

# Information Systems Disaster Recovery Plan Template

---

2006

Latest Revision: 3/13/06



# Table of Contents

Table of Contents.....	2
How to Use This Information Systems Disaster Recovery Plan Template .....	3
Overview.....	4
Objectives of the Disaster Recovery Plan.....	5
Applicability .....	5
Key Definitions.....	5
Information Systems Disaster and Security Incident Response .....	6
Authority.....	6
Administrative Oversight.....	7
Organization & Notification .....	7
Activation and Administration of the Disaster Recovery Plan.....	7
Disaster Recovery Coordinator (DRC).....	7
IS Disaster Recovery Team Emergency Contact Information.....	9
Damage Assessment .....	9
Assessing Resource Needs for Critical Disaster Recovery Operations.....	9
IS Disaster Recovery Command Center .....	10
Recovery Command Center Alternative Site.....	10
Recovery Resources Supply Checklist .....	12
Recovery Resources Supply Checklist .....	12
Recovery Team – Roles & Responsibilities .....	13
Other IS Disaster Recovery Support Teams .....	13
Communication Strategies.....	14
IS Disaster Recovery Team Status Report.....	14
Administration .....	14
Corporate/System Level.....	15
Media/Public Relations.....	15
Recovery Priorities.....	15
INFORMATION SYSTEM CRITICALITY ASSESSMENT .....	16
Recovery Processes and Procedures .....	17
Data Backup Procedures.....	19
Telecommunications.....	19
General Recovery Pre-Planning.....	19
Telecom Emergency Communications and Resources.....	20
Telecom/Communication Infrastructure.....	20
Guidelines for Master Telecom Disaster Recovery Plan for Each Site .....	20
Real-Time Disaster Operations and Options .....	21
Electronic Health Record (EHR) .....	22
Other Checklists.....	23
Risk Analysis of Potential Disaster Threats/Responses.....	23
Power Failure .....	23
Utility Failure (HVAC).....	23
Water Damage/Flooding.....	24
Fire/Smoke Damage.....	24
Equipment/Hardware Failure.....	24
Explosion .....	24

System/Application/Software Failure.....	25
Tornado/Storm Damage.....	25
Human Failure/Sabotage.....	25
Pandemic.....	25
Electronic Restoration.....	25
Workforce Member Education and Training.....	28
Review and Testing of Disaster Recovery Plan.....	28
Resources Used to Develop the IS Disaster Recovery Plan Template.....	28
Applicable Standards/Regulations:.....	29
Attachments.....	29
EMERGENCY CONTACT LISTS.....	29
Departmental Information.....	29
Disaster Recovery/Security Incident Response Team.....	29
Organizational Leadership/Key Workforce Members.....	30
Corporate Level Contact Information.....	30
System/Vendor Contact Information.....	31
Law Enforcement/Government Agency Contact Information.....	32
Other External Contact Information.....	32
IS DISASTER RECOVERY SUPPORT TEAM CHARTER FORM.....	33
IS DISASTER RECOVERY STATUS REPORT FORM.....	34
DEPARTMENT INFORMATION SYSTEMS DOWNTIME PLAN/PROCEDURE TEMPLATE.....	35

## **How to Use This Information Systems Disaster Recovery Plan Template**

This template document has been created by the Ministry Health Care Disaster Recovery Team to assist organizations in establishing both system and local information systems disaster recovery processes, including a documented disaster recovery plan.

As a template, information provided in this document is broad in nature and reflects state and federal regulations, accrediting standards, and industry best practices. Organizations must review the information presented in this template and determine local applicability and need for customization. Areas within this document that require local customization are highlighted in “red” ink.

Additionally, the template does not provide the needed specificity in identifying local processes to address:

- Telecommunications (backup processes continue to evolve at local level and across the system)
- Electronic health record (EHR) availability and backup procedures (dependent on local applications, systems, resources, etc.)
- Alternative sites (dependent on applications and systems; currently under system review)

Ministry Health Care will work with local organizations in Phase II of the information system disaster recovery plan process to facilitate implementation of the plan template and supporting disaster recovery processes. Workforce training and education with regard to the plan and processes will be part of the Phase II implementation process.

As Ministry Health Care continues to work toward increased information system standardization and support, portions of this plan template may be subject to change.

## Overview

This Information Systems Disaster Recovery Plan (DRP) has been developed by Ministry Health Care [Insert Organization's Name] information systems (IS) leaders to provide guidance for responding to IS disasters and other security incidents. Disasters and security incidents may threaten the organization's ability to carry out its mission as well as other operational functions. Advance planning and preparation will allow the organization to:

- Continue serving its patients and community;
- Ensure the availability of patient protected health information as well as business information;
- Minimize loss and facilitate recovery of core IS and other business assets;
- Preserve the organization's public image and reputation within the community;
- Prevent the disaster or incident from threatening the organization's long-term stability and viability;
- Heighten organizational awareness, allow for advance preparation, and workforce education and training; and
- Comply with applicable state and federal regulations and accrediting agency standards.

The DRP is a collection of references, guidelines, policies, procedures, forms, and suggestions designed for responding to security incidents and disasters. Components of this plan include:

- Disaster Recovery and Restoration
- Emergency Mode Operation
- Applications and Criticality Analysis
- Data Back-Up (see also supporting IS policy)
- Security Incident Response (see also supporting IS policy)
- Testing and Revision

Additionally, there are several documents referred to and/or appended to this plan to provide additional guidance for the management of information security, disasters and other security incidents. Key supporting IS policies include:

- SE-6: Security Incident Response/Reporting
- SE-8: Data Backup for Information Systems

## Objectives of the Disaster Recovery Plan

- To provide MHC organizations with a viable and maintained IS Disaster Recovery Plan (DRP) which, when executed, will support a timely and effective resumption and recovery of all interrupted clinical and business operations.
- To minimize possible adverse clinical outcomes, as well as financial and business impacts, to MHC organizations as a result of an interruption of normal business operations.
- To reduce operational effects of an information systems disaster on MHC organization's time-sensitive business operations and functions by providing a set of pre-defined and flexible guidelines and procedures to be used in directing resumption and recovery processes.
- To meet the needs of MHC patients, workforce members, and other stakeholders and communities reliant on the organization's ability to provide services during and following a disaster situation.
- To protect the public image and credibility of Ministry Health Care organizations.

## Applicability

The DRP has been developed to support the organization's Emergency Preparedness/Disaster Plan, providing further specificity to address IS needs. The DRP applies to all hardware, software, workstations, applications, systems and networks (LAN, WAN, Internet, Intranet), and other components of the organization's information systems.

The DRP is limited to the recovery of IS services only. The DRP does not address disaster prevention or long-term restoration of information systems. The DRP does not address the recovery of business processes that may be lost in the various departmental or business unit operations. Downtime/recovery processes are the responsibility of each department/business unit unless specifically covered in the DRP. Refer to department/business unit plans for appropriate downtime/recovery procedures (See Recommended Department IS Downtime Plan/Procedures Template).

## Key Definitions

**Business Continuity Planning:** Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change.

**Disaster (Information System):** An event that significantly challenges the continuation of normal information system functions impossible; an event which would render the information system unusable or inaccessible for a prolonged period of time (may be departmental or organization-wide).

**Disaster Recovery Coordinator (DRC):** Individual assigned the authority and responsibility for the implementation and coordination of IS disaster recovery operations.

Disaster Recovery Plan (DRP): The document that defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals (DRJ).

Recovery Time Objective (RTO): Amount of down time before outage threatens survival of the organization/mission critical processes.

Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices, or an adverse event whereby some aspect of computer security could be threatened. An IS Disaster would be considered a security incident.

## **Information Systems Disaster and Security Incident Response**

The organization recognizes an information systems disaster as a security incident and shall utilize those established security incident response processes in addressing disaster response and recovery. The organization's Security Incident Response/Reporting (SE-6) and Data Backup (SE-8) policies provide a framework for this IS Disaster Recovery Plan. Additionally, other organizational information security policies and procedures support IS disaster recovery processes and may be utilized in conjunction with this plan.

