DEPARTMENT: Environment of Care **POLICY: EOC- 280**

SUBJECT: Information Services Disaster Recovery & Business Continuity

PURPOSE: Frances Mahon Deaconess Hospital (FMDH) has created this policy in order to maintain the viability and integrity of the business and clinical operation should there be a disaster. This policy will be followed to manage any situation that significantly disrupts critical, important, or marginal business functions that have been defined as a disaster.

RESPONSIBILITY:

- Information Services (IS) staff

DEFINITIONS:

- **Internal Emergencies –** An Internal Emergency involves an incident within the hospital that disrupts normal hospital operations. Incidents include bomb threats, internal utility failures, and equipment failures.
- **External Emergencies –** An External Emergency involves an incident beyond the immediate boundaries of the hospital. External Emergencies include snowstorms, utility outages, and tornadoes that may not impact the hospital directly, but could require a status alert for the facility.
- **Critical functions** – Critical business and clinical functions are identified as communication of medical information with clinical staff and contracted providers, and the systems necessary to complete this communication (software, computers, etc).
- **Important functions** – Important business and clinical functions are identified as telephone systems, voice mail, computers and software not used for direct communication of medical information, safety and security and finance operations.

POLICY:

The Disaster Recovery Policy provides an organized process to initiate, manage, and recover from a variety of emergencies, both external and internal, which could disrupt the information systems at FMDH. This policy addresses the most probable occurrences that would disrupt the information systems at FMDH. The Disaster Recovery Policy will work in conjunction with FMDH's Emergency Operations Plan (EOP) (EOC-200). Each FMDH Department has outlined the steps to be taken in order to provide the necessary services needed for patient care and business support functions during any disruption.

1. Preparedness
    a. FMDH maintains spare equipment and parts for essential systems in areas other than where the essential equipment is running.
    b. Whenever possible, FMDH operates primary and backup devices in different physical locations within the facility.
    c. FMDH uses backup software that allows restoring of systems to alternative hardware.
    d. Contacts
        i. Grabar Voice and Data

1. (888) 239-1311

ii. Meditech
    1. (781) 821-3000
    2. (508) 879-4000

iii. Meditech Servers (Park Place)
    1. (800) 343-4654

iv. Iatrics
    1. (978) 539-0734

v. Symantec Corporate Workspace (nSuite)
    1. (800) 342-0652

vi. Cerium Networks
    1. (406) 256-2233

vii. Med Dispense
    1. (402) 806-1826

viii. eClinical Works
    1. (508) 475-0450

ix. Fuji (PACS)
    1. (800) 272-8465 – sy 0107089530

x. General Servers (Dell)
    1. (866) 930-3355 – # 2018538

xi. AppAssure
    1. (703) 480-0100

e. Additional contact information is available in the IS-Biomed Equipment System Responsibility spreadsheet, located in the Information Services policy and procedure folder on the Intranet.

2. Mitigation
    a. FMDH backs up servers on the Local Area Network (LAN) in full each night. Offsite copies of tapes are stored at a third party.
    b. This backup process is outlined in the policy File and File Server Backups (IS-211).
3. Hazard Vulnerability Analysis
    a. Frances Mahon Deaconess Hospital identifies the potential hazards, threats, and adverse events and assesses the impact on the care, treatment, and services sustained during an emergency. The assessment is a Hazard Vulnerability Analysis (HVA) which is designed to assist in gaining a realistic understanding of the vulnerabilities and to help focus the resources and planning efforts. A list of priority concerns will be developed from the HVA and are evaluated annually. The HVA will include the likelihood of those events occurring, and the consequences of those events, and the ability to provide services during those events. The hospital's HVA is reviewed annually by the Safety Committee.

PROCEDURES:

The cycle from the occurrence of a disaster to the full restoration of normal processing may have four phases which include: initial response, preparation for temporary back up site operation, restoration, and return to permanent facility.

Information received by Frances Mahon Deaconess Hospital concerning an external emergency facing the community or an internal emergency involving the function of the Hospital will be passed directly to the CEO, COO, or designated administrative person in charge during normal business hours or the on-duty charge nurse after hours and on weekends. This person will evaluate the issues concerning this emergency and determine if initiation of the EOP is warranted.

Once it has been determined to activate the EOP, the individual who takes the role of Incident Commander will notify the on-site hospital staff, administration, and other staff as appropriate as soon as possible, following the procedures laid out in the EOP.

