ARKANSAS SCHOOL FOR MATH, SCIENCES, + THE ARTS

Backup & Recovery Process

The Role of IT in Disaster Recovery and Continuity of Operations

IT maintains the technology infrastructure critical to all campus processes. This includes connectivity, phone service, and access to campus software. Disaster recovery and continuity of operations depends on the extent of the damage to:

- Software
- Hardware
- Facilities, especially the server room
- Combinations of the above

The critical campus software products are Workday and underlying Microsoft infrastructure including Windows Server platforms including Office 365 and Microsoft Azure. The platform for online classes is Blackboard, which is hosted offsite but has a connection directly to ASMSA through the setup of a single sign on (SSO).

Campus connectivity is provided by 2 incoming fiber lines provisioned from ARE-ON and managed by the same company up to the Firewall. The phone system is Voice Over IP (VOIP) and is connected by ARE-ON.

The Server room is in CIC. The room has 1 dedicated AC unit. Room temp monitoring. room.

The connections to other buildings are by fiber. Switches are located at key juncture points. IT maintains a complete inventory of all equipment, key information, location, and service date.

The software environment is protected by industry-standard methodology – virus scan, blocking, NG firewall, physical security, and required user authentication. The software/hardware environment is protected by the following back up procedures:

All file servers at ASMSA:

- Are backed up at a file level basis daily via Campus NAS
- The NAS server is a RAID5 array for data integrity and redundancy.
- NAS backups are stored locally (One in CIC and a Second NAS located in Admin), and an encrypted backup is taken offsite.

The campus Workday environment:

- All cloud based and can be accessed anywhere and anytime.

Recovery Process Tasks Lists

In response to a disaster, various functional areas on campus, including IT, administration, maintenance, and faculty/division chairs, are ready to perform the following tasks to provide recovery and continuity of operations for the campus.

IT task list: In response to a disaster, IT staff will:

- Initiate crisis management plan
- Initial damage assessment and estimate time to recovery.
- Notify administration of extent of the damage
- Initiate call list
- Protect systems.
- Check network connectivity and electricity.
- Perform shut down procedures, including power down and unplug all machines.
- Perform recovery processes.

On site

- Checklist of usable resources still available Notify vendors of resources needed.
- If necessary, provide remote access to designated personnel.
- Restart systems as appropriate
- Verify functionality of systems

Alternate site

- Notify alternate IT site.
- Notify vendors to stand by
- Checklist of usable resources still available
- Notify vendors of resources needed.
- Move IT operations and available resources to alternate sites.
- Start setting up alternate location.
- Provide remote access to designated personnel.
- Provide support in the cleanup of the server room following the disaster.

Ongoing during recovery

- Report to administration on status of recovery effort
- Coordinate media and press releases with the public information officer