PURPOSE

To help ensure that Business Continuity remains and mission critical data can be restored in a timely manner at the University of Arkansas for Medical Sciences ("UAMS").

SCOPE

The UAMS Workforce.

DEFINITIONS

Backup means creating a retrievable, exact copy of data.

Disaster means an event that causes harm or damage to UAMS information systems. Disasters include, but are not limited, to the following: earthquake, tornado, flood, fire, extended power outage, equipment failure, or a significant cybersecurity event.

Confidentiality means ensuring that data or information is not made available or disclosed to unauthorized persons or processes.

To access any other terms or definitions referenced in this policy: https://hipaa.uams.edu/wp-content/uploads/sites/136/2019/02/DEFINITIONS-HIPAA.pdf

POLICY

UAMS Information Technology (IT) will establish and implement, as needed, the UAMS IT Disaster Recovery Plan (DRP) which contains contingency policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages IT supported systems that contain UAMS data. The IT Division is committed to employing all appropriate strategies for anticipating and controlling crisis situations by implementing the IT DRP.

PROCEDURE

1. IT Management is responsible for establishing and maintaining the IT Emergency Recovery Plan (ERP). The plan will include:

    A. The Disaster Recovery Plan (DRP) that contains procedures which will serve as a guide to IT Management and Staff for:

a. Verification of redundant network and offsite server systems which are defined in the Disaster Recovery Critical Systems List. This list assesses the relative criticality of specific applications and data in support of other contingency plan components. The list is updated as new systems or redundant equipment for existing systems are purchased, and as system status is upgraded to higher priorities.
b. Implementation of Backup procedures for all server systems that IT supports. The recovery plan establishes and implements procedures to use these Backups for the process of restoring these server systems and their data.
c. Replacing hardware via Vendor Agreements which define schedule based on availability of hardware.
d. Procedures that allow physical facility access during emergencies to support restoration of data.

B. A Business Continuity Plan (BCP), which serves as an emergency mode operation plan to establish and implement procedures to enable continuation of critical business processes while operating in emergency mode. The BCP is comprised of departmental procedures supplied to IT for publishing in the Emergency Response Plan and will serve as a guide to UAMS staff toward continuing normal business operations during an IT Emergency

2. Individual UAMS Division Areas or Department designees will assist in the development of plans for their areas of responsibility, to include appropriate maintenance of their respective plans, which are to be consistent with the overall Policies and Procedures established by senior IT Management.

3. All employees are expected to comply with established practices and procedures of the ERP, which are designed to minimize the risk to themselves and others, as well as to minimize threats to personnel, technical resources, property, or to the security of the facility. Individual workstation users on the network are responsible for Backups and data security for local storage space.

4. The Disaster Recovery Plan will be reviewed and updated annually.

5. An IT Disaster will be called, and the IT Disaster Recovery Plan initiated, when any situation occurs that disables access to the systems in the Data Center and requires ordering new hardware to be delivered to an alternate location for setup and access.

6. Copies of the Disaster Recovery Plan and other documents referenced in the Plan will be stored off-site on the third-party Disaster Recovery Website. The documents will be readily available for reference online, or for delivery in the event of an emergency situation that restricts or prohibits access to the normal workplace.

7. When an IT Disaster is called, the Disaster Recovery Plan should be referenced.

- IT staff responsible for getting systems back on-line should access the Emergency Response Plan section and follow the instructions under their department heading.

- All other UAMS staff should follow their established Business Continuity Plans

SANCTIONS

Violation of this Policy will result in disciplinary action, in accordance with Administrative Guide Policy 4.4.02*, Employee Discipline* and UAMS Administrative Guide Policy 2.1.42, *HIPAA Sanctions Policy.*

Signature:  **Date: May 9, 2023**