Central Islip Union Free School District

Board of Education & School District Policy Book
50 Wheeler Rd. | Central Islip | N.Y. | 11722
(631) 348-5000
https://www.centralislip.k12.ny.us

Section	Section Title	Type
8000	Support Services	Local
Policy	**Policy Title**	
8630.1	Disaster Recovery and Business Continuity Policy	

Natural, civil and unplanned disasters can create havoc on the district network causing immediate loss of connectivity, student data, staff data, financial data, application data, Email, communications and documents. The Central Islip School District has created scenarios and plans to quickly recover in the event of a disaster.

The Superintendent's designee, the Administrator for Instructional Technology, shall plan and test for multiple levels of disasters to ensure the district is as prepared as possible if disaster strikes.

The Disaster Recovery Plan is constantly reviewed and updated, and is kept on file with the Superintendent of Schools, the Administrator for Instructional Technology and appropriate technical staff.

Contained within the district's Disaster Recovery Plan:

- Complete listing of all domain controllers including hardware and warranty information.
- Complete listing of all district servers including all software application, vendor support contact information and specific program recovery details.
- Complete listing of all routers and switches as well as infrastructure mapping and topography including all configuration files hardware support information.
- Complete listing of all Physical Host Servers and all Virtual Servers including all IP Addresses and remote access information.
- Complete list of district UPS (Uninterrupted Power Supply), battery information and support information.
- Back Up Standards, Procedures and Locations.
- Disaster Scenarios and Recovery Plans
- All Vendor Support Contacts (Hardware, Software, ISP, Fiber, etc.).

ROUTER & SWITCH CONFIGURATION FILES

Switches, routers, firewalls and other device configurations are backed up to a server disk share, which is in turn backed up to enclosure. Configurations are updated as they are changed.

DOMAIN CONTROLLERS

- Disk-to-disk off-site backup and replication to a server in another building.
- Backup completion is monitored by in-district staff.
- Replication does not allow for historical file recovery (as files are backed up nightly, there is no way to go back to prior versions of files or retrieve files that have been recently deleted from backup).
- Volume Shadow Copy is enabled on Domain Controllers which allows for retrieval of recently deleted or altered files as long as server is functioning. The available history is dependent on free disk space and volume of changes.

DISASTER SCENARIOS & RECOVERY PLANS

1. **Hard Drive Failure:** Most servers which host information include a RAID array for hard drives so that they can continue to function even after losing a hard drive. The failed drive can be replaced with minimal impact on server availability. In the case where a drive failure causes data loss, repair or restoration from backup or replicated server will be employed.
2. **Single/Multiple Server Failure:** Server hardware will be repaired or rebuilt and operating system, applications and data will be repaired or restored from backup. In many cases, such as Terminal Servers, Domain Controllers and Exchange Servers, there is already server redundancy which will allow systems to continue to function while repairs are made, resulting in minimal impact to availability and no data loss.
3. **Internet Connectivity Loss:** In the event of an Internet outage, every Principal is equipped with a Verizon Wireless MiFi Broadband Card and account. Principals can use their MiFi Card to connect up to 10 devices to the Internet and maintain necessary communications throughout the outage. For longer outages, this type of access can be arranged on a building-wide basis.
4. **Wide Area Network Connectivity Loss:** If the Wide Area Network connections between the schools fail, each school has local Domain Controllers, Terminal Servers and File Storage to allow the schools to function independently. If there is an extended outage, traffic can be rerouted over Internet connections using Virtual Private Network

connections, or in the case of schools with line-of-site connectivity, a temporary wireless solution can be put into place.

5. **Inability to Physically Access Hardware:** All systems are configured with Remote Access, so in the cases of a security or health situation which prevents building access, system can be accessed both for technical support and configuration, as well as user access to applications and data.
6. **Inability to Access a Building:** In case a building is not accessible, district offices can be relocated to any in-district computer lab within any accessible building. If needed, Wincap will be contacted to migrate the server into the new designated location.
7. **Off-Site Backup of Critical Data:** In the event of a total loss due to a larger disaster, critical information including Student Data Records and Financial Records are replicated nightly and stored securely in off-site hosted locations with considerable geographical separation from the district.

1st Reading: February 10, 2014
2nd Reading: March 10, 2014
Adoption date: March 10, 2014