Cybersecurity Incident Response Plan

THIS DOCUMENT IS CLASSIFIED AS:

Public (Template Only)

DISTRIBUTION: Authorized Technology Department Engineers Only

Table of Contents

Date	Version	Revised by	Summary of Changes
11/11/2020	1.0		Initial document creation

1.0 Detect

1.1 Detect Purpose

Although information may be incomplete, initial input from the person who discovers an incident will be useful for subsequent investigation.

1.2 Detect Procedure

a. The person who discovers the incident will create a Ticket
b. If the user is NOT part of the IT department, they will contact their technician for an initial interview.

1.3 Ticket Content

a. What equipment is involved?
b. What user is involved?
c. How was the incident detected?
d. When was the incident detected?
e. Why the user thought an incident has occurred?
f. Location

Further information should be gathered by the technician

a. Is the equipment business critical?
b. IP address and MAC address
c. Other useful information

2.0 Assessment

2.1 Assessment Purpose

What level of intervention is required?

2.2 Assessment Procedure

a. The IR team will read the ticket
b. A new categorization based on privilege, maliciousness, and automatic ATP response will be added
    - Privilege: is the account or system related to PII or is mission critical
    - Maliciousness: Discovery or lateral movement
    - ATP Response: Is Microsoft ATP sufficient or is a manual response required

2.3 Assessment Determinations

a. Is the incident real?
b. Is the incident still in progress?
c. Is the account compromised?
d. What is the impact if the attack succeeds?
    - Scope? Class or school wide? District wide?
e. Is a response urgently required?
f. What response is appropriate?
    - Isolate, Analysis, Reimage?
g. Will the response alert the attacker?
    - Does it matter?

3.0 Response

3.1 Response Purpose

This could be a general Response Procedure, or different procedures can be made for different incidents, i.e., Worm, Virus, System Failure, Ransomware, etc.

3.2 Triage Procedure

a. Based on the Assessment, use the related response
b. If the response below was insufficient, remember to document the steps to improve the process

3.2.1 Critical Response

a. Escalate to engineer or supervisor

3.2.2 High Response

a. Restrict App execution in ATP
b. Isolate the system in ATP
c. Contact Systems Administrator/Engineer to disable the account
d. *Notify ITS or User?* & Create a Ticket
e. Obtain infected device
f. Monitor logs for signs of continued activity
g. Perform analysis

3.2.3 Normal Response

a. Temporarily isolate or restrict app execution to confirm scope
b. *Notify ITS or User?* & Create a Ticket
c. Change the account password
d. Give staff a loaner computer if necessary
e. Perform manual remote remediation as required

3.2.3 Low Response

a. Microsoft ATP took care of it, right?
b. Check logs to ensure infection prevented

3.3 Forensics Procedure if ≥ High

a. If necessary, get Safety involvement for chain of custody
b. Obtain sample and determine purpose
    - Files modified? Registry? IPs connected? Data Exfiltration?
c. Review system logs
d. [if ≥ High] *Interview victim to determine incident cause?*

3.4 Recovery Procedure

a. Reimage if necessary
b. Ensure newest image used
c. Ensure device is onboarded into ATP and agent online
d. Restore from backups as necessary

4.0 Report

4.1 Report Purpose

To ensure procedure effectiveness, reports should consolidate all the information (infection, remediation) for review.

4.2 Incident Report Procedure if ≥ High

a. Type of incident
b. Incident start date
c. Date incident detected
d. Location of incident
e. Who detected the incident
f. How incident was detected
g. Scope of incident
h. Date incident remediated
i. Summary of incident
j. Suggestions for prevention

4.3 Subjective Improvement Procedure

a. What went well?
b. What needs improvement?
c. Suggestions for training
d. Any amendments to the IR Plan?

5.0 Review

5.1 Review Purpose

It is necessary to debrief management and determine what changes are applicable.

