MiSecure

Incident Response Worksheet v2.0

Last updated: [Date Here]

Where does this document live?

Digital location: [Enter the on-line location]

Physical location: [Enter the location of a printout of this document, often in the Emergency Operations Plan]

Key Information

The resources listed below will almost certainly be critical during a cybersecurity incident. You should list where both physical and digital versions of this information exist. You should develop a process to keep an off-network version up-to-date.

Resource	Purpose / Note
Command Center Location [Enter Here]	This is the physical location in the building, away from technical operations, where the incident response team can eat, meet & retreat. This should not be in the IT operational area.
Out-of-band (OOB) Communication Method [Enter Here]	Define how you will communicate during the event. Members of the team will need access to devices that are secured, probably not attached to the local domain. All members will need access to a site such as Slack, … Where messages can be securely exchanged and files shared. Make sure your team does not use work email accounts on systems such as Slack. This should be tested regularly.
Location of Passwords [Enter Here]	Where are your passwords for key systems stored and/or backed up? This may be a backup of a Bitwarden or KeePass system or a simple printout of each team member's passwords.
Network Diagrams [Enter Here]	Where is the most recent print out of your network diagram. Network diagrams should include important IP and VLAN information as well as the physical location of MDF and IDF locations.
IP Addresses, VLANs & Routing Tables [Enter Here]	This should be a print of a digital backup of your IP address database. Your core routing table should also be included
How To Disconnect From The Internet [Enter Here]	This should list the physical location of the router / switch port(s) that need to be physically disconnected in order to disconnect from the Internet.

1. Incident Response Team Members

Enter the name of the person that will be primarily responsible for each role. You may consider adding a secondary person if feasible. One person may fill multiple roles. Individuals from other partner organizations may also fill roles. Make sure each member is notified and reminded regularly of their role and understand their responsibilities. Enter the name here and the contact information in the Appendix.

Role	Contact(s)	What They Do
Cyber Incident Response Management *Usually the superintendent, associate superintendent or principal. They need to have the authority to make major operational decisions for the district.*	**Name** Email Phone	• Decide whether to cancel school • Provides authorization for major steps such as whether to contact legal or insurance • Works very closely with the Coordinator to make these decisions • Support the ongoing effort to recover from an event • Coordinate the effort of the entire team
Cyber Incident Response Coordinator *Usually the IT Director. For smaller districts or bigger crises, this may be the ISD IT Director*	**Name** Email Phone	• Provide overall support to the entire team. • Make sure the right people are doing the right things. • Communicate to Administration.
[Lead] Technical Engineer(s) *Whoever manages the servers, backups, networks and firewalls.*	**Name** Email Phone	• Review extent of compromise • Able to change passwords and policies • Review EDR reports / alerts • Access user activity logs

Role	Contact(s)	What They Do
Technical Support Team *Multiple names may go in here. Google Workspace admins, Field technicians. This team will change depending on the specifics of the event*	**Name** Email Phone	● Review user email activity ● Access server logs ● Manage firewalls and review logs ● Check various servers and systems for compromise and manage those servers
Administrative Support / Incident Recorder *Usually an administrative assistant familiar with the technology department*	**Name** Email Phone	● Maintains the incident logs ● Provide lunches ● Run errands
Communications / Media Team *The PR or HR Director if there is one or someone from the Business Office. Could also be a principal or other administrator*	**Name** Email Phone	● Manage public communications ● Manage staff communications ● Manage parent/student communications ● Maintain backup communication methods for parents ● Set up a call center ● Talk to press or prepare talking points for other leaders ● Develop a call tree for front-line communications ● Update social media
Data Governance *Usually principals or guidance counselors. Whoever manages student data imports and exports*	**Name** Email Phone	● Determine severity of data leaks ● Identify most likely data sources that may have been breached ● Contact appropriate reporting authorities
Business / Finance *The Business Manager and possibly other staff from the business department*	**Name** Email Phone	● Review financial systems ● Contact Cyber Insurance ● Authorize emergency spending ● Place holds on accounts

2. Response Contacts

These are individuals/organizations that you will likely need to notify and/or work with, but not part of the IRT.

Role	Contact(s)	What They Do
Cyber Insurance *If you have cyber liability insurance, they can provide legal representation, forensics, mitigation and recovery resources.*	**Name** Email Phone	Immediately. They should be contacted as soon as you determine you have a serious cyber incident. The business office will be able to identify whether you have cyber liability insurance and the proper contact procedures.
Legal Representative *All communication with staff and the public needs to be reviewed by your district's legal This may be provided by your cyber insurer*	**Name** Email Phone	You can get this from your business manager and/or superintendent
Board President *Typically contacted by the Superintendent or the Cyber Incident Response Manager.*	**Name** Email Phone	As soon as an incident is confirmed
ISD Technology Director *If you are a local district and utilize the ISD for technology services (networking, firewalls, Internet, etc), they will play a critical role at all stages in the event and need to be contacted in order to protect other networked entities.*	**Name** Email Phone	As soon as an incident is confirmed

3. Extended Resources

You may not need all of these resources.

