



**Western Line**  
**SCHOOL DISTRICT**

2023-2024  
IT Disaster Response Plan

### Revision History

REVISION	DATE	NAME	DESCRIPTION
Original	06/06/2023	Kimberly Orgeron	

# Information Technology Statement of Intent

This document delineates our internal procedures for technology disaster recovery, as well as our process level plans for recovering critical technology platforms. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems and our data. Our mission is to ensure information system up time, data integrity and availability and business continuity.

## Objectives

The principal objective of the disaster recovery plan (DRP) is to develop, test and document a well-structured and easily understood plan which will help the school system recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan.
- The need to ensure that proposed contingency arrangements are cost-effective.
- The need to consider implications on all WLSD sites.
- The need to ensure that key operations and critical services experience minimal downtime, so as not to disrupt the business of WLSD or the education of our students.

## Definitions

- Barracuda Backup Appliance - is the backup product used by WLSD. It allows for backup of physical and virtual machines.
- RAID - Redundant Array of Independent Discs
- VOIP - Voice Over Internet Protocol. A phone system which utilizes internet protocol for voice communication rather than the traditional telephone system.
- Internet Service Provider - For WLSD this is C-Spire
- LAN - Local area network. This refers to the networking of computers within a building.
- WAN - Wide area network. This refers to the networking of computers from site to site.
- Key Personnel

## Key Personnel

- Dr. Lawrence Hudson, Superintendent

- James Johnson, Asst. Superintendent
- Glenda Ketchum, Interim Business Manager
- Daphne Young, Federal Programs Director
- Kimberly Orgeron, Technology Coordinator and Public Relations Officer
- Henry Miller, Maintenance Director
- Wanda Leslie, SPED Director
- Renae Humphrey, Human Resources
- James Branning, Safety and Transportation Director
- Chris Bozek, Network Consultant from Synergetics

## Overview

### Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to all relative documents.

### Plan Documentation Storage

DRP will be available on the WLS D website under the Technology Department section. A hardcopy will be stored in a fire-proof safe at the WLS D Central Office.

### Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. Primary storage of data backups is the WLS D Barracuda Backup device.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	The Barracuda Backup device is backing up nightly. A copy is also uploaded to the cloud for off site storage.
Email	Cloud based solution.
Disaster Recovery	All servers are currently backed up via Barracuda. The Barracuda and cloud have enough storage to accommodate all servers that have been selected to be backed up.

Finance	Marathon is backed up each evening offsite by Central Access. It is also backed up daily by the Barracuda.
Student Information System	SAM Spectra is hosted offsite by Central Access.
Library System	Destiny is hosted offsite by Follett.

## Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. Key trigger issues that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Loss of data
- Flooding
- Loss of structure

## Communications with Employees

Directors will serve as the focal points for their departments while designated employees will contact other employees to discuss the crisis/disaster and the immediate plans.

## Communications with Public

The public information officer will communicate, as necessary, to the public at the direction of the superintendent. These communications will include alternate methods of contacting schools, if necessary.

# Technology Disaster Recovery Plan

## Disaster Recovery Plan for Servers

The backup plan for each situation is outlined below.

1. Individual server failures will be handled by Synergetics DCS. The servers will be spun up from a backup and hosted on the virtual servers.
2. Data Corruption/Accidental Deletion - In the event of data corruption or accidental deletion, Windows Volume Shadow Copy will be tried first (if enabled on the server in

question) as this is the fastest method. Otherwise, Barracuda can perform file level recovery from either backup repository.

3. Backup Storage RAID Failure - In the event of a Backup Storage RAID failure the following steps will be performed:
  - a. Contact Barracuda and they will ship a replacement preloaded with the last set of backups from the Cloud Storage
4. Ransomware - In the event of a ransomware attack the following steps will be performed:
  - a. Determine extent of damage (Active Directory servers only, etc.)
  - b. If only AD servers are affected then the AD server will be restored from the Barracuda as necessary

## Disaster Recovery Plan for Phones

In the event of a phone outage, all locations have the option of utilizing a district issued Cellular phone to maintain communications.

## Disaster Recovery Plan for Local Area Network (LAN)

Replacement switches, cabling and other hardware is kept on hand to replace/repair any issues with LAN connectivity within a building. Such issues will be made top priority with a target down time of no more than three days. Synergetics DCS will assist with any issues that arise.

## Disaster Recovery Plan for Local Area Network (WAN)

The WLSO WAN is managed by C-Spire. WLSO IT will maintain communications with C-Spire and manage any expectations that arise from users.