Infrastructure Security and Backup Policy

System Backups and Data Recovery:

The Lindenhurst Memorial Library requires that their computer systems maintained by the Network and Systems Specialist fall under one of several backup profiles as described below. The purpose of a systems backup is to provide a level of business continuity of our computer system in the event of a hardware/software failure, physical disaster, or human error.

All core infrastructure and staff workstations are backed up on an automated schedule, to ensure the ability to provide a means of restoring the data of a computer system in the event of a hardware/software failure, malicious attack on the Library's infrastructure, physical disaster, or human error.

Each backup profile consists of either a full back up or incremental backup. A full backup contains every file on the system, whereas an incremental backup includes only those files that have changed since the last full backup. Backups are performed on a periodic schedule as determined by the Library in conjunction with the Network and Systems Specialist.

Two copies of each backup are produced. One is maintained onsite, and one offsite for protection against building events, natural disasters, malicious attack or hardware failures. The primary copy is onsite on a dedicated storage device located within the main library building, in a locked server rack. A secondary copy is replicated to an offsite location. Data is retained for a period of one year. A full backup is generated monthly to ensure an up-to-date range of data. Daily incremental back-ups occur as needed to check for any changes to data.

Administration Server:

A scheduled full backup of the separate Administration File server, Time clock server, accounting software and Administration staff user data are taken on a monthly backup cycle. These backups are also replicated to the offsite backup location.

Incremental backups of the Administration File server, Time clock server, accounting software and Administration staff user data are taken on a nightly backup cycle. These backups are then replicated to the offsite backup location.

Network Infrastructure:

A scheduled full backup of all network appliances configurations and data is taken on a weekly backup cycle. These backups are then replicated to the offsite backup location.

Staff File Server:

A scheduled full backup of the Staff File server, Application server, Patron Library Card software, PcReservation Software, Anti-Virus Software, and non-administration staff user data is taken on a monthly backup cycle. These backups are then replicated to the offsite backup location.

A scheduled incremental backup of the Staff File server, Application server, Patron Library Card software, PcReservation Software, Anti-Virus Software, and non-administration staff user data is taken on a nightly backup cycle. These backups are then replicated to the offsite backup location.

Security and Data Protection

Firewalls and Network appliances:

All devices connected to the Lindenhurst Memorial Library network must be placed behind a Library owned security system to maintain Library approved network traffic and to protect against malicious software entering the Library Network.

Network Access:

All devices connected to the Lindenhurst Memorial Library network, not including the Library provided public WIFI, are to be approved by the Network and Systems Specialist or Library Director and provided a designated static IP address or wireless network associated password.

All unused physical ports on Library owned network devices are set to disabled within the network device interface, and only re-enabled after given the approval by the Network and Systems Specialist or Library Director.

Anti-Virus:

All Library owned devices connected to the Lindenhurst Memorial Library must have Anti-Virus software installed by the Library to protect against the installation and/or spread of malicious software within the library network.

Updates:

All Library owned devices connected to the Lindenhurst Memorial Library network will have updates applied to all installed software and operating systems monthly or when needed to patch a software vendor alerted issue.

Patron Privacy:

All Library owned public workstations connected to the Lindenhurst Memorial Library network have software installed to ensure all patron data is erased prior to the use of that workstation by any future patrons.

Access Permissions:

All Library owned devices connected to the Lindenhurst Memorial Library network are put on the Library domain. All permission levels, and access to shared resources, will be approved by the Network and Systems Specialist or Library Director. All software installations on Library owned devices will be approved by the Network and Systems Specialist or Library Director.

Administrative Rights and Passwords:

The Network and Systems Specialist and Library Director will both have copies of all passwords for network hardware/software, servers, patron and print management systems, back-up systems, filters, and any other related security or system controls.

Approved: November 21, 2020