A key security incident resource is the *National Institute of Standards and Technology (NIST) Special Publication 800-61, Computer Security Incident Handling Guide*. This document provides much detail and additional resources to aid an organization in appropriate response to information security incidents and reflects best practices in information security. [The document is available at the following link](#) and may be considered as supporting documentation to this plan:

<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

Another useful NIST document is *Special Publication 800-34, Contingency Planning for Information Technology Systems* available at the following link:

<http://www.csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>

## **Authority**

The Disaster Recovery Coordinator (DRC), in conjunction with the organization's administrative leadership, shall have the responsibility and authority to take whatever steps necessary to identify, respond, contain, and eradicate the impact of an IS disaster.

## Administrative Oversight

The organization's senior administrative leadership will provide oversight in the development and management of the IS Disaster Recovery Plan. A senior administrative leader shall also be assigned to provide support and assistance during IS disaster recovery processes. This individual shall also research the organization's disaster insurance coverage and determine available financial resources.

## Organization & Notification

### Activation and Administration of the Disaster Recovery Plan

Upon notification of a suspected or confirmed information security incident/disaster, the IS leadership (e.g., management/technical analyst)\* shall verify, assess, and record the scope of the incident/disaster and determine the appropriate response:

- Application, system, and/or network out of operation.
- Impact localized, departmental, organizational, and/or enterprise-wide.
- Impact on critical mission operations and services.

If the IS leadership feels that the incident meets the criteria of a "disaster," the IS leader shall:

1. Activate of the Disaster Recovery Team (Security Incident Response Team-SIRT).
2. Identify an Individual to Act as the DRC (IS leader/technical analyst preferred).

\*In the absence of an IS leader, the organization's administrative leadership shall act as the **DRC** and facilitate the implementation of this plan and assign the tasks involved in IS disaster plan recovery.

Once an IS Disaster has been declared and the IS Disaster Plan activated, the DRC shall communicate such to senior administrative leaders and implement the IS recovery steps outlined in this plan. The DRC shall determine the need to notify external resources (See Communication & Organization) including business partners and vendors to assist with IS disaster recovery activities.

## Disaster Recovery Coordinator (DRC)

<b>Disaster Recovery Coordinator (DRC) Position Description/Job Action Sheet</b>	
<b>Position Assigned To:</b>	IS Leader or Designee
<b>Position Reports To:</b>	President/CEO or Designee
<b>Authority Level:</b>	<b>To Be Determined</b>
<b>Mission/Responsibility:</b>	Implement, organize and direct information systems disaster recovery operations.

**Disaster Recovery Coordinator (DRC)  
Position Description/Job Action Sheet**

<b>Criticality Level</b>	<b>Job Actions</b>
<b>Immediate (0-6 Hours)</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Review DRC Job Action Sheet and IS Disaster Recovery Plan</li> <li><input type="checkbox"/> Identify Disaster Recovery Command Center/Assembly Site</li> <li><input type="checkbox"/> Notify Disaster Recovery Team Members</li> <li><input type="checkbox"/> Assemble Team at Command Center</li> <li><input type="checkbox"/> Assemble Resources (See Checklist)</li>   <li><input type="checkbox"/> Provide Team Briefing/Document Information Provided at Briefing</li> <li><input type="checkbox"/> Review Tasks to Be Performed and Assign Personnel</li> <li><input type="checkbox"/> Notify Other Key Leaders/Workforce Members as Necessary</li> <li><input type="checkbox"/> Notify Vendors/Stakeholders/Law Enforcement Agencies or other Emergency Government Agencies as Necessary</li> <li><input type="checkbox"/> Determine Need for Additional Support Teams and Assign Team Leader/Members</li>   <li><input type="checkbox"/> Provide Teams with Status Report Forms</li> <li><input type="checkbox"/> Request Team Facilitators to Track Resource Utilization on Status Report Form</li> <li><input type="checkbox"/> Communicate Key IS Disaster Recovery Information/Contacts/Locations Internally</li> <li><input type="checkbox"/> Contact External Vendors and Other Business Stake Holders</li> <li><input type="checkbox"/> Contact MHC Corporate IS Resources</li>   <li><input type="checkbox"/> Determine Need for Media Communication</li> <li><input type="checkbox"/> Designate Media Contact; Instruct All Others Not to Make Statements to Media</li> <li><input type="checkbox"/> Prepare Media Statement Proactively if Felt Necessary</li> </ul>
<b>Intermediate (6-12 Hours)</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Assess Continued Staffing Needs/Staff Relief</li> </ul>
<b>Ongoing</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Damage Assessment</li> <li><input type="checkbox"/> Assess Recovery Priorities</li> <li><input type="checkbox"/> Communicate IS Disaster Recovery Status with Administration</li> <li><input type="checkbox"/> Assess Resource Needs for Operations</li> <li><input type="checkbox"/> Approve Expenses Related to Recovery Processes</li> </ul>
<b>Extended (&gt;12 Hours)</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Assess Need for Staff Relief/Additional Resources</li> </ul>
<b>Follow-Up (Following Disaster)</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Facilitate “post mortem” evaluation of IS disaster and recovery processes</li> <li><input type="checkbox"/> Revise IS Disaster Recovery Plan and Processes as Necessary</li> <li><input type="checkbox"/> Train and Educate Staff on IS DRP Revisions</li> </ul>

## **IS Disaster Recovery Team Emergency Contact Information**

Members of the IS Disaster Recovery Team shall be contacted immediately once the IS DRP has been activated. The following information should be provided at the time of contact:

- A Brief Description of the Problem
- Location of the IS Disaster Recovery Command Center
- Phone Number of the IS Disaster Recovery Command Center
- Identification of Immediate Support Required (Services, Equipment, Etc.)
- Information Regarding How the Facility Can be Entered (Need for Badge/Identification)

Contact information is available as an attachment to this plan.

## **Damage Assessment**

Damage assessment shall be carried out to determine disaster recovery requirements. A preliminary damage assessment shall address:

- Cause of the emergency or disruption.
- Potential for additional disruptions or damage.
- Areas affected by the disruption.
- Status of physical infrastructure (where computer equipment is located).
- Inventory and functional status of computer equipment.
- Type of damage (e.g., water, fire, electrical surge, etc.).
- Items to be replaced (e.g., hardware, software, other).
- Estimated time to restore to normal operations.

## **Assessing Resource Needs for Critical Disaster Recovery Operations**

Once the DRP is activated, the DRC will determine what resources are required to support critical functions. This analysis should take into consideration the following resources and potential questions:

Human Resources: Can people get to work? Are there critical skills and knowledge possessed by the appropriate people? Can people easily get to an alternative site?

Processing Capability: Are the computers or other hardware harmed? What happens if some of the equipment is inoperable, but not all?

Automated Applications and Data: Has data integrity been affected? Has an application been sabotaged? Can an application run on a different processing platform?

Computer-Based Services: Can the computers communicate? To where? Can people communicate? Are information services down? For how long?

Infrastructure: Do people have a place to work? Do they have the equipment to do their jobs? Can they occupy the department/building?

Documents/Paper: Can needed records be found? Are they readable?

### IS Disaster Recovery Command Center

The Command Center will function as the centralized location for IS disaster recovery processes. The DRC will make the determination as to the location of the Command Center. **The location will be determined by the disaster type and available resources.** The Command Center location must be able to accommodate the necessary critical resources and equipment required for disaster recovery (see Recovery Resources Supply Checklist):

- Hardware, Software, Other Equipment
- Electrical Support
- Telecommunications Support
- Desks, Chairs, Tables, Lights

<b>Primary Location</b>			
Facility Name:		Floor/Room:	
Address:			
Phone Number:		Fax Number:	
Contact Person:		Phone Number:	
Alternate Contact:			
Security Considerations:			

### Recovery Command Center Alternative Site

The IS leadership shall make the determination as to whether or not recovery activities should be relocated to an alternative sites. A pre-determined alternative site should be designated for major disruptions with long-term effects. The alternative site should allow the organization to recover and perform systems operations for an extended period of time.

<b>Alternative Location</b>			
Facility Name:		Floor/Room:	
Address:			
Phone Number:		Fax Number:	

Alternative Location			
Contact Person:		Phone Number:	
Alternate Contact:			
Security Considerations:			

Examples of typical types of recovery command centers and options include:

Cold Site: A basic facility with adequate space and infrastructure (electrical power, telecommunications connections, environmental controls) to support the organization's information systems. The site would not contain information technology or office equipment.

Warm Site: A partially equipped facility containing all or some of the system hardware, telecommunications and power sources. The site would be maintained in operational status ready to receive relocated staff. The site may exist as a normal operational facility for another system or function, or it may need to be prepared to receive relocated staff and equipment.

