Disaster Recovery Plan
for Center Moriches School District
Information Technology Operations

I. Plan Overview

The disaster recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs in the Center Moriches School District that impacts Information Technology (IT). Each supported site, Clayton Huey (CH) and Secondary Campus (HSMS), has a section containing general recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the sensitive nature of the information contained in the plan, the plan should be treated as a confidential document.

II. Plan Approval

This plan has been reviewed and approved by the Center Moriches School District Board of Education.

_________________________ _________________________

Wendy R. Turkington
Board of Education President

Date

III. Disaster Declaration

Personnel authorized to declare a disaster or resume normal operations are:

Name	Title
Russell Stewart	Superintendent of Schools
Lynda Adams	Deputy Superintendent

IV. Plan Activation

This plan will be activated in response to internal or external threats to the Information Technology Systems of CMUFSD. Internal threats could include fire, bomb threat, or loss of power or other utility or other incidents that threaten the staff and/or the facility. External threats include events that put the facility in danger. Examples might include severe weather or a disruptive incident in the community. Once a threat has been confirmed, the plan management team will assess the situation and initiate the plan if necessary based upon the approval of the Superintendent of Schools or their designee.

Resuming Normal Operations

Once the threat has passed, equipment has been repaired or replaced or a new data center has been built and functional, the disaster recovery team will assess the situation, declare the disaster over and resume normal operations.

V. Plan Overview, Objectives and Decisions

Plan Overview

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples the school's computer systems operated by the Information Technology Services Department. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available. This plan is designed to reduce the number of decisions which must be made when, and if, a disaster occurs.

This plan is a "living document." It is the responsibility of everyone involved in Center Moriches' disaster recovery efforts to ensure that the plan remains current. When you are aware of any changes to personnel, hardware, software, vendors or any other item documented in the plan, please bring them to the attention of the plan administrator.

Plan Objectives

The overall objectives of this plan are to protect Center Moriches' computing resources and employees, to safeguard the vital records of which Information Technology Systems is the custodian, and to guarantee the continued availability of essential IT services. The role of this plan is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data center and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in IT capabilities. This plan assumes the most severe disaster, the kind that requires moving computing resources to another location. Less severe disasters are controlled at the appropriate management level as a part of the total plan.

The basic approach, general assumptions, and possible sequence of events that need to be followed are stated in the plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The plan is a roadmap from disaster to recovery. Due to the nature of the disaster, the steps outlined may be skipped or performed in a different sequence. The general approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs. It is also assumed vendors and knowledgeable personnel from CMUFSD will be actively enlisted to help during a recovery situation.

The plan represents a dynamic process that will be kept current through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the plan will be revised to reflect the current IT environment.

The Disaster Recovery Management Team consists of: CMUFSD information technology personnel and administration, and potentially technology support vendors as needed.

VI. Disaster Recovery Phases

Step 1: Disaster Assessment
Step 2: Recover from Disaster
Step 3: Rebuild Systems
Step 4: Return to Home

Disaster Assessment

The disaster assessment lasts from the time the disaster is declared until it is under control and the extent of the damage can be assessed. Cooperation with Suffolk County Emergency Services Personnel is critical.

Recover From Disaster

When the decision is made to move primary processing to another location, this phase begins. The Disaster Recovery Management Team will assemble and call upon team members to perform their assigned tasks. The most important function is to fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternate location, Step 2 is complete.

Rebuild Systems

This phase involves continuing operations at the alternate location. In addition, the process of restoring the primary site will be performed.

Return to Home

This phase involves the reactivation of the primary data center at either the original or possibly a new location. The activation of this site does not have to be as rushed as the activation of the alternate recovery center. At the end of this phase, a thorough review of the disaster recovery process should be taken. Any deficiencies in this plan can be corrected by updating the plan.

VII. Disaster Decision Tree

Event	Decision
Both sites destroyed/unusable	Activate disaster recovery plan A
Either site destroyed/unusable	Activate disaster recovery plan B
Both sites unusable for two days or less	IT team assess situation and recommends resolution, Activate disaster recovery plan C
Either site unusable for two days or less	IT team assess situation and recommends resolution, Activate disaster recovery plan C

VIII. Disaster Recovery Plans

Disaster Recovery Plan A

Both sites, CH and HS/MS are destroyed or unavailable.

