incident Response Policy annually, at a minimum, and in the event of a major system change
3. Providing training to end users on administrative controls described in the Incident Response Policy

Mainstay Technologies is responsible for:

1. Overseeing the implementation and management of all technical controls described in the Incident Response Policy
2. Providing training to end users on technical controls described in the Incident Response Policy

3. Incident Response Roles and Responsibilities

The Incident Response Team's (IRT) goal is to mitigate or prevent loss to the Organization by providing rapid and skillful response to a potential or actual incident. Loss could be in the form of negative financial impact, public reputation, lack of regulatory or legal compliance, business interruption, or breach of data.

Any suspected incidents must be reported to the IRT immediately by contacting Mainstay Technologies (support@mstech.com or 603-524-4774 Option 1).

The combined IRT has the expertise and authority to properly diagnose, report, and manage incidents on behalf of MACS.

The MACS Incident Response Team includes:

Role	Owner	Back-Up	Description
IRT Lead	Susannah Williams, Assistant Director	Amy Bottomley, Executive Director	Has authority to confirm the incident type and categorization in coordination with Mainstay Technologies. Acts as coordinator for internal incident response. Provides management oversight of the incident handling process.
IT Infrastructure Response	Mainstay Technologies		Conducts initial technical triage and reviews all applicable server or network logs. Completes technical reviews, documents findings, and supports recovery efforts as needed.
Cybersecurity Response	Mainstay Technologies		Confirms adherence to Information Security policies throughout incident handling. Acts as liaison for external investigators as well as third-party information security vendor(s); coordinates with the IRT Lead regarding the handling of evidence.

			Prepares Incident Lessons Learned report. Works as a Security Operation Center reviewing all logs on but not limited to antivirus and intrusion detection to investigate anomalies and document the root cause of the incident along with containment of the incident. Once the incident has been contained and remediated, works to bring all systems online.
Communication	Amy Bottomley, Executive Director	Susannah Williams, Assistant Director	**Internal Communications:** Determines the impact to the internal staff and dictates what information can and should be made available to staff. **External Communications:** Determines the impact to external clients and manages communications in conjunction with the IRT and Leadership team. The Communications Resources work to initiate any crisis communication planning as needed.
Human Resources	Amy Bottomley, Executive Director		Handles any incidents in which employee negligence or misconduct is part of the incident.
Physical Security	Susannah Williams, Assistant Director		Confirms any physical security breaches and works with the IRT to review and document security camera footage, badge access reports, and other physical access records deemed necessary.
External 3rd Parties	Amy Bottomley, Executive Director		After informed by the IRT Lead, determines if external Legal counsel will be brought in as part of this process.

			Works with the IRT and Executive leadership to determine if the incident in progress requires the Insurance company to be alerted.

MACS IRT members are provided with incident response training within 30 days of assuming an incident response role or responsibility, with additional training(s) provided as needed but at least on an annual basis thereafter.

Training will be conducted via annual tabletop exercises and a review of this policy. MACS maintains training records.

4. Incident Response Policy Phases and Procedures

MACS' Incident Response Program includes the following phases: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. Incident Response Phases are coordinated with Contingency Planning Phases for effective response activities.

1. *Preparation*: The preparation phase encompasses all actions taken to prepare for Incident Response. Training is essential to Incident Response preparation. The IRT must be properly trained to handle incidents, and all staff must understand the escalation process.
2. *Identification:* When an incident is reported or detected, the identification phase begins. Incidents must be logged with as much detail as possible as early as possible. All incidents will be manually logged by the IRT, and any client-specific Incident Response handling criteria is consulted.
3. *Containment:* Containing and limiting the impact of an incident is a critical aspect of the containment phase. The portion of the Information System impacted should be isolated immediately and to the maximum extent possible following identification. Members of the IRT should be careful to properly log and preserve as much evidence as possible while deciding how to contain the situation and limit further damage.
4. *Eradication:* The Information System must be cleared of all vulnerabilities associated with the incident. The goal is to confirm that the Information System is stable and is no longer vulnerable to repeated exploit, vulnerability, or issue.
5. *Recovery:* The Information System should be brought back online with the following considerations:
    a. Consult all applicable Contingency and Business Continuity policy guidance.
    b. Certify data integrity.

c. Certify a clean system and confirm that all necessary layers of security protection are in place.
d. Confirm functionality and business routines with a select group.
e. Confirm continuous monitoring of the impacted Information System.

6. *Lessons Learned:* The IRT with MACS leadership should review the entire incident as soon as possible following the completion of the Recovery phase. Actions should include:

a. Create a follow-up report.
b. Create a post-incident internal and external communications plan if needed.
c. Inspect incident documentation for thoroughness and accuracy.
d. Confirm that evidence is properly archived and either in alignment with records retention policies or logged as an exception.
e. Identify anything that would improve future incident response capabilities and integrate changes into the existing plan or other plans such as Business Continuity and Disaster Recovery (BCDR).
f. Review plans to implement new security layers and or policies and procedures to prevent future incidents.
g. Consider integrating similar incidents into future IR and BCDR testing and tabletop exercises.
h. Consider incorporating any new improvements into future budget and strategic planning.
i. Identify additional training opportunities that may assist in future incident prevention.
j. Measure any residual impact to the organization and track ongoing preventative plans and activities.

5. Incident Tracking and Categorization

All facts, documentation, and data related to the incident must be recorded to aid in the incident handling process and future review. Whenever possible, IRT members should work in teams of two so that one person can perform technical tasks and the other can perform logging activities. Where necessary, the IRT should safeguard and restrict access to sensitive information related to the management of the incident. This could be a major containment factor for data integrity, chain of custody, and communications security.

The IRT is responsible for tracking the incident lifecycle.

The incident documentation should contain the following whenever possible:

1. Names and roles of individuals involved
2. Date and time stamps
3. Incident summary
4. Current status and any earlier status changes
5. Correlated incidents, if applicable
6. All actions taken by incident handlers

7. Impact assessment
8. Contact information for any critical resources
9. Evidence – links, lists, or attachments
10. Details regarding other information systems that are or may be at risk
11. Reports from IRT members
12. Next phase or step in the process and timeframe if available

MACS will categorize reported incidents utilizing the four following incident classifications:

1. Malfunction(s) due to design/implementation errors or omissions
2. Untargeted malicious attack(s)
3. Targeted malicious attack(s)
4. Insider threat(s)

Incident categorization may guide or impact response activities as deemed appropriate by the IRT Lead.

6. Testing

The organization conducts testing of the incident response capability at least annually. In the event a security incident is reported requiring the activation of the Incident Response Policy and supporting procedures within the most recent 12-month period, the results and lessons learned of the reported incident may replace the testing exercise for the current year.

When applicable, Incident Response and Business Continuity and Disaster Recovery Testing are coordinated to ensure they do not contradict each other's objectives or result in duplicate efforts/activities.

Board Approved: 12/13/23