Resource	Contact Information	When To Contact?
Michigan Cyber Command Center (MC3) *MC3 is a division of the Michigan State Police. They investigate the criminal aspect of cyber incidents. They may offer support from the Michigan Cyber Civilian Corps (MiC3) which can help with forensics, mitigation, eradication & recovery. They also know when and how to reach out to other agencies such as the FBI or Secret Service.*	mc3@michigan.gov 877-MI-CYBER (877-612-9237)	They should be contacted as soon as you determine you have a serious incident. You need to determine whether to contact your cyber insurer or the State Police first.
MS-ISAC Cyber Incident Response Team (CIRT) *Free for SLTT organizations. They can help with incident response, forensics, log analysis and mitigation.*	soc@cisecurity.org 866.787.4722 https://www.cisecurity.org/isac/report-an-incident	If you do not have cyber-insurance or have decided to not involve them, you should contact the CIRT very early since they can support your team at every stage of incident response.
Internet Service Provider *For many, this may be MiSEN or Merit. Different providers provide different tools that may be helpful to contain, eradicate or recover from an incident.*	**Name** Email Phone	If you are experiencing a DDoS attack, your ISP may be able to invoke some protections. If you need to disconnect from the internet your provider should be informed so that they don't start their own troubleshooting procedures. Your provider may have additional cybersecurity tools (such as perimeter firewalls or packet monitoring) that can be leveraged to identify and contain the incident.
Local Law Enforcement *Some cyber incidents don't rise to the regional or state level, such as a district student hacking grades, a staff member accessing inappropriate resources or community threats. These issues can typically be managed by local law enforcement. Local law enforcement will also know when and how to reach out to other agencies such as the FBI or Secret Service.*	**Name** Email Phone	Once it is determined that the incident is contained and there is not a need to address it with cyber insurers or the MC3. Many events may not to be reported to local law enforcement if they have already been reported to cyber insurance and MC3.
ISD Business Manager *The ISD Business Manager may be on your IR Team, but if not they need to be notified on any serious event*	**Name** Email Phone	If they are not a part of the IR Team, they should be informed, but told not to share any information unless otherwise directed. Any communications regarding the incident needs to originate from the Cyber Incident Response Manager. However, if the incident is at a local district, ISD business services should be extra-alert for any suspicious activity involving the district or its employees.
ISD Superintendent *The superintendent may be on your IR Team, but if they are not, they need to be notified on any serious event*	**Name** Email Phone	If they are not a part of the IR Team, they should be informed, but told not to share any information unless otherwise directed. Any communications regarding the incident needs to originate from the Cyber Incident Response Manager. While the ISD Superintendent may not be directly involved, s/he will almost certainly want to support the district and work with ISD engineers to ensure the security of shared regional services
Maintenance Director *Secure building, oversee bus drivers, control HVAC*	**Name** Email Phone	The Maintenance Director should be notified quite early, especially if building security systems (eg security cameras or keyless entry systems) have been impacted.
Food Services Director *Access food service servers & activity logs, review payment / charges*	**Name** Email Phone	They can be informed a little later in the process unless systems specific to their department are impacted.
Transportation Director *Utilize the transportation systems to design & monitor bus routes.*	**Name** Email Phone	If the incident occurs while students are depending on district transportation, then the Transportation Director should be informed immediately. They will need to ensure that students can be safely transported. Otherwise, inform them with enough lead time so that they can make a decision regarding safe transportation.

4. Cybersecurity Support Systems

Access to these systems will likely be necessary during a cybersecurity incident.

Resource	Contact Information	When To Contact?
EDR / MDR / XDR Provider	**Product Name** Email Phone	Protects servers and devices and often provides the initial alert. Access to this service will be critical during an incident.
Mass Notification Systems	**Product Name** Email Phone	To help streamline administrative processes, promote stakeholder collaboration and personalized learning. Access to information of all enrolled students in their household.
Firewall / Network Support	**Product Name** Email Phone	Provides network security, cloud security, endpoint protection, and various cloud-delivered security. Secures network from cyber attacks in a high efficient and automatic way.