Decision Point	Actions			
Both buildings destroyed. Equipment lost.	1. Need to determine alternate location to set up new data center and user workstations.	2. Need to order replacement hardware. • Servers • Switches • SANs • Workstations	3. Configure and install new equipment.	4. Restore data for applications and users.
Both buildings unusable. Equipment intact.	1. Need to determine alternate location to set up new data center and user workstations.	2. Retrieve necessary hardware from buildings once buildings are accessible.	3. Re-configure equipment for alternate location.	

Recovery Time / Objectives

The Recovery Time reflects the estimated recovery times based on current configurations and operations. This is a generalized estimate, assuming destruction of current equipment. Other factors such as the district's procurement process, environment and reliance on outside vendors could increase these times.

Service	Recovery Time
LAN (Local Area Network, includes starting server(s) for Active Directory and DNS)	20 days estimate
WAN (Wide Area Network)	30 days estimate
Internet access	20 to 30 days estimate

Disaster Recovery Plan B

Either site, CH or HS/MS are destroyed or unavailable.

Decision Point	Actions				
Either building destroyed. Equipment lost.	1. Need to determine alternate location to set up user workstations.	2. Set up workstations in alternate locations. Re-configure network and bring up replicated virtual servers at second site.	3. Need to order replacement hardware. • Servers • Switches • SANs • Workstations	4. Configure and install new equipment at restored site.	5. Migrate replicated data back to alternate site.
Either building unusable. Equipment intact.	1. Need to determine alternate location to set up user workstations.	2. Set up workstations in alternate locations. Re-configure network and bring up replicated virtual servers at second site.	3. Once the building is available migrate replicated data back to site.		

Recovery Time / Objectives

The Recovery Time reflects the estimated recovery times based on current configurations and operations. This is a generalized estimate, assuming destruction of current equipment. Other factors such as the district's procurement process, environment and reliance on outside vendors could increase these times.

Service	Recovery Time
LAN (Local Area Network, includes starting server(s) for Active Directory and DNS)	5 to 20 days estimate
WAN (Wide Area Network)	5 to 30 days estimate
Internet access	20 to 30 days estimate

Disaster Recovery Plan C

Either site unusable for two days or less.

Decision Point	Actions			
Either site unusable for two days or less.	1. Communicate with CM administration on necessity of action.	2. Communicate with utility companies and Emergency Management Services.	3. Determine course of action based upon available information.	

Recovery Time / Objectives

The Recovery Time reflects the estimated recovery times based on current configurations and operations. This is a generalized estimate. Other factors such as the district's procurement process, environment and reliance on outside vendors could increase these times.

Service	Recovery Time
LAN (Local Area Network, includes starting server(s) for Active Directory and DNS)	2 days estimate
WAN (Wide Area Network)	2 days estimate
Internet access	2 days estimate

IX. Recovery Time / Objectives

The Recovery Time reflects the estimated recovery times based on current configurations and operations. This is a generalized estimate, assuming destruction of current equipment. Other factors such as the district's procurement process, environment and reliance on outside vendors could increase these times.

The Application Level Restoration are dependent on a plan (A, B, or C) being completed prior to the time allotted below.

Application Level	Recovery Time
Level 1	Immediate after LAN,WAN, and Internet restored
Level 2	5 to 20 days after LAN and Internet restored
Level 3	15 to days after LAN and Internet restored
Level 4	When possible

Level 1 – eSchoolData, emails (Microsoft Online), eBoards. *This assumes outside service providers are functioning.*
Level 2 – Finance Manager, cmschools.org website
Level 3 – User data files, less critical applications (Read180, Waterford, etc.).
Level 4 – Remote access (Citrix)

These Recovery Times should be considered *best-case* estimates. Currently, CMUFSD does not have computer hardware available for immediate recovery nor contracts in place to obtain hardware on a priority basis. In the event of a disaster, hardware would have to be located, purchased, shipped, installed, and configured before any software or data could be installed or restored. The availability of the relevant equipment and shipping times could vary greatly depending on the timing and scope of the disaster.

The network services and application recovery times are additive in nature in the case of a disaster that affects servers and the LAN. However, a WAN or Internet disaster takes significantly longer to recover from due to the installation schedules of telecommunications providers/installers.

Adopted: January 29, 2014