# Information Technology Failure Response Plan

**Montana Specific IT Failure Resources and Information**

**1. Montana State Emergency Preparedness Resources and Links**

* [Large-Cyber-Incident-Handling.pdf (dojmt.gov)](https://dojmt.gov/wp-content/uploads/Large-Cyber-Incident-Handling.pdf): This workgroup is tasked with developing national industry standard best practices for Incident Response and Incident Handling of large cyber related incidents. This document is to provide technical best practices on dealing with a high or critical cyber incident.
* [The Essential Guide to Protecting Against Supply Chain Attacks | Splunk](https://www.splunk.com/en_us/form/essential-guide-to-protecting-against-supply-chain-attacks.html?utm_campaign=bing_amer_en_search_generic_security&utm_source=bing&utm_medium=cpc&utm_term=supply%20chain%20attacks&utm_content=GdAgstSupChnAtckBF_EB&_bt=71468422103412&msclkid=0c390e02811b1a79a7cf6f69ebff83a1): Detect the top five supply chain threats: lateral movement, privilege escalation, command and control, malware deployment and data exfiltration. Use Splunk to find each threat at any stage of the security journey, and the specific data sources and MITRE ATT&CK techniques and tactics you will need to do it.
* [How to mitigate the risk and consequences of IT failures | ITProPortal](https://www.itproportal.com/features/how-to-mitigate-the-risk-and-consequences-of-it-failures/): The threat that IT outages pose to businesses is critical and need to be mitigated proactively to ensure that our ‘always on’ world is in fact, always on.
* [IT Disaster Recovery Plan | Ready.gov](https://www.ready.gov/it-disaster-recovery-plan):  What do you when your information technology stops working? Build an IT Disaster Recovery Plan and be prepared for an IT Disaster Recovery Plan
* [Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD) (nist.gov)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-15.pdf): This Publication explains how to strengthen security for small businesses from predators of network based and reduces the ability of compromised devices to participate in network-based attacks such as DDoS campaigns
* [SP 800-84, Test, Training and Exercise Programs for IT Plans & Capabilities | CSRC (nist.gov)](https://csrc.nist.gov/publications/detail/sp/800-84/final): This publication seeks to assist organizations in designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events in an effort to aid personnel in preparing for adverse situations involving information technology (IT). Exercises train personnel, exercise IT plans, and test IT systems, so that an organization can maximize its ability to prepare for, respond to, manage, and recover from disasters that may affect its mission. The guide describes the design, development, conduct, and evaluation of events for single organizations, as opposed to large-scale events that may involve multiple organizations.
* [SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems | CSRC (nist.gov)](https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final)- This publication assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle.

**2. Montana Local Emergency Preparedness Resources and Links: please add in local information specific to the county or counties where your Health Center (s) are located.-**

<Incorporate any of your organization’s existing response plan information throughout this template.>

<FIND and REPLACE WORDS: Look for the words in GREY. Find and replace the following words in this Response Guide. >

Insert LOGO in the upper right corner of the header.

* <insert organization’s name> or <insert Organization’s name> = Your Organization’s Name
* Patient, patients, patient = Use the most appropriate words that describes the individuals that your organization services (i.e., patient, resident, participant, client, etc.)

Insert additional organizational information in all other areas marked in GREY. <Delete these instructions in RED>

## Mission

To provide for business continuity and availability of essential automated systems for the facility in the event of a massive or sustained information technology failure, cyber-systems compromise, or deliberate attack.

## Directions

Read this entire response guide and review the Incident Management Team checklists.

Use this response guide as a checklist to ensure all tasks are addressed and completed.

## Objectives

|  |
| --- |
| * Maintain patient care capabilities |
| * Isolate and repair affected information technology systems |
| * Notify affected end user supervisory personnel and provide directed guidance on information technology systems use |

<Impute your organization’s IT Recovery Plan here. Delete these instructions in RED>

## Incident Management Team Checklists

### Incident Commander

|  |  |
| --- | --- |
| **Checkmark** | **Immediate Actions (0-2 hrs)** |
|  | Notify facility Chief Executive Officer, Board of Directors, and other appropriate internal and external officials of situation status |
|  | Activate the Emergency Operations Plan, Information Technology Failure Plan, and facility Incident Management Team (IMT) |
|  | Activate the facility Emergency Operations Center |
|  | Establish operational periods, objectives, and regular briefing schedule. Consider the use of Incident Action Plan Quick Start for initial documentation of the incident |
|  | Consider limiting or ceasing nonessential services |
|  | **Intermediate Response (2-12 hrs)** |
|  | Conduct regular briefings and situation updates with IMT to determine the situation status and timelines for restoration of services |
|  | Continue to implement operational periods and update incident objectives within the Incident Action Plan |
|  | **Extended Response (Greater than 12 hrs)** |
|  | Reassess incident objectives and Incident Action Plan and revise as indicated by the response priorities and overall mission |
|  | Plan for return to normal services in coordination with IMT; consider consulting with emergency medical services and other community facilities regarding their status and plans |
|  | Reevaluate the facility’s ability to continue its medical mission |
|  | **Demobilization/Recovery (Greater than 24 hrs)** |
|  | Declare incident termination |
|  | Monitor full system recovery and the return to normal operations |

