Cybersecurity Incident Response Plan

Organization

Date/Revision

Purpose of Plan

Event or Incident

Event: an occurrence in the environment that reflects a change in normal behavior. Events can be positive or negative.

Example: a suspicious email is identified

Incident: a change in the environment that negatively impacts the organization.

Examples: a cyber attack that impacts processes, a phishing email that harvests login credentials

Reporting an Event or Incident

- A workflow process and reporting system will be identified for the purpose of reporting events and incidents to determine the appropriate action of response.

Phases of the Plan

Preparation/planning

Identify

Containment

Eradication

Recovery

Lessons learned

Review, Test, Train, Maintain

Preparation/Planning

Create a Contact List - APPENDIX IV

Develop a work order and reporting system - APPENDIX I

Build a team of responders (CIRT) - APPENDIX III

Assign roles and responsibilities

Consider temporary elevation of permissions

Consider location and skills for team placement

Consider outside assistance

- *Vendors*
- *Neighboring organizations*

Cross training

Maintain a checklist-The checklist begins at the Identify phase.

Communication

- *Communicate milestones to the team leader*
- *Establish communication channels for external and internal entities*

Perform a risk assessment

Identify potential risks, their likelihood and level of impact - **APPENDIX VI**

Assign a score to each risk to help with prioritization

Identify the symptoms and mitigations – Review *Possible Symptom Chart* below

SYMPTOMS

Pop-ups
Web site redirects or broken links
Repetitive unsuccessful login attempts
Users report suspicious activity (phishing)
Unexplained new user accounts
Unexplained new files or unfamiliar file names
Unexplained modifications to files
Missing or deleted data
Disruption of service
User account inaccessible
System crashes
Poor or sluggish system performance
Bandwidth consumption spikes
Unusual system resource consumption
Unauthorized changes to user permissions or access
Alerts from internal systems

Include recovery time and recovery point objectives

Identify business functions - **APPENDIX V**

Business Function	
System	Food Service
Location	Ele, MS, HS
Stakeholders	Food Service staff
Purpose of system	Point of Sale, meal planning, meal counts, reporting
Dependencies	Internet, software, laptop
Critical Processes	Point of Sale

Sample Business Function Identifier

Contingencies

Personnel

Recruit 3rd parties or managed service providers if needed

Structures

Identify alternate locations for recovery

Tools

If a particular tool is not available, alternates need to be identified.

Example: Internet is down = hotspot, rerouting of traffic to use internal resources (eliminate WAN to use LAN)

Tools: Software and Hardware

Jump bag

Logs and Analysis

Eradication

Preservation

Identify

Verify an incident has occurred

Determine the scope and impact

This Document is closed under RSMo 610.021 Section 21

Mitigation strategies
Refer to the threat identification chart and possible playbooks for detailed instructions.

Recovery time and point

Report incidents to proper authorities (within 4 hours)

DESE-mandated: https://dese.mo.gov/sites/default/files/dac_forms/MO5003218.pdf

State auditor-mandated: https://auditor.mo.gov/SchoolDataBreachHotline/Form

P3-State Fusion Centers: https://www.p3tips.com/TipForm.aspx?ID=2600&TemplateID=129

CISA- https://www.cisa.gov/report

FBI- https://www.ic3.gov/Home/ComplaintChoice

Containment

Remove affected system from the network. Leave powered on.

Limit the scope and magnitude

Root cause analysis

Eradicate

Clean it up

This Document is closed under RSMo 610.021 Section 21

Rebuild or replace

Validation

Communication

Documentation

Recover

Recovery time objective
Determine the amount of time to restore processes

Recovery point objective
Determine a point of restoration. Bring up critical processes first

Restore-partial or full

Validation and testing

Identify a clear demark for when command is transferred

Learn

What happened?

Gaps in the plan

Documentation

Review, Test, Train & Maintain

Paper walk-through

- *Review plan details*

Functional exercise

- *Scenario walk-through*

Field exercise

- *Performing the work*

Full interruption

Review

- *Risk management*
- *Business impact*
- *Scope, timeline, requirements, constraints*

Appendices

Appendix I – Work Order/Reporting Form

Incident Response Work Order

Date: _____ Time: _____

Incident: _____

Reported by: _____

Location: _____

Description of incident/symptoms:

_____

_____

_____

_____

_____

_____

_____

Responded by: _____

Incident Response Plan initialized: Yes ☐ No☐

Date: _____ Time: _____

Appendix II – Service Agreements-Identify 3rd party vendors for services and applications

Service Provider	Service	Contact
MOREnet	Internet Service Provider	573-884-8694 help@more.net or security@more.net

Appendix III – Incident Response Team

Role	Name	Phone
Leader *Alternate*		
Investigator *Alternate*		
Internal Comm *Alternate*		
External Comm *Alternate*		
Documentation *Alternate*		
IT Assist *Alternate*		
Legal Representative		

Appendix IV – Contacts List

Contact	Name(s)	Phone
Superintendent		
CIO, CFO, Tech Director		
Communications Director		
General/Legal Counsel		
HR Director		
Insurance Co-Cyber Risk Policy		
Law Enforcement		
Credit Monitoring Services		
Vendors		

Appendix V – Business Functions- These categories can be broken down into sub-categories

Business Function	Importance	
Facilities	Mission Critical ☐ Important ☐	Vital ☐ Minor ☐
Finance	Mission Critical ☐ Important ☐	Vital ☐ Minor ☐
Human Resources	Mission Critical ☐ Important ☐	Vital ☐ Minor ☐
IT	Mission Critical ☐ Important ☐	Vital ☐ Minor ☐
Food Service	Mission Critical ☐ Important ☐	Vital ☐ Minor ☐
	Mission Critical ☐ Important ☐	Vital ☐ Minor ☐
	Mission Critical ☐ Important ☐	Vital ☐ Minor ☐

Appendix VI – Threat Chart

Risk	Recovery Time/Point	Threat	Symptoms	Mitigation
8	>1 hour Full recovery	Malware/Virus	Pop Ups, Sluggish, Unresponsive	Remove from network, anti-virus scan/clean, reimage, scan again (or reference playbook for details)

Appendix VII – Risk Matrix-Consider Recovery Time and Recovery Point Objectives

Unacceptable High Medium Low

	IMPACT				
Likelihood	Catastrophic 5	Critical 4	Serious 3	Minor 2	Insignificant 1
Almost Certain 5	25	20	15	10	5
Likely 4	20	16	12	8	4
Possible 3	15	12	9	6	3
Unlikely 2	10	8	6	4	2
Improbable 1	5	4	3	2	1