Quitman School District
IT Disaster Recovery Plan

School Board
Approved

JUL 18 2022

Quitman School
District

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	Spring 2022	Matthew Champion	
1.1	Summer 2022	Matthew Champion	Updated Key Personnel

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 QSD sites.
- The need to ensure that key operations and critical services experience minimal downtime, so as not to disrupt the business of QSD or the education of our students.

Definitions

Veeam - Veeam is the backup product used by QSD. It allows for backup of virtual machines.

VMWare vSphere - vSphere is the server virtualization product utilized by QSD. It allows multiple virtual servers to run on one physical server.

SAN - Storage Area Network. This is a collection of hard drive space which can be partitioned virtually. It works with the vSphere system to allow for timely data transfer.

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 QSD 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

Dr. Minnie Dace, Superintendent
Mrs. Elisa Mayo, Finance Director
Mrs. Tracy Dearing, Federal Programs Director
Mr. Matthew Champion, IT Director
Mr. Joseph Holloman, Maintenance Director
Mr. Adam Boyette, SPED Director
Mrs. Carrie Holloman, HR
Mr. Ricky Graham, Transportation
Mrs. Debra Martin, PIO
Mr. Mike Hollingsworth, Consultant

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 QSD website under the Technology Department section. A hardcopy will be stored in a fire-proof safe at the QSD Central Office and also in a fire-proof safe in the QSD Technology Department.

Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. Primary storage of data backups is the QSD Technology Department Network Operations Center. This strategy entails the maintenance of a duplicate site which will enable timely switching of servers. This duplicate site has been identified as LAUREL SCHOOL DISTRICT, located 43.5 miles South of the Network Operations Center. The Finance system is located at the QSD Central Office and backed up nightly to an off-site location configured by Central Access using error detection methods to ensure data integrity.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Veeam is currently backing up nightly to a SAN and also offsite to Laurel. In the event of a disaster the servers can be spun up using the image that has been backed up.
Email	Cloud based solution.
Disaster Recovery	All virtual servers are currently backed up via Veeam. The SAN has 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.
Web Server	The web server is backed up nightly via Veeam.
Student Information System	SAM Spectra is hosted offsite by Central Access.
Library System	Destiny is hosted offsite by Follett.
SPED Information System	SpedTrack is hosted offsite by SpedTrack

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
- Fire
- 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 Millenium Consulting Service, LLC. 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, Veeam can perform file level recovery from either backup repository.
3. Primary Storage SAN/RAID Failure - In the event of a Primary Storage RAID failure the following steps will be performed:
    - Replace SAN/RAID or prepare alternative storage
    - Restore virtual machine images from Veeam server
4. Backup Storage RAID Failure - In the event of a Backup Storage RAID failure the following steps will be performed:
    - Replace RAID or prepare alternative storage
    - Reinstall Veeam server and Veeam software
    - Setup new local Veeam repository
    - Load Veeam configuration backup from offsite repository
5. Ransomware - In the event of a ransomware attack the following steps will be performed:
    - Determine extent of damage (Active Directory servers only, Veeam server, etc.)
    - If only AD servers are affected then the AD server will be restored from the Veeam onsite repository as necessary
    - If the Veeam server is affected then the Veeam server will be wiped and reloaded from the backup repository

Disaster Recovery Plan for Phones

In the event of a phone outage, all locations have the option of utilizing a Public Switched Telephone Network (PSTN) line to ensure a constant line of communication to parents, community, etc. Should the Public Switched Telephone Network (PSTN) line not be an option, key staff will utilize cell phones, (district provided cell phones first, personal cell phones second) 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. Millennium Consulting Service, LLC will assist with any issues that arise.

Disaster Recovery Plan for Local Area Network (WAN)

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