Seaford Public Library

Electronic Systems Risk Assessment & Management

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 annually review 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
4. Biological Viruses: Remote access to the Library is setup for the Director, Assistant Director, Network Administrator and Accountant. In the event of a county-wide or larger virus outbreak or lockdown, the Library Director will closely monitor and follow guidance provided by relevant health authorities.

In the event of a systems emergency, the Library Director or person in charge of the facility will:

1. Take immediate action to ensure security
2. Notify the 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 and 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.
4. All follow-up actions to be determined by the Director

Steps to prevent recurrence:
An initial investigation shall commence within 24 hours of detection. The investigation will include the identification of affected systems, the scope of the incident, root cause and preventive action recommendations. The Library Director shall appoint an Incident Response Designee who will lead the investigation, and findings will be documented and shared with the Director and Assistant Director.

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. Immediately upon completion of the backup, data is sent to cloud storage
4. The designee will review the plan annually.

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.

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

Adopted 5/8/2017
Revised 7/8/2024
Amended: 9/9/2024