Hot Site: A fully equipped facility ready to support system requirements and configured with the necessary system hardware, supporting infrastructure and support staff. The site may be staffed 24/7. Hot site staff members are available to begin preparing for system arrival as soon as they are notified.

Mobile Site: A self-contained, transportable shell custom-fitted with specific telecommunications and information technology equipment necessary to meet the organization's systems requirements; available for lease through commercial vendors. The facility is often contained in a tractor-trailer and may be driven and set up at a desired alternative location.

Mirrored Site: A fully redundant facility with full real-time information mirroring the organization's operations; identical to the original site in every respect.

# Recovery Resources Supply Checklist

<b>Recovery Resources Supply Checklist</b>	
<p><b>Workspace</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Desk, Chairs, Tables, Lights</li> <li><input type="checkbox"/> Electrical Support</li> <li><input type="checkbox"/> Telecommunications Support</li> </ul>	<p><b>Documentation</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Hardware Inventory Lists and Serial Numbers</li> <li><input type="checkbox"/> Software Inventory Lists and License Numbers</li> <li><input type="checkbox"/> Network Schematic Diagrams</li> <li><input type="checkbox"/> Equipment Room Floor Grid Diagrams</li> <li><input type="checkbox"/> Contract and Maintenance Agreements</li> </ul>
<p><b>Hardware</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> PC's/Laptops</li> <li><input type="checkbox"/> Printers</li> <li><input type="checkbox"/> Scanners</li> </ul>	<p><b>Forms</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Maintenance Forms</li> <li><input type="checkbox"/> Message Pads</li> </ul>
<p><b>Software</b></p> <p><b>Back-Up Copies of Data Files</b></p>	<p><b>Other Supplies</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Office Supplies (pens, paper, folders, paper clips, scissors, staplers, tape, etc.)</li> <li><input type="checkbox"/> Office Equipment (shredder, copiers, etc.)</li> <li><input type="checkbox"/> Camera/Video Recorder</li> <li><input type="checkbox"/> Film/Blank Recoding Media</li> <li><input type="checkbox"/> Duct Tape</li> <li><input type="checkbox"/> Backup Media</li> <li><input type="checkbox"/> Flashlights and Spare Batteries</li> <li><input type="checkbox"/> Telephone Log</li> <li><input type="checkbox"/> Area Maps</li> </ul>
<p><b>Communications</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Telephones</li> <li><input type="checkbox"/> Cellular Phones With Chargers</li> <li><input type="checkbox"/> Fax and Backup Fax</li> <li><input type="checkbox"/> Dedicated Telephone Line(s)</li> <li><input type="checkbox"/> Radios (Walkie-Talkie) As Required</li> <li><input type="checkbox"/> Organizational Contact Information/Directories</li> <li><input type="checkbox"/> Telephone Directories</li> <li><input type="checkbox"/> Telephone Log</li> </ul>	
<p><b>Other</b></p>	

## Recovery Team – Roles & Responsibilities

Title	Position*	Responsibilities
Disaster Recovery Coordinator	<ul style="list-style-type: none"> <li>▪ Director of IS</li> <li>▪ IS Leader</li> <li>▪ Security Officer</li> <li>▪ Administrator</li> </ul>	See Disaster Recovery Coordinator Position Description/Job Action Sheet
Operations Recovery Coordinator	<ul style="list-style-type: none"> <li>▪ IS Leader or Technical Support Person</li> </ul>	Implement IS disaster recovery processes; facilitate recovery of IS operations as directed by DRC.
Network Recovery Coordinator	<ul style="list-style-type: none"> <li>▪ Local or Enterprise Network Administrator</li> </ul>	Implement IS disaster recovery processes; facilitate recovery of organization/enterprise network as directed by DRC.
Clinical Applications Coordinator	<ul style="list-style-type: none"> <li>▪ IS Clinical Applications Coordinator</li> <li>▪ Nursing Leader</li> </ul>	Implement IS disaster recovery processes as necessary in the absence of IS applications and systems.
Business Applications Coordinator	<ul style="list-style-type: none"> <li>▪ IS Business Applications Coordinator</li> <li>▪ Business Leader</li> </ul>	Implement IS disaster recovery processes as necessary in the absence of IS applications and systems.
Communications Coordinator	<ul style="list-style-type: none"> <li>▪ Director of Public Relations</li> </ul>	In conjunction with the DRC and Administration, develop and authorize communications with news media or public regarding disaster.
Administrative Leader	<ul style="list-style-type: none"> <li>▪ President/CEO</li> <li>▪ Senior VP</li> <li>▪ Other Leadership Team Member</li> </ul>	Support DRC/activities. Investigate insurance coverage and resources. Facilitate securing critical resources. Investigate legal issues.
Administrative Assistant		Provide necessary administrative and clerical support to DRC and support teams.
*Customize Position Titles Locally		

## Other IS Disaster Recovery Support Teams

The DRC may determine the need to establish additional support teams based on the circumstances of the IS disaster. Additional teams which may be created include, but are not limited to:

- Administrative Support Team
- Human Resources Team
- Recovery Site Operations Team
- Applications Teams
- Telecommunications Team
- Restoration & Salvage Team
- Legal Team
- Acquisitions & Supplies Team

Prior to the establishment of a support team, the DRC will identify the following oversight, responsibilities, and reporting. A sample team charter may be used to document key information.

<b>IS Disaster Recovery Support Team Charter: Title</b>	
<b>Description/Scope</b>	<i>Description and purpose of Team. Scope of services Team to address.</i>
<b>Responsibilities</b>	<i>Directives assigned to Team to be addressed/resolved.</i>
<b>Authority Level</b>	<i>To be Determined by DRC and Administrative Representative.</i>
<b>Facilitated By</b>	<i>Team Leader, As Appointed by DRC.</i>
<b>Members</b>	<i>To be Determined by DRC and Team Leader.</i>
<b>Reports To</b>	<i>DRC or Designee (Identity Position).</i>
<b>Reports When</b>	<i>Reporting Schedule to be Determined by DRC.</i>
<b>Resources Required</b>	<i>To be Determined by DRC and/or Team.</i>
<b>Location</b>	<i>Physical Location in Which Team will be Operating.</i>
<b>Other</b>	<i>At the Discretion of the DRC.</i>

A blank template of this form is available as an attachment to this plan.

## **Communication Strategies**

### **IS Disaster Recovery Team Status Report**

The DRC will determine the need to complete status reports. The Disaster Recovery Team and all other disaster recovery support team leaders will be responsible for completing the “IS Disaster Recovery Status Report Form” when requested by the Coordinator. The Coordinator will compile information from the status report(s) to use in communicating to senior administrative leadership, corporate resources, and other external contacts and stakeholders (a blank template of this form is available as an attachment to this plan).

### **Administration**

The administrative leader assigned to the disaster recovery process shall act as a liaison between the DRC/Team and administration. The leader will be responsible for communicating disaster recovery activities on an as needed basis.

## Corporate/System Level

The DRC will determine the need for notification of Ministry Health Care **leadership** and/or Information Systems staff members. The Corporate Office shall be notified of any disaster/security incident that:

- A. Results in adverse patient care outcomes or significantly impacts operational functions;
- B. Requires additional IS resources and support beyond the scope of the local organization's IS staff;
- C. Impacts more than one MHC organization or facility;
- D. Requires involvement with local, state or federal law enforcement agencies; and
- E. Results in adverse publicity and require media relations skills.

The DRC may also request assistance from other MHC affiliated organizations for IS support. The Coordinator may contact the organizations directly or request assistance from corporate IS in coordinating supporting services and resources from the other organizations.

## Media/Public Relations

All MHC IS disaster related information (spoken or written) shall be coordinated and issued to members of the media by the Communications Coordinator or a member of senior leadership. Certain types of information security incidents may generate the attention of the news media. The organization may also choose to initiate contact with the news media in certain circumstances. The organization's designated media relations contact should serve as the liaison between the organization and the news media. In the absence of a media relations contact person, administration will designate a media relations contact or seek assistance from the MHC corporate office in working with the news media. The media relations contact can serve as a single point of contact for the news media, which eliminates the need to involve the Disaster Recovery Team members and leaves them free to manage the security incident. The IS leader or a member of the Disaster Recovery Team should be prepared to share information with the media relations contact. Key considerations when working the media relations contact/news media includes:

- Ensure that the contact has a clear understanding of the technical issues so that they may communicate effectively and accurately with the press.
- False or misleading information may ultimately cause more damage to the organization's reputation
- Contact the organization's legal counsel if unsure of legal issues.
- Establish a single point of contact (media relations contact) when working with the news media to ensure that all inquiries and statements are coordinated.
- Keep the level of technical detail low – do not provide attackers with information.
- Be as accurate as possible, **yet concise**.
- Do not speculate.
- Ensure that any details about the incident that may be used as evidence are not disclosed without the approval of investigative agencies.

