



Comsewogue Public Library Disaster Plan for Computer and Data Recovery

Objectives of this plan: Ensure sufficient back up of critical computer resources; designate responsibilities ensuring compliance with strategies; to assure plan compliance to the greatest extent possible.

Citation of Responsible Personnel: Library Director or designee and Network Administrator or designee. The Network Administrator and the Library Director will review annually standard actions and procedures to prevent data loss, and propose updates/revisions as needed.

Types of Disasters/Events/Incidents:

1. Exterior: weather, physical plant issues
2. Interior: floods, accidents, utility failure, mandatory lock down
3. Network: Virus/malware/hacking

The Library Director or person in charge of the facility in the event of a computer emergency will:

1. Take immediate actions to ensure security
2. Notify Library Director who will notify President of the Board of Trustees, Network Administrator, and other critical individuals in an appropriate order according to circumstances
3. Continue actions to ensure data and hardware security
4. Document all emergencies/incidents in writing to the Library Director

Standard response to emergency situations:

1. The Network Administrator or designee will determine severity of emergency and impact on computers and the network
2. Network Administrator will collaborate with Library Director, Department Heads and act quickly to prevent loss of data
3. The Network Administrator or designee will oversee the shutdown of affected computers and/or the entire network as needed

Actions Routinely Taken to Prevent Data Loss:

1. UPS and surge protection on Library servers is maintained
2. Server backups are to occur nightly
3. Backups are rotated off-site 1 per week for 5 weeks
4. Immediately upon completion of the backup (starting July 31, 2013), data is sent to cloud storage

Network Security:

A network firewall is installed monitoring and regulating all inbound/outbound traffic. Servers hosting data available to the outside only have ports open that are necessary to function.

Anti-virus:

All computers have anti-virus software installed. Updates are done automatically as they are available.