1. External Emergencies:
    a. In the event of an external emergency, such as a tornado, flood or the like, IS staff will use the following guidelines according to the time allowed before the onset of the emergency/disaster.
        i. During normal hours the Director of Support Services is notified of potential disaster and will notify IS staff. After hours the IS on-call staff is notified of potential disaster and will notify the Director of Support Services. Director of Support Services or designee will report to the briefing area as per the EOP.
        ii. IS staff will meet in IS office and await further instructions.
        iii. IS staff will verify location and date of last backup
        iv. IS staff will gather working flashlights, extra batteries, and plastic for covering PC equipment from the supplies located in the Emergency Management storage area.
        v. Verbally inform Meditech, MedDispense, Symantec, Winscribe, eClinical Works, Fuji and any other vendors of impending disaster and changes or needs.
        vi. If danger of power outage or weather damage, instruct hospital staff via loudspeaker system or telephone to unplug PC and printer equipment from wall outlets.
        vii. Run any census reports as desired by Incident Commander or section chief.
        viii. If extreme danger of weather and water damage, instruct hospital staff via loudspeaker system, telephone and LAN to move any computer equipment away from windows. Offer IS staff assistance in this effort.
        ix. Determine if additional backups of data are needed. If so, at Logistics Chief's direction,
            1. notify users to log off appropriate system
            2. disable access to system
            3. take backup of system
        x. Determine if file servers should be shut down. If so, at Logistics Chief's direction, begin notifying staff of shutdown and begin orderly shutdown of servers
        xi. If required, telephone calls will be re-routed to pre-designated areas

xii. Determine when computer equipment may be powered on and brought on-line. Follow normal startup procedures for servers. Notify hospital users via telephone or loudspeaker system when systems are available for use.

2. Internal Emergencies:
    a. In the event of an internal emergency, such as a bomb threat, explosion, chemical spill, power failure or the like, IS staff will follow the following guidelines.
        i. During normal hours the Director of Support Services is notified of potential disaster and will notify IS staff. After hours the IS on-call staff is notified of potential disaster and will notify the Director of Support Services. Director of Support Services or designee will report to the briefing area as per the EOP.
        ii. IS staff will meet in IS office and await further instructions.
        iii. IS staff will verify location and date of last backup
        iv. IS staff will gather working flashlights, extra batteries, and plastic for covering PC equipment from the supplies located in the Emergency Management storage area.
        v. Verbally inform Meditech, MedDispense, Symantec, Winscribe, eClinical Works, Fuji and any other vendors of impending disaster and changes or needs.
        vi. Determine if additional backups of data are needed. If so, at Logistics Chief's direction,
            1. notify users to log off appropriate system
            2. disable access to system
            3. take backup of system
        vii. Determine if file servers should be shut down. If so, at Logistics Chief's direction, begin notifying staff of shutdown and begin orderly shutdown of servers.
        viii. Determine if any other computer equipment is in danger of being damaged. If so, assign IS staff to power down and move equipment as needed.
        ix. If required, telephone calls will be re-routed to pre-designated areas
        x. Determine when computer equipment may be powered on and brought on-line. Follow normal startup procedures for servers. Notify hospital users via telephone or loudspeaker system when systems are available for use.
3. Power Failure
    a. In the event of a power failure, IS staff will advise all hospital staff to shut off all non-essential equipment. Non-essential equipment is equipment that is not used in direct patient care or in support of direct patient care.
    b. Emergency power system
        i. FMDH is equipped with a diesel backup power generator which provides power to the FMDH emergency circuit during an interruption of normal electrical service.
            1. The generator has fuel enough for 5 days of continuous operation and a plan for the reliable re-supply of fuel exist.
        ii. All servers and phone switches are on emergency generator power, and also have battery backups.

4. Communication Failure:
    a. Telephones
        i. If the phone system is down, the IS staff will troubleshoot the telephone system to determine if the failure is an internal or external failure/problem.
        ii. Staff will follow the Telephone and/or Paging Systems Failure procedure (EOC-751).
        iii. If voice mail is not functional, messages will be taken and callers will be provided with alternate means of contact (i.e.; cellular, radios) to reach their parties
    b. Radios
        i. Radios are available for communication inside of the facility. Personal cell phone will be used as well as radios.
5. Environmental Failure (Server Room):
    a. If a problem is detected concerning the server room environment, such as electrical, water damage, excessive heat, cold, or humidity, appropriate IS and Maintenance staff will be notified immediately. If the issue arises after hours, the on-call staff will be contacted by using the information on the call schedule located in the Meditech system.
6. Notes:
    a. In the event all electronic systems are down, each department has a manual procedure in place to ensure workflow continues with minimal interruption.
    b. If evacuation is necessary key staff will need to be available to perform functions related to setting up an alternative information system at alternate locations.
7. Testing:
    a. This policy will be tested at least bi-annually, through drill or actual event, documenting the steps to be taken in order to return to business quickly and efficiently.
        i. Steps taken will be documented as the testing takes place.
        ii. The Management Staff will meet after the testing to evaluate what was done and how it could have been done more quickly and/or efficiently following the Post Incident/Drill Critique Procedure (EOC-220) found on the FMDH intranet.
        iii. Each test will be documented and available for review by FMDH's Management staff.
    b. If a real situation occurs that disrupts the day to day business of FMDH, these situations will also be documented using the Post Incident/Drill Critique procedure (EOC-220).
        i. Once the situation has been resolved, FMDH's Management Staff will meet to evaluate what was done and how it could have been done more quickly and/or efficiently.
        ii. Documentation will be available for review by FMDH's Management Staff.

REVIEW PROCESS:

- This policy will be reviewed every two years.