## Recovery Priorities

## System Criticality Assessment & Priorities

Criticality levels are assigned to applications systems based upon the relative importance of the applications and systems to the organization's mission and operations. During the disaster recovery process, resources will be allocated based on established criticality levels, unless otherwise determined by the DRC and/or administrative leadership. *The organization must in advance review all applications, systems, networks, and critical interfaces and assign them to one of the following priority levels:*

### Critical/Priority 1

Applications and systems designated "Critical" are mission-critical, impact patient care or *other key operations*, and require immediate data recovery resources to ensure prompt restoration, recovery, and operability. Failure of these applications and systems to function for even a short period of time could have a severe impact on the organization's ability to carry out its mission and operations.

Recovery Time Objective (RTO): 0-8 Hours.

### Essential/Priority 2

Applications and systems designated as "Essential" and may impact patient care, information services, finance, labor and attendance, and physical security. Failure of these applications and systems is allowable for a short period of time. RTO: 9-24 Hours.

### Necessary/Priority 3

Applications and systems designated "Necessary" and may tolerate a short period of loss of availability. RTO: 25-72 Hours.

### Desirable/Priority 4 (Low)

Applications and systems designated "Desirable" are lower priority and may tolerate a significant loss of availability. Recovery will be initiated when normal IS operations are re-established. RTO: > 72 Hours. Pending resolution of higher priorities; allocation of resources may be questioned

## INFORMATION SYSTEM CRITICALITY ASSESSMENT TEMPLATE

***SAMPLE ONLY - TO BE CUSTOMIZED BY ORGANIZATION TO ADDRESS APPLICATIONS, SYSTEMS, NETWORKS AND CRITICAL INTERFACES***

Local Application/ System/Network/ Interface	Critical Priority 1 RTO: 0-8 Hours	Essential Priority 2 RTO: 9-24 Hours	Necessary Priority 3 RTO: 25-72 Hours
Administration			
Admissions			
Communications -	Network Access	Microsoft Outlook/	

<b>Local Application/ System/Network/ Interface</b>	<b>Critical Priority 1 RTO: 0-8 Hours</b>	<b>Essential Priority 2 RTO: 9-24 Hours</b>	<b>Necessary Priority 3 RTO: 25-72 Hours</b>
External		E-Mail	
Communications - Internal	PBX/Switchboard	Meditech MOX	
Corporate Integrity			
Decision Support/ Reporting Systems			
Financial		Meditech Financials Meditech MM KaufmanHall	
Health Information/ Medical Record	Electronic Health Record (EHR)		
Human Resources		Time & Attendance	Leadership Excellence System
Other		ECHO	HEAT COMPLISTAR
Patient Accounting			
Patient Care	PCI/Order Entry Dictation/Transcription LastWord Meditech	Pyxis	
Revenue			
<b>Enterprise Application/ System</b>	<b>Critical Priority 1 RTO: 0-8 Hours</b>	<b>Essential Priority 2 RTO: 9-24 Hours</b>	<b>Necessary Priority 3 RTO: 25-72 Hours</b>
TBD			
TBD			
Human Resources		API LaborWorkz	
TBD			
TBD			
TBD			
TBD			

## Recovery Processes and Procedures

1. Upon assessment of damage and activation of disaster recovery processes, the IS leadership/SIRT will determine the appropriate data recovery strategy.
2. The data recovery processes shall reflect the organization's information system priorities. Data recovery activities shall take place in a pre-planned sequential fashion so that system components can be restored in a logical manner and should take into consideration:
  - A. Personnel: The IS leadership and workforce members, as well as the SIRT members, involved in data recovery processes will be the most valuable resource. These individuals may be asked to work at great personal sacrifice and resources shall be provided to meet their personal and professional needs.
  - B. Communication: Notification of internal and external business partners associated with the organization's information systems.
  - C. Salvage of Existing IS Equipment and Systems: Initial data recovery efforts shall be targeted at protecting and preserving the current media, equipment, applications and systems. A priority shall be to identify and obtain storage media. The IS equipment shall be further protected from the elements or removed to a safe location, away from the disaster site if necessary (Alternative Sites).
  - D. Designate Recovery Site: It will be necessary to determine if the data recovery efforts can be carried out at the original primary site or moved to another location (see [Command Recovery Center](#) Alternative Site section). The choice of using an internal or a remote site will be dependent on the damage and estimated recovery of the computing and networking capabilities.
  - E. Backup/New Equipment: The recovery process will rely heavily on the ability of the organization's vendors to quickly provide replacements for the resources which cannot be salvaged. Emergency procurement processes will be implemented to allow the IS leadership to quickly replace equipment, supplies, software and any others items required for data recovery.
  - F. Reassembly Process: Salvaged and new data recovery equipment and components shall be reassembled at the recovery site to begin data recovery processes.
  - G. Restoration of Data from Backups: Data recovery will rely on the availability of the backup data from the storage site. Initial data recovery efforts will focus on restoring the operating systems by pre-determined priority (See Amendment A).
  - H. Restoration of Applications Data: IS leadership will work with the individual departments/application owners to restore each running application. As a period of time may have elapsed between the time that the backups were made and the time of the disaster requiring data recovery, the application owners must address mechanisms to capture and restore the lost interim data.
  - I. Move Back to Restored Permanent/Primary Site: If the data recovery process has taken place at an alternative site, the equipment and systems that have been assembled at the alternative site will need to be returned to the original site when available.

3. Upon termination of recovery activities and **once** normal IS operations are back in place, than reconstitution efforts should begin. If the original site is unrecoverable (e.g., burned in fire), then the reconstitution activities may be applied to preparing a new site to support information system requirements. Reconstitution activities should address:
  - A. Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental control, office equipment, and supplies.
  - B. Installing system hardware and software.
  - C. Establishing connectivity and interfaces with network components and external systems.
  - D. Testing system operations to ensure full functionality.
  - E. Backing up operational data on the contingency system and uploading to restored system.
  - F. Shutting down the contingency system.
  - G. Terminating contingency operations.
  - H. Removing and/or locating all sensitive materials at the contingency site.
  - I. Arranging for recovery staff to return to the original/new facility.

## **Data Backup Procedures**

Data backup processes shall be established through existing policy and procedures. The IS Department is responsible for overseeing organizational data backup and recovery processes for those applications, systems, and networks under its control. Users of unique departmental and/or individual applications, systems, and networks will be responsible for data backup and recovery unless arrangements have been made in advance with the IS Department (See SE-8: Data Backup for Information Systems Policy).

## **Telecommunications**

### **General Recovery Pre-Planning**

- Identify Critical Telecom Assets for Each Facility (including **location of** serial numbers, software versions, and other amplifying data).
- Identify Spare Parts Available for a Particular Class of Switch.
- Identify What Parts for XX Type of Switch Are Located at [Location] and Available for Backup at Other Locations.
- Document Fully Each Telephone Switch and Devices Attached to or Supported by the Telephone Switch
- Develop and Document a Contingency Plan to Include:
  - ♦ Loss of Any Telephone Switch - Identifying Who Would Respond to a Loss of a Switch
  - ♦ Alternative Communications, such as POTS Circuits, that could be Converted to DID Phones, etc.

- ◆ Response to Extended Loss of Either a Switch or Communications Lines and Trunks
- ◆ Response if Telephone Switches are IP Enabled, Could Any Other Switch Assume Control and Provide Services to the Sites' Telephones Until the Affected Switch Comes Back on Line
- ◆ Establishment of Reasonable Time-lines for Restoration of Services for Loss of Any Switch, Communications Line(s) or Trunk. Availability of an Adequate Number of Cell or Satellite Phones to Support Recovery

### Telecom Emergency Communications and Resources

Telecom leadership is responsible for identifying partnership with local governmental agencies in establishing a communication plan and resources in a disaster situation. Often this is facilitated with local government emergency management officials who rely heavily on coordinating services with local healthcare providers. At a minimum, Telecom leadership should identify the following for their organization:

<b>Telecom Emergency Information &amp; Contacts</b>	
Telecom Emergency Contact Phone Number	
Telecom Emergency Contact Position/Person Numbers	Desk
	Cell
	Pager
Alternative/Backup Contact Phone Number	
Help Desk Phone Number	
Satellite Phone Number	
Ham Radio Communication Backup Information	

Telecom leadership shall determine the need to collect similar data from the organization's individual sites as well as other emergency telecommunications partners (e.g., neighboring MHC or AHS organizations, local emergency management structures, etc.).

