Garrett County Public Schools

IT Disaster Recovery Plan

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	Summer 2015	Jeff Gank	

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

Definitions
AppAssure
        AppAssure is the backup product utilized by GCPS. It allows for backup of virtual machines, and will provide a hosting environment.
Hyper-V
        Hyper-V is the server virtualization product utilized by GCPS. 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 Hyper-V 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 GCPS, these include DotCOM, Comcast, and Verizon.

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

Name Title
Dr. Janet Wilson, Supt
Mr. Tim Thornburg, HR
Mr. Larry McKenzie, Finance
Ms. Barb Baker, Asst. Supt. Ed Services
Mr. Jeff Gank, IT
Mr. Bill Swift, Maintenance
Mr. Scott Germain, FNS
Mr. Jim Morris, PIO
Mr. Rich Wesolowski, Transportation

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 GCPS website, and a hardcopy will be stored in a fire-proof safe, located in Dennett Road Data Center

Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. Primary storage location of data backups is Dennett Road Educational Complex Data Center. This strategy entails the maintenance of a duplicate site which will enable timely switching of servers. This duplicate site has been identified as Northern Middle School, located 23 miles north of the Data Center. A 1 gigabit connection exists between the Data Center and Northern Middle School. The Finance/HR system is located at Central Office, and backed up daily via tape. Tapes are stored in a fire-proof safe, which is housed in the data center at Dennett Road.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	AppAssure is currently backing up Active Directory servers on an hourly basis. In the event of a disaster, the servers can be exported directly to either AppAssure server. The exported VM can also be ran from either AppAssure server.
Email	Cloud based solution.
Disaster Recovery	All virtual servers are currently protected by AppAssure. Each server currently has enough storage to accommodate all servers.
Finance/HR	CIMS currently gets backed up each evening to a tape drive. It also gets a full backup done weekly.
Web Server	All web servers are currently backed up with AppAssure.
Student Information System	The PowerSchool server is currently backed up with AppAssure.
Library System	Destiny is currently backed up with AppAssure.
Building Security	The iDenticard server is currently backed up with AppAssure.

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 public information 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 by AppAssure. The server will be stood up from a backup and hosted on the AppAssure server or moved to one of the Hyper-V hosts.
2. In case of a Hyper-V 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 be ran off of AppAssure devices.
4. If there is a full SAN failure critical servers will be hosted off of each AppAssure server.

Disaster Recovery Plan for Phones
In the event of a phone outage, most locations have the option of utilizing a temporary VoIP phone to ensure a constant line of communication to parents, community, etc. Should VoIP not be an option, 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)
Most of the GCPS WAN is managed by the ISP. GCPS IT will maintain communications with the ISP, and manage expectations of users.