### Public Information Officer (PIO)

|  |  |
| --- | --- |
| **Checkmark** | **Immediate Actions (0-2 hrs)** |
|  | Prepare an initial risk communication for staff and patients regarding the cyber-systems situation and recommend actions until the system are restored |
|  | Update internet, intranet, and social media with the facility’s status and any alteration in services |
|  | Notify key staff including house supervisors, Chief of Staff, Business Continuity Branch Director, support services, and others designated in the Business Continuity Plan as it applies to cyber-system disruptions |
|  | Monitor media outlets for updates on the incident and impacts on the facility. Communicate this information via regular briefings to the IMT and the Incident Commander |
|  | **Intermediate Response (2-12 hrs)** |
|  | Establish an essential information center as needed to address all staff or patient care issues that may arise as a result of the disruption |
|  | Update patients, staff, and visitors on situation status |
|  | Address social media issues as warranted; use social media for messaging as situation dictates |
|  | **Demobilization/Recovery (Greater than 24 hrs)** |
|  | Issue a final media update with facility status and appropriate service disruption information, in collaboration with the Incident Commander |

### Liaison Officer

|  |  |
| --- | --- |
| **Checkmark** | **Immediate Actions (0-2 hrs)** |
|  | Coordinate with community partners in accordance with local policies and procedures (e.g., consider local Emergency Operations Center, other area facilities, local emergency medical services, etc.) to provide incident details, community status, estimates of casualties, and establish process for requesting supplies, equipment, or personnel not available in the facility |
|  | If the disruption is deliberate and targeted, contact local law enforcement, the Federal Bureau of Investigation (FBI) Cyber Division, and the state cyber terrorism division, as appropriate |
|  | **Intermediate Response (2-12 hrs)** |
|  | Continue to update local emergency management and other officials regarding situation and facility status |
|  | Keep local emergency medical services advised of any health problems and trends identified, in cooperation with Infection Control |
|  | **Demobilization/Recovery (Greater than 24 hrs)** |
|  | Communicate final facility status and termination of the incident to the local Emergency Operations Center, area facilities, local emergency medical services, and officials |

### Safety Officer

|  |  |
| --- | --- |
| **Checkmark** | **Immediate Actions (0-2 hrs)** |
|  | Provide for the safety of patients, staff, and visitors in areas impacted by the automated system shutdowns |
|  | Initiate the HICS 215A to assign, direct, and ensure safety actions are adhered to and completed |
|  | **Intermediate Response (2-12 hrs)** |
|  | Conduct ongoing analysis of existing response practices for health and safety issues related to patients, staff, and facility; recommend corrective actions and update HICS 215A as required |
|  | **Demobilization/Recovery (Greater than 24 hrs)** |
|  | Monitor the safe restoration of services and systems |

### Operations Section Chief

|  |  |
| --- | --- |
| **Checkmark** | **Immediate Actions (0-2 hrs)** |
|  | Determine if personnel and resources are available to successfully complete the Operations Section strategies and tactics as outlined in the Incident Action Plan. If not, contact Logistics Section Chief to request additional personnel or resources |
|  | Provide for the continuation of patient care and management activities, including the documentation of medication administration, patient care, and supply use |
|  | Implement downtime patient care documentation and critical diagnostic and support systems until systems can be restored |
|  | Direct an inspection of critical monitoring functions that may be affected by the incident |
|  | Conduct a risk assessment of affected environmental systems (e.g., heating, ventilation, air conditioning, and utilities) and implement plans to maintain affected systems that support facility operations |
|  | Provide for security of the facility, including manual patrols and controls of ingress and egress |
|  | Work closely with the IMT to implement the Business Continuity Plan |
|  | Assess the degree of cyber system intrusion or disruption. Recommend any interim measures and corrective actions |
|  | **Intermediate Response (2-12 hrs)** |
|  | Prepare for demobilization and system recovery |
|  | Recommend, in collaboration with Operations Section Chief, when to resume normal activities and services |
|  | Evaluate the need to shelter-in-place or evacuate patients to ensure safety |
|  | Continue patient care and management; identify patient care systems that are affected during the restoration process |
|  | Assess affected environmental systems and modify response actions as necessary |
|  | Continue facility security as well as traffic and crowd control |
|  | Continue to implement the Business Continuity Plan and procedures |
|  | **Demobilization/Recovery (Greater than 24 hrs)** |
|  | Monitor the restoration of normal operations; coordinate with the Planning Section Chief to ensure cancelled procedures and appointments are addressed |
|  | Restore patient care and management activities, including normal staffing plan |
|  | Notify risk management and legal services of any actual or potential protected health information compromises or violations |
|  | Re-establish security systems that may have been impacted by the incident |
|  | Monitor and assist with restoration of information technology systems, utilities, and communications |