### Telecom/Communication Infrastructure

- Identity and physically map all telecom circuits, including circuits that are used for data communications.
- Determine what, if any, hybrid overlaid circuits could cause other facilities to lose telephone or data communications (e.g., Ministry WAN router at St. Joseph's Hospital and impact of loss of circuits feeding the router/s).

### Guidelines for Master Telecom Disaster Recovery Plan for Each Site

Examine and Document the Following:

- Statement of overall intent of the telecom DR and subsequent recovery plan.
- Identification of management responsibilities and senior leadership support.

- Inventory of the communications network components.
- Site inventory of non-telecom equipment located in telecom environment.
- Primary switch/front end processor: what make, version, software, license keys, etc.
- Determination if multiplexing and central office equipment is included in planning phase.
- Contact lists for local staff and other site staff.
- Vendors - to include after hours emergency contact information.
- Telecom and network support personnel - who will respond to an incident.
- User and/or remote sites that are supported by switch or site equipment. Determine is this user/remote site critical?
- Dictation and transcription: determine [planned recovery approach](#) and include support for dictators and transcribers?

#### Step-by-Step Recovery and Priority Ordering:

- Extremely critical telecom networks and equipment: identify and plan to recover first.  
Very critical networks and equipment: second after extremely critical networks.  
Sub-Critical networks: +48 hours need to be recovered but not critical for operations  
Software: have copies available offsite or at which vendor?
- If software at vendor, do they have license keys, etc to activate software?
- Who will install software?
- Host command lists and macro's used in primary switch. Printed copy?

#### General Telecom Support Information:

- Modem/multiplexer and any data dialup equipment on site.
- Internet? Who is responsible for connectivity?
- Telecom and network staff – must work together on development of DR plan, etc.
- Dial backup numbers at all sites for troubleshooting, etc.
- Access numbers for switched/packet networks in the event of complete site failure provided by which vendor and in what timeframe?

### **Real-Time Disaster Operations and Options**

Telecommunications back up and recovery processes may be coordinated with the telecommunications vendor. The organization shall have in place other emergency backup resources in the event of a telecommunications disruption. Viable communications backup resources include:

- Telecommunications system with inherent backup system.
- Dedicated direct phone lines independent from the telecommunications system.
- Organizational/personal cell phones with text messaging options.<sup>1</sup>
- Public pay phones.
- Internal walkie-talkies.
- Satellite phone.
- Emergency Department radio dispatch center.

---

<sup>1</sup> In a wide-spread geographic disaster, text messaging options may succeed where voice channel circuits may become jammed. The use of text messaging may aid in keeping voice channels free for emergency communications.

- Local Ham Radio Operators.

## **Electronic Health Record (EHR)**

The availability of patient electronic health records (EHR) is mission critical to ensure for safe and effective communication of patient information between healthcare providers. Established procedures shall ensure that EHR is routinely backed up and the information recoverable. In the event of downtime disruption and inability to access the EHR, the organization shall:

### Communications:

1. Identify operations or services that will be impacted and make necessary notification of the unavailability of the EHR.

### Access to Historical Patient Health Information:

2. Implement existing backup systems to access historical patient health information (e.g., backup medium and/or server, MPI directory, paper medical record, archived transcribed documents, available diagnostic information from laboratory information system (LIS, etc.).
3. Identify and make available resources for retrieval, delivery, return, etc.

### Creation of New Patient Health Information:

4. Make available to healthcare providers temporary paper documentation tools including, but not limited to:
  - A. Medical Record Chart Folder.
  - B. Key Patient Care Documentation Forms:
    - a. History & Physical.
    - b. Plan of Care.
    - c. Physician Orders.
    - d. Progress Notes.
    - e. Operative Report.
    - f. Medication Administration Record/Profile.
    - g. Discharge Summary.
    - h. Diagnostic Study Results.
5. Identify processes and procedures to carry out:
  - A. ADT (Admission, Discharge, Transfer) Transactions.
  - B. Order Placement and Communication.
  - C. Diagnostic Study Results Reporting.
6. Identify processes, procedures, and responsible individuals to ensure processing of paper documentation following resumption of EHR applications. All paper documentation information must be incorporated into the EHR.

## Other Checklists

To be determined based on organizational needs.

## Risk Analysis of Potential Disaster Threats/Responses

It is impossible to predict all of the things that can go wrong and lead to an information systems disaster. However, it is possible to identify a likely range of threats and dangers and provide basic guidance. Risks are normally classified in three types:

1. Natural – hurricane, tornado, flood, fire, etc.
2. Human – operator error, sabotage, malicious code, etc.
3. Technological - equipment failure, software error, telecommunications network outage, power failure, etc.

Listed below are the most likely threats to MHC information systems as well as brief statements reflecting immediate objectives for containment, recovery, and restoration. Also addressed are basic controls that may reduce:

1. The likelihood or probability of a threat exploiting an identified system vulnerability and/or
2. The magnitude of impact of the exploited vulnerability on the system.

Existing controls may be management, operational and/or technical controls depending on the identified threat and the risk to IS operations.

## Power Failure

Thirty percent of disasters are related to power outages.<sup>2</sup> MHC organizations traditionally address emergency utilities management through environment of care plans and facilities management processes. IS leaders are responsible for ensuring that emergency power backup needs for critical applications, systems, and networks are addressed in these plans. In the absence of a formalized organizational approach to emergency utilities management, IS leaders will at a minimum ensure that UPS units are in place and emergency back-up generators are available and working when applicable. In the event of power failure, the DRC will work with facility management to determine available backup power resources to meet organizational IS needs. The DRC will determine IS emergency equipment backup priorities (see Criticality Analysis) and strive to ensure resumption of IS operations to the fullest extent possible given the circumstances, consistent with the DRP.

## Utility Failure (HVAC)

Critical to IS equipment operations is appropriate heating, ventilation, and air conditioning (HVAC). Failure of any one of these utilities may disrupt IS equipment/operations. IS leaders shall work with available facility services/plant operations personnel to ensure appropriate

---

<sup>2</sup> “Power Plans,” Healthcare Informatics, April 2005

ongoing monitoring of HVAC as well as availability of emergency back-up resources (e.g., service, repair, equipment, etc.). In the event of utility failure, the DRC will work with facility management to [access](#) available backup utility resources to meet organizational IS needs. The DRC will determine IS emergency equipment backup priorities (see Criticality Analysis) and strive to ensure [resumption of IS operations](#) to the fullest extent possible given the circumstances, [consistent with the DRP](#). In the event of an air conditioning failure, the DRC may want to investigate the availability of renting or purchasing a portable backup air conditioning unit.

## **Water Damage/Flooding**

Water is often a factor in disasters, whether from fire suppression, roof damage, plumbing failures, chemical spills, or other natural disasters. With the exception of furniture or durable equipment, nothing should be stored on the floor. A moderate stock of emergency supplies for water damage should be available and include:

- Plastic Tarps
- Wet-Pick Up Vacuum
- Absorbent Towels/Wipes
- Floor Squeegees

The ability to swiftly place tarps over computers, equipment, files and other critical components can dramatically curtail the extent of damage. IS leaders are responsible for ensuring that preventive fire and smoke equipment is in place. In the event of water damage and/or flooding, the DRC will determine IS emergency equipment backup priorities (see Criticality Analysis) and strive to ensure IS operations to the fullest extent possible given the circumstances, consistent with the DRP (see also “*Electronic Restoration*”).

## **Fire/Smoke Damage**

Fire and smoke damage to information systems can be prevented through the establishment of fire suppression systems (such as a sprinkler system), as well as fire and smoke detectors. MHC organizations traditionally address fire safety through the organization’s environment of care plans and fire safety. IS leaders are responsible for ensuring that preventive fire and smoke equipment is in place [and functioning](#). In the event of fire and/or smoke damage and/or flooding, the DRC will determine IS emergency equipment backup priorities (see Criticality Analysis) and strive to ensure [resumption of IS operations](#) to the fullest extent possible given the circumstances (see also “*Electronic Restoration*”).

