Introduction

This document defines the backup guidelines within the Randolph County School System. These systems are typically servers, Storage Area Network devices (SAN), or Network-Attached Storage devices (NAS) but can include other devices. The Randolph County School System uses 2 (two) Hper-V servers, one standalone domain controller, and 4 (four) specialty devices All servers and devices are backed up at intervals defined by their role and level of critical information stored on the server or device. All protected data (Financial and Student Information Data) will be backed up daily. Backups may be in the form of virtual server snapshots/images, individual file backups and/or SQL database backups.

Purpose

- To safeguard the information assets of the Randolph County School System.
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

Detailed Procedure Statement

The Directory of Technology is designated as the backup manager. The backup manager will be responsible for setting up, monitoring, and verifying backup and restore jobs according to the following guidelines.

All Servers deployed in the Randolph County School System are classified under one of 8 possible categories:

- Application Server
- Backup Server
- Database Server
- Management/Monitoring Devices
- Domain Controller
- Email Server
- File Server
- Task Server

Back up schedules are based on the above categories with the exception of the key enterprise systems, which have additional daily backups performed to optimize recovery. Daily backup jobs are completed on an appliance unit while monthly backup jobs are completed onto tapes housed in the tape library. Systems will be backed up according to the schedule below:

SAN & NAS Appliances

All data stored on the SAN and/or NAS appliances are attached to other servers and will be backed up during those severs back up periods

Application Serves will be regularly backed up as follows:

Enterprise Systems
Full backup daily (Monday)
Incremental (Tuesday – Saturday)
Full Backup Monthly

Other Application Severs
Full backup at least once a week
Full backup monthly

Backup Servers will be regularly backed up as follows
Full backup daily (Monday)
Incremental (Tuesday – Saturday)
Full Backup Monthly

Database Servers will be regularly backed up as follows:
Full backup daily (Monday)
Incremental (Tuesday – Saturday)
Database snapshots twice daily
Full Backup Monthly

Domain Controllers will be regularly backed up as follows:
Full backup daily (Monday)
Incremental (Tuesday – Saturday)
Full Backup Monthly

Email Server stores will be regularly backed up as follows:
The Randolph County School System uses the Google email platform and a level of redundancy is provided by Google.

File Servers will be regularly backed up as follows:

Enterprise Systems
Full backup daily (Monday)
Incremental (Tuesday – Saturday)
Full Backup Monthly

Other Task Servers
Full Backup once a week
Full Backup Monthly

The daily backups are stored in the IDF/District Office on an appliance and then replicated to an identical appliance located off- site. Locally stored backups are stored in a fireproof storage safe. Any failure that occurs during a backup job is emailed to the designated backup manager daily, and any failures will be addressed on that same day.

Servers are selected randomly for a complete disaster recovery to test the full recovery of systems. Depending on the type of server, testing the backup and recovery is performed either twice a year or once a year.

The Technology Coordinator will maintain electronic records demonstrating the corrective action of failed backups and test restores to demonstrate compliance with this Procedure for auditing purposes. In addition, the Technology Coordinator will identify problems and take corrective action to reduce any risks associated with failed backups.

Data Recovery:

- In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 to 5 business days after the destroyed equipment has been replaced.

- In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 to 2 business days.

PROCEDURE

Overview

The purpose of this procedure is to establish a standard for the management and protection of district electronic information.

Areas of responsibility

The District of Technology will perform duties.

Procedure details

The frequency and extent of backups must be in accordance with Backup Policy. The Technology Coordinator will adhere to the following:

- Become familiar with District's backup hardware and software.

- Determine the importance of the servers and the data contained within via consultation with Information Technology Services Supervisors and setup backup sets accordingly.

- Create, delete, and modify existing backup sets in accordance with Backup Policy.

- Review daily backup logs and correct any errors to ensure data integrity.

- Perform quarterly tests on backup sets to ensure entire servers can be restored in case of disaster recovery.

- Respond to restore requests in accordance with Backup Policy.

Applicability

This Procedure applies to any and all Information Technology Department staff. It is critical to the functionality of the district that any person who fails to adhere to this Procedure may be subject to disciplinary action.