DATA RECOVERY AND PROTECTION PROCEDURES 6524-R

The purpose of these procedures is to outline the data protection and recovery procedures to ensure network security and maintain continuity of technology operations for Watauga County Schools.

Scope

The primary component of data recovery will be effective, timely data and system configuration backup. Other components should include (but not be limited to): 1) the acquisition of top quality equipment that operates efficiently with built-in redundant features to help avoid data loss due to system failure; 2) centralized management and acquisition of all network equipment and workstations to ensure recoverability of configurations and settings; 3) implementing effective, up-to-date virus protection on all network servers and workstations; 4) effective controls to prevent downloading and installation of errant applications and programs without prior approval and opportunities for testing of those programs; and 5) other measures deemed necessary by the district level technology director, as newer issues emerge.

Responsibilities

1. District technology staff will be responsible for the following backups;
    a. All centralized backups from designated schools and Central Office
    b. Centralized file servers (both virtual and physical)
    c. Network switch settings and configurations
    d. Firewall settings and configurations

2. School based technology personnel will be responsible for backing up the following;
    a. Any mission critical files, configurations, data, etc. which are not handled centrally.

3. Finance, Personnel, and Transportation will be responsible for backing up systems configurations and data exclusive to their individual systems (not housed on WCS centralized servers).

4. All Watauga County Schools' employees are responsible for backing up the following:
    a. Data stored on their individual workstation hard drives. This may be done by copying this data to external media (i.e. CDs, USB drives, etc.) In the course of normal maintenance to workstations, it may be necessary to reconfigure workstations thereby losing any data saved on individual hard drives. Employees are expected to maintain critical data on network or cloud storage to assure proper file backups.

Virus Protection Guidelines

All files downloaded to the Watauga County Schools' computer network might potentially harbor computer viruses or other destructive programs (collectively called "viruses"); and therefore, all downloaded files must be scanned for such viruses. Virus detection programs and practices shall be implemented throughout the school system. Training must take place to ensure that all computer users know and understand safe computing practices. Designated staff shall make certain that all computer equipment has the most current anti-virus software and appropriate patches installed.

1. Virus education and training is the shared responsibility of the WCS Technology Department and the school-based technology staff:
    a. Providing directions for use of anti-virus software, including scanning for viruses on files or external devices, as required.
    b. Providing guidance before any software is added to the network or individual device, whether from public software repositories, or other systems.
2. System configuration management is the responsibility of the WCS Technology Department and includes:
    a. Installation and management of anti-virus software on all LAN servers and workstations
    b. Periodic review of overall controls to determine weaknesses
    c. No network connections to outside organizations without a mutual review of security practices
    d. Use of software that can be verified to be free of harmful code or other destructive aspects.
3. Incident management procedures include:
    a. Verification of a virus threat
    b. Identify the personnel/program responsible for mitigation of threat
    c. Maintain process for identifying, containing, eradicating and recovering from virus threat
    d. Individual reporting of all virus incidents that extend beyond a single PC to the WCS Technology Department

Other Considerations

Although backing up data is critical to all applications, proper backups will not always assure effective restoration of systems. Whenever possible, redundant systems should be ready for reconfiguration and restoration in the event of a disaster. Testing of recovery procedures should be executed whenever possible.

Procedure

In the event of infrastructure and/or server failure, plans for restoring computing and network facilities for the Watauga County Schools are outlined below. This plan lists those measures that are in place to assist in such a recovery, as well as the actual steps taken after the disaster to begin

the restoration process.

Restoration Process

1. Technology Director is contacted with the report of the network disaster.
2. Technology Director directs appropriate personnel to conduct damage assessments and construct a priority list for restoration/recovery.
3. Technology Director and other appropriate personnel use the priority list to develop a strategic plan for network recovery.
4. Director will keep the Superintendent informed of findings and plan for recovery.

Suggested prioritization of network components:

Highest priority – network backbone (firewall, switches, wiring components, call managers, main servers that contain critical operational data)
Medium priority – web filter, network print services, desktop computer of critical personnel
Low priority – instructional computer labs, desktop computers and individual peripherals

The WCS Technology Department will maintain and review these procedures for implementation in the event of a disaster. As network requirements and configurations change, the WCS Technology Department will make recommendations to the WCS Media/Technology Advisory Committee to reflect current requirements.

Adopted: April 10, 2017

Replaces: Policy 4.02.55 Disaster Recovery Policy and 4.02.65 Virus Protection Policy