## **Equipment/Hardware Failure**

IS leaders shall ensure a preventive maintenance program for IS equipment and hardware with appropriate backup processes in place. Failure of IS equipment or hardware will be assessed by IS leaders and appropriate steps taken to remedy the situation as soon as possible. In the event that equipment and/or hardware failure is determined to be an IS disaster, the DRC will determine emergency backup priorities (see Criticality Analysis) and strive to ensure [resumption of IS operations](#) to the fullest extent possible given the circumstances, [consistent with the DRP](#).

## **Explosion**

See Power and Utility Failure as well as Fire/Smoke Damage.

## **System/Application/Software Failure**

IS leaders shall ensure a preventive maintenance program for IS systems, applications, and software with appropriate backup processes in place. Failure of IS systems, applications, and/or software will be assessed by IS leaders and appropriate steps taken to remedy the situation as soon as possible. In the event that system, application, and/or software failure is determined to be an IS disaster, the DRC will determine emergency backup priorities (see Criticality Analysis) and strive to ensure resumption of IS operations to the fullest extent possible given the circumstances, consistent with the DRP.

## **Tornado/Storm Damage**

IS leaders shall determine the need to take emergency precautions upon notification of tornado or severe storms. Under the organization's emergency preparedness plan, information shall be communicated throughout the organization with regard to severe weather or tornado threat (e.g., Code Gray – Tornado Warning, etc.). IS leaders shall immediately respond and assess potential threats and determine appropriate preventive actions prior to the actual onset of storm or tornado conditions (see sections on "Power and Utility Failure" as well as "Water Damage").

## **Human Failure/Sabotage**

IS leaders shall determine appropriate actions in conjunction with Administration and/or Human Resources should human failure or sabotage result in an IS disaster. In the event of sabotage, Administration will determine the need to involve local and federal law enforcement agencies. The DRC will determine emergency backup priorities (see Criticality Analysis) and strive to ensure resumption of IS operations to the fullest extent possible given the circumstances, consistent with the DRP.

## **Pandemic**

IS leaders shall work with Administration and the Infection Control Nurse/Department to monitor threats posed by a pandemic emergency situation. IS shall be prepared to recognize the specialized needs of caring for pandemic patients, which may include quarantine and resulting limited access to areas housing information services applications, systems, networks, hardware, software, and other equipment. Additionally, IS leaders shall be prepared to address the need to accommodate workforce members on site and at remote locations, providing appropriate access when needed, should it not be feasible to allow members on site.

## **Electronic Restoration**

Prior to proceeding with electronic restoration, the organization needs to determine how to proceed. Electronic restoration is a process that requires considerable technology resources. An electronic restoration business partner should be identified as a IS disaster planning proactive measure. The business partner/process should address:

- What Can be Restored
- Criteria for Electronic Restoration
- Types of Contamination that Can be Removed

- Procedures for Fully Effective Electronic Restoration
- Cleaning Process
- Post Restoration Performance Expectations

What Can Be Restored: Electronic restoration has emerged as a highly sophisticated discipline. Research, development and testing have lead to increasingly refined, field-proven techniques for restoring a wide range of damaged electronic equipment that includes everything from computers to highly sensitive medical, manufacturing and telecommunications technology. Electronic restoration may be possible under extraordinary circumstances such as complete immersion in floodwaters as well as exposure to heat, smoke or corrosive vapors.

Criteria for Electronic Restoration: To completely remove contaminants and ensure total operational ability, damaged electronic equipment must meet certain criteria.

- It must be possible to remove contaminants completely from all surfaces.
- The success of the cleaning treatment must be reproducible and must not rely on chance results.
- The cleaning process itself must not cause any, or only cosmetic, damage to the equipment in question.
- The cleaning process must clearly be:
  - ◆ More economical than complete replacement of the equipment;
  - ◆ Or, significantly reduce business interruption due to long procurement time.

Types of Contamination That Can Be Removed: Fire and water damage, "natural contamination," and environmental factors all produce contaminants that damage vital electronic components. Each type must be dealt with as rapidly as possible, on a case-by-case basis. This is particularly true for fire and smoke damage that affect components differently than water damage or "natural contamination." Skilled electronic restoration specialists have the ability and the field experience to rapidly assess damage, access chemical expertise/analysis and establish a protocol to remove the contaminants. An experienced electronic restorer with access to a comprehensive array of specialty cleaning solutions can successfully remove the following contaminants:

- Soot Deposits
- Aggressive Deposits from Smoke and Chemical Vapors (Hydrochloric Acid)
- Deposits from Water (Lime, sludge, Mud)
- Residues of Chemical Extinguishing Powders
- Dust Deposits
- Other Pollution (Environmental, Operational, etc.)

Procedures for Restoring Damaged Electronics: Once it has been determined by the organization to begin an electronic restoration process and the technology meets the criteria, the following steps must be taken to ensure the electronics are restored properly.

1. Immediate action to avoid further damage, particularly after the impact of smoke and water damage, such as cutting all power and ending use of the equipment.
2. Chemical analysis of the type and concentration of contaminant.
3. Determination of the restoration protocols, procedures and cleaning chemicals.
4. The actual cleaning process including disassembly of the equipment and cleaning of individual components, frequently in many individual steps, by specially trained electronics specialists.
5. Optical and chemical quality testing.
6. Reassembly.
7. Adjustment and return to service.

The first and probably most important thing to remember is that time is the enemy of electronics and the best friend of corrosion. It is essential to hinder the destructive chemical process (corrosion), and prevent avoidable harm before comprehensive repairs begin. If preventive measures are taken rapidly, the organization will increase its chances for a successful restoration and limit the expense.

The individual/entity charged with electronic restoration shall evaluate the type of damage and take the appropriate measures. Experts in the fields of restoration and electronic restoration will come up with the correct course of action for the organization's particular needs and develop a plan to get the organization back up and running as quickly as possible.

In the case of fire damage, hydrochloric acid (HCl) is one of the biggest problems. When this is mixed with water from sprinkler systems or fire hoses, the corrosion of electronics progresses rapidly. This corrosive effect, however, can be minimized by applying a protective lubricant directly on the electronic components, removing all water from the room and lowering the relative humidity to below 40%. Once this is done, the chemical reaction of hydrochloric acid and metals will be drastically reduced and will allow technicians the time needed to restore the electronics.

When a room or area is flooded, electronic devices should be turned as soon as possible. Once electronic equipment is turned off, batteries removed and battery back-ups turned off, they will endure exposure to water relatively well. The longer the equipment is on, while partially or fully in water, the greater the chance for more significant and irreparable damage and short-circuiting. Once water comes in contact with the metal on circuit boards, the corrosion process has begun. Thus, it is essential for drying to begin as soon as possible, either by removing all water and lowering the relative humidity or removing the electrical equipment and placing it in drying rooms or drying ovens. When all the water has dried, the electronic restorer will use the appropriate chemicals to remove any contaminants, such as mud or lime residue.

To determine if other contaminants are present, electronic restoration experts will perform additional evaluation procedures. This is essential in order to select the appropriate cleaning compound to remove the contaminant without harming the electronics in any way.

Cleaning Process: To completely remove contaminants, all equipment components must be accessible. The cleaning process is done in the following five steps:

1. Disassemble the equipment - down to the last circuit board, if necessary, so that all components can be accessed.
2. Carefully decontaminate all individual components.
3. Perform visual and chemical tests to ensure the success of the cleaning operation.
4. Reapply protective coatings as needed.
5. Reassemble equipment.

All of these procedures must be carried out by trained and experienced electronic technicians to ensure the success of the restored equipment. Highly qualified technicians are able to dismantle any electronic device and reassemble it after a successful cleaning process. This can only be accomplished routinely if the electronic restoration partner has an established system for uniform disassembly and reassembly. Most qualified electronic restoration companies have engineers, chemists, and technical publications at their disposal in order to develop unique solutions to new challenges.

Success and Reliability of Restored Electronic Equipment: How successful is the restoration process and how reliable are the electronic components after restoration? It is estimated that 60 - 70% of all restored systems go back into operation without further repairs or disturbances. Observations of restored systems over a long period of time have shown that the reliability of the system is at least equal, in some cases better, than before the damage occurred.