5. Critical Assets

These are systems that you may need to review during an incident. You may not have all of these systems so you may need to add/remove on this list to fit your environment.

Resource	Contact/Point Person Info	Software/Hardware Info	Access Method (IP, URL, etc.)
Authentication	**Product Name** Email Phone		
Email System			
Identity Management (IDM)			
Student Information System (SIS)			
Data Warehouse			
Financial System			
Onsite File-Storage			
Offsite File-Storage			
HVAC			
Phone System			
Security Cameras			
Bus Security Cameras			
Sports Cameras			
Door Access Controls			
DNS Servers			
DHCP Server			
Network Access Control (NAC)			
Password Manager			
Password Change Server			
Network Management Tool			
Remote Support Tool			
Remote Access (e.g. VPN, RDP)			
Food Services			
Library Management			
Transportation System			

6. Critical Procedures / Business Continuity

These are critical systems that need to be operational as soon as possible during or following a cybersecurity incident. You need to review and add / remove / prioritize these processes specifically to your district. Note that priorities may change during the time-of-year or other variables.

Resource	Contact Information	When To Contact?
Payroll	**Name** Email Phone	● Let banks know to secure/look for suspicious activity or freeze account ● How do you run/process the next payroll if systems are down? Some districts have simply re-run the previous payroll.
Building Security	**Name** Email Phone	● Lock/secure buildings/access controls if controllers unlock buildings automatically and need to override if servers are down. Someone go and physically lock the doors ● Security Cameras
Building Maintenance	**Name** Email Phone	● HVAC controls ● Depending on time of year, consider cold/freezing pipes ● Burglar/Fire alarms may be offline if they are networked based. ● Lighting Controls are sometimes networked.
Accounts Payable	**Name** Email Phone	● Support agreements up to date. ● Contact vendors about delayed payments due to the incident and see if they work with the district. ● Finance Systems may be offline, they need to understand how to manually verify invoices.
Student Supports	**Name** Email Phone	● Consider if the attendance system is impacted and what other options exist to monitor student attendance ● Are any systems supporting curriculum impacted, and how will teachers be able to work around those systems for things like lessons and grading? ● Are there manual systems to manage food services? ● Are there any systems that could impact student safety and health, such as mediation?
Public Communications	**Name** Email Phone	● If the website is impacted, a simple “unavailable” message should be displayed until the district is instructed by cyber insurer or legal ● No social media posts should be made or responded to without consent of cyber insurer or legal advisors. ● Be prepared for a response to local or even national news.
Parent Communications	**Name** Email Phone	● Consider how the district will communicate with parents in order to provide status updates and/or whether school will be held. ● Work with the Public Communications contact to provide information via the website and social media. ● The district may need to refer to printed contact information
Transportation Systems	**Name** Email Phone	● Consider how drivers may transport students home safely with the aid of transportation systems ● Note that much of the information in the transportation system is considered PII or personally identifiable information.

7. Critical Log File Locations

Where are your most important logs? Most of these are typically in a Security Information and Event Management (SIEM) server and/or on a logging server associated with your firewall. It isn’t necessary to list every log file location, but some log files will be especially helpful during incident response.

Description	Point of Contact	Physical Location & Physical backup location (if backed up)	How to get access or manage [no passwords]
Centralized Logging / SIEM	Model/brand: Identifier/(s/n): Name: Phone:		
Firewall			

Description	Point of Contact	Physical Location & Physical backup location (if backed up)	How to get access or manage [no passwords]
Routers			
Switches			
Authentication			
Email			
EDR / MDR / XDR			
DHCP / DNS			
IDS / IPS (may be firewall)			
Content Filter (may be firewall)			

8. Additional Documentation / Information

Every network is different and yours may have other important sources of information that could be useful during an incident. Some examples are included but you are expected to expand this section. If resources are only available digitally, consider an immutable, offline backup.

Description	Physical Location & Physical backup location (if backed up)	Digital Location
Where are backup network configuration files (e.g. routers, switches, etc)		
Where is the server inventory?		
Is there an alternative network available for IT staff (Charter, 5G, etc)		
Location of data backups		
<Include district-specific information here>		

Appendix A: Incident Log Template

Where are your most important logs? Most of these are typically in a Security Information and Event Management (SIEM) server and/or on a logging server associated with your firewall. It isn't necessary to list every log file location, but some log files will be especially helpful during incident response.

Date & Time	Person	Action Taken Or Findings	Follow Up
You may need to include precision to the seconds or even milliseconds	*Who has taken action or reported or made a discovery?*	*Provide as much detail as possible. If referencing another document or resource, clearly identify it and its location*	*Based on the Action / Findings, what follow up is needed?*