5.2 Review Procedure

a. Review reports
b. Communicate to stakeholders
c. Begin change control, if appropriate

5.3 Optional Stakeholder Communication Procedure

d. Contact Communications Department
e. Contact school administration

80.0 Definitions

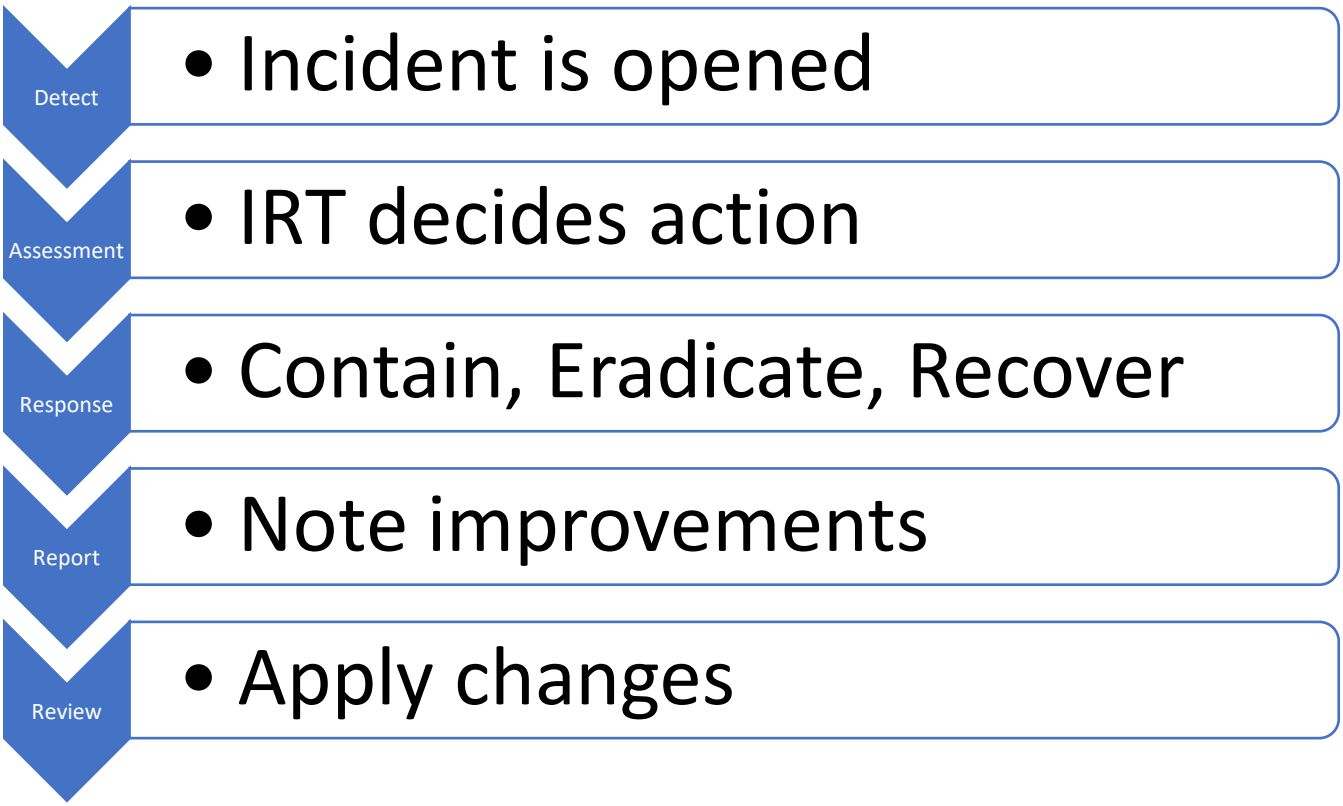
80.1 Incident (cybersecurity)

A Cyber Security Incident is any event that threatens the confidentiality, integrity, or availability of the information resources we support or utilize internally, especially sensitive information whose theft or loss may be harmful to individual students, our partners or our organization

80.2 Incident Response Team

The incident response (IR) team is the cybersecurity group

80.9 Flowchart



81.0 Incident Response Team

81.1 Cybersecurity Administrator/IR Manager

81.1.1 Jan Doe

Email:

Phone:

Cell:

81.2 Cybersecurity Incident Specialist

81.2.1 Jon Doe

Email:

Cell:

82.0 Related Groups

82.1 Security Operations Team

List names here

82.2 Escalation

List names to escalate

81.3 Legal Team

If necessary: Human Resources

81.6 Communications Team

If necessary: Communications Department