## **Workforce Member Education and Training**

Members of the organization's workforce shall be provided education and training in emergency preparedness and disaster recovery upon hire and as needed to reflect any significant changes to the organization's emergency preparedness/disaster recovery practices, including information system disaster events and security incidents. Workforce members with specific responsibilities for IS disaster recovery shall receive the necessary education and training required to ensure that they can carry out their assigned duties in the event of an IS disaster event.

## **Review and Testing of Disaster Recovery Plan**

The DRP should be reviewed on an annual basis or as often as necessary to ensure that the information contained in the plan is up-to-date and reflects current workforce information (titles, names, and contact information), [applications/systems](#), vendors, and other external contacts information. Additionally, after each disaster incident, whether a planned drill or actual disaster, the plan should be reviewed and revised to address practical application issues.

## **Resources Used to Develop the IS Disaster Recovery Plan Template**

- "Creating an Actionable Disaster Recovery Plan," StoneBridge Group, HIMSS, April 2003
- "Electronic Restoration: Critical Considerations," Disaster-Resource.Com
- "An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12
- "Disaster Recovery Plan," St. Joseph's Hospital, 1991
- "Business Resumption Plan," Disaster Recovery Journal Website

- St. Clare’s Clinical Downtime Procedure
- “Disaster Recovery White Paper,” WEDI, April 2005
- “CMS Information Systems Security/Risk Assessment” Documents, 2004
- “Contingency Planning Guide for Information Technology Systems,” NIST, 800-34, June 2002
- Louisiana Hospital Association, Hospital Emergency Incident Command System

### Applicable Standards/Regulations:

- 45 CFR §164.308(a)(7) – HIPAA Security Rule Contingency Plan
- JCAHO Standard EC.4.10 – The Organization Addresses Emergency Management
- JCAHO Standard EC.7.10 – The Organization Manages its Utility Risks
- JCAHO Standard IM.2.30 – The Organization has a Process for Maintaining Continuity of Information

### Attachments

### EMERGENCY CONTACT LISTS

#### Departmental Information

INFORMATION SYSTEMS DEPARTMENT		
Information Services Helpline	Ext. 0000	M-F/8:00 a.m.- 5:00 p.m.
IS Department	Ext. 0000	M-F/7:00 a.m.- 5:00 p.m.
Information Services On-Call Contact (Pager)	000-000-000	After Hours

#### Disaster Recovery/Security Incident Response Team

DISASTER RECOVERY/SECURITY INCIDENT RESPONSE TEAM			
Position/Department	Name	Extension	After Hours Contact Information (Cell Phone/Pager)
Director, Inf. Services			
Security Officer			
Administrator/President			
Security/Plant Mgmt.			
Privacy Officer			
Risk Manager			
Human Resources			
Legal Counsel			
Media Relations			

<b>DISASTER RECOVERY/SECURITY INCIDENT RESPONSE TEAM</b>			
<b>Position/Department</b>	<b>Name</b>	<b>Extension</b>	<b>After Hours Contact Information (Cell Phone/Pager)</b>

**Organizational Leadership/Key Workforce Members**

<b>ORGANIZATIONAL LEADERSHIP/KEY WORKFORCE MEMBERS</b>				
<b>Position</b>	<b>Name</b>	<b>Home Phone</b>	<b>Cell Phone</b>	<b>Pager</b>
Administrator/CEO				
Administrator on Call				
VP-				
VP-				
VP-				
Security				
Plant Operations				

**Corporate Level Contact Information**

<b>MHC INFORMATION SYSTEMS STAFF CONTACT INFORMATION</b>				
<b>Name</b>	<b>Position</b>	<b>Home Phone</b>	<b>Cell Phone</b>	<b>Pager</b>

### System/Vendor Contact Information

Official System Name	
Acronym	
System Description	
Contact	
Phone #	
Emergency Phone #	
E-Mail	
Web Site/Support	
Contract Number	
Other	

Official System Name	
Acronym	
System Description	
Contact	
Phone #	
Emergency Phone #	
E-Mail	
Web Site/Support	
Contract Number	
Other	

Official System Name	
Acronym	
System Description	
Contact	
Phone #	
Emergency Phone #	
E-Mail	
Web Site/Support	
Contract Number	
Other	

Official System Name	
Acronym	
System Description	
Contact	
Phone #	
Emergency Phone #	
E-Mail	
Web Site/Support	
Contract Number	
Other	

Official System Name	
Acronym	
System Description	Electronic Restoration
Contact	
Phone #	
Emergency Phone #	
E-Mail	
Web Site/Support	
Contract Number	
Other	

### Law Enforcement/Government Agency Contact Information

Agency	Emergency	Other
Police Department	911	
Sheriff's Department	911	
State Patrol		
Fire Department	911	
Wisconsin Emergency Management	Check Nearest Office	<a href="http://emergencymanagement.wi.gov/">http://emergencymanagement.wi.gov/</a>
Federal Bureau of Investigation	Check Nearest Office	
U.S. Secrete Service (Regional Office)	414-297-3587 (Milwaukee)	

*Wisconsin Emergency Management specializes in Hazard Mitigation, Warning & Communications, Emergency Police Services, Disaster Response & Recovery, Hazardous Materials & EPCRA, Radiological Emergency Preparedness, and Exercise & Training for the State of Wisconsin. Emergency Management efforts are coordinated with state and federal agencies, as well as volunteer and private sector partners.*

### Other External Contact Information

Agency	Emergency	Other
Electric		
Water		
Gas		
Telecommunications-Phone		
Internet Service Provider		

## IS DISASTER RECOVERY SUPPORT TEAM CHARTER FORM

<b>IS Disaster Recovery Support Team Charter:</b>	
<b>Description/Scope</b>	
<i>Description and purpose of Team. Scope of services Team to address.</i>	
<b>Responsibilities</b>	
<i>Directives assigned to Team to be addressed/resolved.</i>	
<b>Authority Level</b>	
<i>To be Determined by DRC and Administrative Representative.</i>	
<b>Facilitated By</b>	
<i>Team Leader, As Appointed by DRC.</i>	
<b>Members</b>	
<i>To be Determined by DRC.</i>	
<b>Reports To</b>	
<i>DRC (Identity Position).</i>	
<b>Reports When</b>	
<i>Reporting Schedule to be Determined by DRC.</i>	
<b>Resources Required</b>	
<i>To be Determined by DRC and/or Team.</i>	
<b>Location</b>	
<i>Physical Location in Which Team will be Operating.</i>	
<b>Other</b>	
<i>At the Discretion of the DRC/Team Leader.</i>	



# DEPARTMENT INFORMATION SYSTEMS DOWNTIME PLAN/PROCEDURE TEMPLATE

**Summary:** The purpose of this plan is to ensure that each department/business unit has in place a plan and supporting procedures in the event of information system downtime. Each Department/Business Unit is responsible for identifying critical operations/essential processes that must be addressed during a downtime event. The Unit shall identify the critical or essential operations/processes external to the department, as well as those operations/processes that are internal to the department.

While this plan may be stored and made available on-line, in the absence of on-line access, paper copies should be available to those staff members responsible for or responding to downtime events.

**Responsibility:** Department or business unit leadership under the direction of administrative leadership.

**Downtime:** Period of time when information system applications, systems, and/or networks are unavailable due to planned or unplanned events. Scheduled downtime includes pre-defined events which have either been scheduled at regular intervals (e.g., routine back-up) or pre-scheduled in advance for maintenance purposes (e.g., system upgrade). Unscheduled downtime may occur at any time, usually as a result of failure in utilities, telecommunications, hardware, software, etc.

**Critical Operations/Essential Processes:** Those operations or processes that will impact the delivery of critical services by the department/business unit and/or result in significant operational losses if disrupted.

