

Mount Olive School District Disaster Recovery Plan

Section 1. Major goals of this plan

The major goals of this plan are the following:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

Section 2. Personnel

Super - Dr Robert Zywicki

Director - Kimberley Markus

Director of B&G - Glenn Miller

Network Engineer - Jim Neglia

Telephony Admin - Kathy Steinert

Network Support Specialist - Ryan Feidler

Network Support Specialist - Shane Sexton

Section 4. Inventory profile

Inventory

Add hardware
inventory

Section 5. Information services backup procedures

Ryan F

Section 6. Disaster recovery procedures

For any disaster recovery plan, the following three elements should be addressed.

Emergency Response Procedures

To document the appropriate emergency response to a fire, natural disaster, or any other activity in order to protect lives and limit damage.

Backup Operations Procedures

To ensure that essential data processing operational tasks can be conducted after the disruption.

Recovery Actions Procedures

To facilitate the rapid restoration of a data processing system following a disaster.

Disaster action checklist

1. Plan Initiation
 - a. Notify Superintendent, Director on Innovation and Director of Buildings and Grounds
 - b. Contact and set up disaster recovery team
 - c. Determine degree of disaster
 - d. Implement proper application recovery plan
 - e. Monitor progress
 - f. Contact all other necessary personnel--both user and data processing
 - g. Contact vendors--both hardware and software
 - h. Notify users of the disruption of service
2. Follow-Up Checklist
 - a. List teams and tasks of each
 - b. List all personnel and their telephone numbers
 - c. Establish user participation plan
 - d. Determine applications to be run and in what sequence
 - e. Identify number of workstations/laptops needed
 - f. Check out any off-line equipment needs for each application

- g. Check on forms needed for each application
- h. Set up primary vendors for assistance with problems incurred during emergency
- i. Take copies of system and operational documentation and procedural manuals.
- j. Ensure that all personnel involved know their tasks

Section 7. Restoring the entire system from Backup (local & Cloud)

Section 10. Rebuilding process

The management team must assess the damage and begin the reconstruction of a new data center.

If the original site must be restored or replaced, the following are some of the factors to consider:

- What is the projected availability of all needed computer equipment?
- Will it be more effective and efficient to upgrade the computer systems with newer equipment?
- What is the estimated time needed for repairs or construction of the data site?
- Is there an alternative site that more readily could be upgraded for computer purposes?

Once the decision to rebuild the data center has been made, go to Section 12. Disaster site rebuilding.

Section 11. Testing the disaster recovery plan

In successful contingency planning, it is important to test and evaluate the plan regularly. Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document. Use these checklists as you conduct your test and decide what areas should be tested.

Section 12. Disaster site rebuilding

- Floor plan of data center.

- Determine current hardware needs and possible alternatives. (See Section 4. Inventory profile.)
- Data center square footage, power requirements and security requirements.
 - Square footage _____
 - Power requirements _____
 - Security requirements: locked area, preferably with combination lock on one door.
 - Floor-to-ceiling studding
 - Detectors for high temperature, water, smoke, fire and motion
 - Raised floor

Vendors

Floor plan

Include a copy of the proposed floor plan here.

Section 13. Record of plan changes

Keep your plan current. Keep records of changes to your configuration, your applications, and your backup schedules and procedures. For example, you can get print a list of your current local hardware, by typing: