Norwayne Local School District

Information Technology Disaster Recovery Plan

December 2018

Revision History

Revision	Date	Name	Description
Original	**December 2018**	**Ryan Wile**	

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 uptime, 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 Norwayne sites.
- The need to ensure that key operations and critical services experience minimal Downtime and maintain continuity of daily operations and student education.

Definitions

HyperV: HyperV is the server virtualization product utilized by Norwayne. It allows multiple virtual servers to run on one physical computer.

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

VoIP: Voice over Internet Protocol. A phone system which utilizes internet protocol for voice communication, rather than the traditional telephone system.

ISP: Internet Service Provider. For Norwayne, it is provided by our ITC.

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.

ITC: Information Technology Center. For Norwayne it is Tri-County Computer Services Association.

DRP: Disaster Recovery Plan

Key Personnel

Name	Title
Karen O'Hare	**Superintendent**
Ryan Wile	**Technology Coordinator**
Bill Vance	**Maintenance Supervisor**
Sandy Hadsell	**Treasurer**
Roy Templeman	**Director- TCCSA**

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

The DRP will be available on the district website, and a hardcopy will be available in each district building.

Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. Primary storage location of data backups is on state managed servers in Columbus, Ohio. This strategy allows for a secure offsite storage location for all data backups. A 1 gigabit connection exists between the Data Center and Northern Middle School. The Finance/HR system software is accessed remotely as a service provided by our ITC.

Key Business Process	Backup Strategy
IT Operations	Active Directory, the Staff Network File Storage Location, Access Control and Print Server info is incrementally backed up multiple times each day to a remote location via TCCSA's contracted backup service.
Email	Email is provided through a cloud based solution
Finance/HR	Provided by a contracted solution accessed remotely.

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 the building

Communication with Employees

Managers 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.

Communication with Public

The district office will communicate, as necessary, to public. These communications will include alternate method 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 byTCCSA. The server will be restored from a backup and restored to the designated HyperV host.
2. In case of a HyperV host server failure all virtual machines will be ran off of one server. Each host sever is capable of running all servers independently.
3. In case of a partial SAN failure the affected servers will recreated either on stand alone servers or a HyperV server.
4. In case of a partial SAN failure the affected servers will recreated either on stand alone servers or a HyperV server.

Disaster Recovery Plan for Phones

In the event of a VoIP phone outage, most locations have the option of utilizing a temporary hardline phoneline to ensure a constant line of communication to parents, community, etc. Should VoIP and the hardline are not options, key staff will utilize cell phones to maintain communications.

Disaster Recovery Plan for Local Area Network (LAN)

Replacement switch, 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 one school day.

Disaster Recovery Plan for Wide Area Network (WAN)

Norwayne internet access is provided and managed by TCCSA. In the event of an outage, TCCSA will be contacted and responsible for restoring service.