### Planning Section Chief

|  |  |
| --- | --- |
| **Checkmark** | **Immediate Actions (0-2 hrs)** |
|  | Establish operational periods, incident objectives, and the Incident Action Plan in collaboration with the Incident Commander |
|  | Determine the effect of system interruptions on the ability to gather and share incident information and impacts |
|  | Collect and collate manual documentation of the incident. |
|  | **Intermediate Response (2-12 hrs)** |
|  | Ensure that updated information and intelligence is incorporated into the Incident Action Plan. |
|  | Initiate staff and equipment tracking |
|  | Update and revise the Incident Action Plan |
|  | Initiate patient tracking |
|  | Collect documentation of actions, decisions, and activities |
|  | Prepare for demobilization and system recovery |
|  | **Demobilization/Recovery (Greater than 24 hrs)** |
|  | Finalize and distribute the Demobilization Plan |
|  | Conduct debriefings and After-Action Review with:   * IMT * Administrative personnel * All staff * All volunteers |
|  | Draft an After-Action Report and Corrective Action and Improvement Plan for submission to the Incident Commander, describing:   * Summary of the incident * Summary of actions taken * Actions that went well * Actions that could be improved * Recommendations for future response actions |
|  | Collect, organize, secure, and file incident documentation |
|  | Prepare a summary of the status and location of all patients, staff, and equipment. After approval by the Incident Commander, distribute it to appropriate external agencies |
|  | Monitor that the status of all impacted clinical and support operations relayed to the appropriate sections for resolution |

### Logistics Section Chief

|  |  |
| --- | --- |
| **Checkmark** | **Immediate Actions (0-2 hrs)** |
|  | Implement emergency internal communication and reporting mechanisms |
|  | Isolate and repair, replace, or remove affected systems from the facility network; establish restoration priorities in accordance with the Business Continuity Plan |
|  | Provide for the integrity of system backup data and begin planning for system restoration |
|  | Implement manual inventory and resupply processes, including medication distribution |
|  | Coordinate the transportation services (ambulance, air medical services, and other transportation) with the Operations Section Chief to ensure safe patient relocation, if necessary |
|  | Obtain and distribute supplies, equipment, medications, and food and water to sustain operations |
|  | **Intermediate Response (2-12 hrs)** |
|  | Recommend, in collaboration with Operations Section Chief, when to resume normal activities and services |
|  | Provide alternate documentation systems and support hardware (i.e., providing laptops and printers to affected areas for temporary use until systems are fully restored) |
|  | Monitor computer systems for new cyber threats |
|  | Plan for migration of manual documentation to electronic processes after systems are restored |
|  | Continue to obtain needed supplies, equipment, medications, food, and water. Route requests for additional resources not available in the facility through the Liaison Officer to outside agencies |
|  | **Demobilization/Recovery (Greater than 24 hrs)** |
|  | Monitor the restoration of normal operations; coordinate with the Planning Section Chief |
|  | Inventory all facility Emergency Operations Center and facility supplies and replenish as necessary, appropriate, and available |
|  | Prepare a summary report of corrective actions and recommendations for updating and improving diagnostic and protective cyber services |
|  | Provide behavioral health support and information about community services to staff, as needed |

### Finance/Admin Chief

|  |  |
| --- | --- |
| **Checkmark** | **Intermediate Response (2-12 hrs)** |
|  | Consider alternate methods to ensure payroll processing and documentation of hours worked |
|  | Track hours associated with the emergency response |
|  | Monitor and track costs related to the disruption of information technology systems including the compromise of automated systems |
|  | **Demobilization/Recovery (Greater than 24 hrs)** |
|  | Compile a final summary of response and recovery costs and expenditures and estimated lost revenue. Submit to the Planning Section Chief for inclusion in the After-Action Report |
|  | Ensure receipt of all-personnel time sheets and documentation needed for the recovery of costs |
|  | Contact insurance carriers to assist with initiating reimbursement and claims procedures |