**Department/Business Unit:** *[Insert Name of Department/Business Unit]*

**Description:** *[Insert Brief Description of Department/Business Unit, Including Responsibilities, Key Stakeholders, Staffing, Hours of Operation, Etc.]*

**Probable Threats:** *[List Likely Threats Unique to Department/Business Unit]*

- Power Outage
- Application/System/Equipment Failure
- Flooding

## **Procedures:**

### 1. Notification of Downtime Event.

- A. **Planned Downtime:** The IS Department shall notify departmental leadership of planned downtime to allow for implementation of downtime processes. Departmental leadership shall be responsible for responding to the notification

Table of Contents..... 2

How to Use This Information Systems Disaster Recovery Plan Template .....	3
Overview .....	4
Objectives of the Disaster Recovery Plan.....	5
Applicability .....	5
Key Definitions .....	5
Information Systems Disaster and Security Incident Response .....	6
Authority .....	6
Administrative Oversight.....	7
Organization & Notification .....	7
Activation and Administration of the Disaster Recovery Plan.....	7
Disaster Recovery Coordinator (DRC).....	7
IS Disaster Recovery Team Emergency Contact Information.....	9
Damage Assessment .....	9
Assessing Resource Needs for Critical Disaster Recovery Operations.....	9
IS Disaster Recovery Command Center .....	10
Recovery Command Center Alternative Site.....	10
Recovery Resources Supply Checklist .....	12
Recovery Resources Supply Checklist .....	12
Recovery Team – Roles & Responsibilities .....	13
Other IS Disaster Recovery Support Teams .....	13
Communication Strategies.....	14
IS Disaster Recovery Team Status Report.....	14
Administration .....	14
Corporate/System Level.....	15
Media/Public Relations.....	15
Recovery Priorities.....	15
INFORMATION SYSTEM CRITICALITY ASSESSMENT TEMPLATE .....	16
Recovery Processes and Procedures .....	17
Data Backup Procedures.....	19
Telecommunications .....	19
General Recovery Pre-Planning.....	19
Telecom Emergency Communications and Resources.....	20
Telecom/Communication Infrastructure.....	20
Guidelines for Master Telecom Disaster Recovery Plan for Each Site .....	20
Real-Time Disaster Operations and Options .....	21
Electronic Health Record (EHR) .....	22
Other Checklists.....	23
Risk Analysis of Potential Disaster Threats/Responses.....	23
Power Failure .....	23
Utility Failure (HVAC).....	23
Water Damage/Flooding.....	24
Fire/Smoke Damage.....	24
Equipment/Hardware Failure.....	24
Explosion .....	24
System/Application/Software Failure.....	25
Tornado/Storm Damage.....	25

Human Failure/Sabotage.....	25
Pandemic.....	25
Electronic Restoration.....	25
Workforce Member Education and Training.....	28
Review and Testing of Disaster Recovery Plan.....	28
Resources Used to Develop the IS Disaster Recovery Plan Template.....	28
Applicable Standards/Regulations:.....	29
Attachments.....	29
EMERGENCY CONTACT LISTS.....	29
Departmental Information.....	29
Disaster Recovery/Security Incident Response Team.....	29
Organizational Leadership/Key Workforce Members.....	30
Corporate Level Contact Information.....	30
System/Vendor Contact Information.....	31
Law Enforcement/Government Agency Contact Information.....	32
Other External Contact Information.....	32
IS DISASTER RECOVERY SUPPORT TEAM CHARTER FORM.....	33
IS DISASTER RECOVERY STATUS REPORT FORM.....	34
DEPARTMENT INFORMATION SYSTEMS DOWNTIME PLAN/PROCEDURE TEMPLATE.....	35
B. and implementing those processes and procedures required to support critical operations/essential functions.	
C. <u>Unplanned Downtime</u> : In the event of unplanned downtime, the IS Department <sup>3</sup> shall notify departmental leadership as soon as possible to allow for implementation of emergency downtime processes. <i>Of Note: Should the     department staff suspect they are the first to discover an unplanned downtime     occurrence, the staff shall immediately notify the IS Department and/or the     appropriate leadership person available (e.g., after hours – nursing     supervisor, on-call management, etc.).</i>	
2. Upon receipt of notification of a downtime event that may impact the department’s ability to provide services, the departmental leadership shall determine the need to contact internal and external stakeholders and provide notification of the event and potential disruption of services.	
A. <u>Internal/Departmental</u> : Departmental leadership shall determine the need to contact:	
1. Departmental workforce members ( <i>See Addendum A - Departmental/         Business Unit Contact Information</i> ).	
2. Department/business unit leaders within the organization which may be impacted by the downtime event.	
B. <u>External/Organization-Wide</u> : Departmental leadership shall determine the need to contact external stakeholders which may be impacted by the downtime event ( <i>See Addendum B – Vendor Support Contact Information</i> ).	

---

<sup>3</sup> Notification may also be issued by other relevant departments (e.g., administration, plant operations, telecommunications, etc.).

3. Departmental leadership shall determine the critical operations/essential processes that must be addressed during a downtime event. Leadership shall include those critical operations that are provided “external” to the department as well as those that are internal to the department. Information shall include the name of the operation, supporting IS application, back-up capabilities/medium, and downtime processes.

Critical Operations/Essential Processes (External): List those departmental operations which may impact other organizational departments and units in the event of downtime (list all applicable operations – examples indicated in red).

Operation	IS Application	Backup	Downtime Processes
<i>Access to Patient Health Information</i>	<i>Meditech PCI</i>	<i>Mirrored Server</i>	<i>1. Access backup server for stored information. 2. Access available paper records.</i>
<i>Creation of Patient Health Information Documents</i>	<i>Meditech PCI, Other Meditech Applications</i>	<i>Manual Process</i>	<i>1. Document in temporary paper back-up record (which includes appropriate forms).</i>

Critical Operations/Essential Processes (Internal): List those internal departmental operations which are critical to operations of the department (list all applicable operations – examples indicated in red).

Operation	IS Application	Backup	Downtime Processes <sup>4</sup>
<i>Chart Tracking</i>	<i>Meditech HIM</i>	<i>None</i>	<i>1. Maintain manual log of chart movements.</i>

4. In the event of an unplanned downtime situation where there has been significant disruption and loss of services, the departmental leadership shall coordinate recovery processes with the IS Department and/or administration as needed.
5. Following a downtime event, the departmental leadership shall evaluate the department’s response and determine the need for future testing and revisions to this plan. If necessary, the departmental leader shall make the necessary revisions to the plan and ensure appropriate communication to impacted internal and external workforce members.
6. The department IS downtime plan and procedures should be reviewed and tested periodically (annual review recommended). Additionally, the plan should be reviewed and tested to reflect updates in applications and systems. Following review and testing, the plan should be revised as appropriate to reflect needed changes.

<sup>4</sup> Including manual processes.

7. Departmental leadership shall be responsible for ensuring that the department's workforce members are provided training, education, and awareness of this plan. This may be carried out through:
- A. Review/sign off of plan document.
  - B. Prominent posting and availability of plan.
  - C. Departmental meetings and inservices covering plan components.

**Addendum A: Department/Business Unit Contact Information**

GENERAL DEPARTMENTAL INFORMATION		
Director	Ext. 0000	M-F/8:00 a.m.- 5:00 p.m.
Department/Business Unit Primary Extension	Ext. 0000	M-F/7:00 a.m.- 5:00 p.m.
On-Call Contact (Pager #)	000-000-000	After Hours

DEPARTMENTAL CONTACT INFORMATION			
Position/Department	Name	Extension	After Hours Contact Information (Include Pager/Cell Numbers)
<i>Director</i>			
<i>Assistant Director</i>			
<i>Supervisor</i>			
<i>Lead -</i>			
<i>Staff Member</i>			

**Addendum B: Vendor Support Contact Information:**

Official System Name	
Acronym	
System Description	
Contact	
Phone #	
Emergency Phone #	
E-Mail	
Web Site/Support	
Contract Number	
Other	

Official System Name	
Acronym	
System Description	
Contact	
Phone #	
Emergency Phone #	
E-Mail	
Web Site/Support	
Contract Number	
Other	

**Responsibility for Implementation:**

- Departmental/Business Unit Leadership

**Approved By:**

Title/Business Unit

**Date:** 00/00/05

**Reviewed by IS Department:**

Title

**Date:** 00/00/05

**Review Date:**

**Key Words:** Downtime, Failure, Outage

**Sources:**

- St. Clare's Clinical Downtime Procedure

**Applicable Standards/Regulations:**

- 45 CFR §164.308(a)(7) – HIPAA Security Rule Contingency Plan
- JCAHO Standard EC.4.10 – The Organization Addresses Emergency Management
- JCAHO Standard EC.7.10 – The Organization Manages its Utility Risks
- JCAHO Standard IM.2.30 – The Organization has a Process for Maintaining Continuity of Information

***Handout: The 2006 AHIMA Convention and Exhibit; Disaster Response and Business Continuity: Lessons from Hurricane Katrina; Sunday, October 8, 2006***