Board Adopted: 12/5/2018
Board Reviewed:
Board Revised: 5/4/2022

Shenandoah Public Library Network Security Policy

Purpose

The Shenandoah Public Library local area network (herein referred to as "the SPL network" or "the network") is critical to the provision of information services to SPL staff and patrons. The SPL library automation system processes sensitive and valuable information. The addition of public access to the Internet within the library has increased the size, complexity, and management concerns related to the operation of the network. Specific security measures and procedures must be implemented to protect the confidentiality of information transactions being processed on the network and to keep critical systems operational. Because all citizens of Shenandoah are encouraged to use the network for informational and educational needs, security risks have increased and more stringent practice in safeguarding resources is necessary than was required when simple standalone PCs were used. These expanding security requirements are addressed in the following network security policy.

This policy has two purposes. First, the policy will emphasize to all Shenandoah Public Library employees and patrons the importance of network security in the library and their roles in maintaining that security. Second, the policy will assign specific responsibilities needed to secure networked information resources.

Scope

The SPL network security policy covers all electronic information resources in the library. It applies equally to network servers, workstations, both staff and public access, network equipment, telecommunications equipment, and peripherals, such as printers, within the library. The policy applies to all library users, managers, and administrators, including Library staff, patrons, contractors, and City staff utilizing the Library's network resources.

Goals

The SPL security program is designed to ensure the availability of networked resources and the integrity and confidentiality of data transmitted over and stored on the network. Specifically, the goals of the program include:

- Ensuring the library network has sufficient security measures applied to protect the integrity of its data, the privacy of information transactions, and the availability of its resources;

- Ensuring the cost of the security measures implemented is commensurate with the risks present on the network;

- Ensuring appropriate budgetary and technical support is available and maintained;

- Training all users to be responsible for the security of data, information, and other computing resources to which they have access, and training staff to maintain accountability practices;

- Enforcing policies and technical mechanisms which contribute to the auditability of network resources;

- Providing sufficient guidance to library staff in the discharge of their responsibilities in network and information security;

- Ensuring that all applicable organizational and departmental policies and procedures are applied and practiced;

- Developing appropriate contingency or disaster recovery plans to provide continuity of operation for all critical functions of the network.

Responsibilities

Responsibility for implementing and maintaining the Library's network security goals is divided among five specific groups.

1. Public Users (PU) - volunteers and public users who have access to the SPL network. End users are responsible for using the network resources in accordance with the provisions of the Library's Computer and Internet Use Policy. All users of data and network services (such as the Internet) are responsible for complying with security policy established by library and network management and for reporting to management any actual or suspected breach of security.

2. Staff Users (SU) - library staff who have access to the SPL network. Staff users are responsible for using the network resources in accordance with the provisions of this

security policy and the Library's Computer and Internet Use Policy. All users of data and network services (such as the Internet) are responsible for complying with security policy established by library and network management and for reporting to management any actual or suspected breach of security.

3. Library Management (LM) - the library director, library board, and other library administration, if applicable, who have functional responsibility for the library. Library Management is responsible for informing staff about this policy, assuring that each person has a copy, and interacting with staff and volunteers on security issues.

4. Network Management (NM) - contract technical support persons or library staff involved in the technical support, management, and operation of the SPL network. Network Management must ensure the continued operation of the network and is responsible for implementing appropriate network security measures as indicated in this security policy.

5. Local Administrators (LA) - library staff responsible for ensuring that end users have access to needed network resources available through the library's servers or Internet access. Local administrators provide day-to-day maintenance of network security in accordance with this security policy. Local administrators are responsible for reporting observed breaches of security policy to network and library management.

Enforcement

When end users fail to comply with this policy, SPL information-while stored, processed or transmitted on the Shenandoah Public Library network-may be exposed to the unacceptable risk of loss of confidentiality, integrity or availability. Violations of security guidelines and procedures established to support this policy will be brought to the attention of management for action and could result in disciplinary action up to and including termination of employment or termination of rights to use the network.

GENERAL POLICIES OF THE LAN

GP1. Every workstation and server shall have a designated local administrator who is responsible for maintaining the security of the computer. All end users of the system are responsible for following all policies and procedures in this policy and the acceptable use policy. SPL staff who manage workstations or servers shall be trained so they can follow all policies and procedures effectively.

GP2. Server security shall be exclusively controlled by the Library Director, the Technology & Teen Librarian and network management. Access to server security mechanisms by all other staff, volunteers, or public users shall be considered unauthorized access.

GP3. The local administrator responsible for each workstation or server must ensure that all software installed on the system is approved for use and is licensed properly.

GP4. All software installation and updates shall be the responsibility of network management or the designated local administrator.

GP5. The Technology & Teen Librarian shall oversee the backup of server and workstation hard drives.

GP6. Each staff member and contract worker shall have access to only passwords needed for the performance of duties. Users must not share or disclose passwords. Volunteers and members of the public should never receive library passwords.

GP7. The following statements apply to the construction of passwords for network devices:

- Passwords must be at least 10 characters
- Passwords must be comprised of a mix of upper and lowercase characters, numbers and special characters.
- Passwords must not be comprised of an obvious keyboard sequence (i.e. QWERTY).
- Passwords must not include "guessable" data, such as personal information like birthdays, addresses, library public information, phone numbers, locations, etc.

GP8. Privileged account passwords must be changed at least every year.

- The exception is the Task Administrator password, which should not be available except to Network Management.

- If any network device password is suspected to have been compromised, all network device passwords must be changed promptly.
- If any employee leaves the library, all passwords to which they could have had access must be changed promptly. This statement also applies to any consultant or contractor who has access to administrative passwords.

GP9. Use of network hardware or software such as traffic monitors/recorders and routers shall be restricted to network management or a designated local administrator.

GP10. Disposal of IT assets, such as network servers and routers, shall be done in compliance with City of Shenandoah guidelines for disposal of City property. Electronic media, such as tapes, disk drives, etc. shall be physically destroyed. IT contractors may be selected to perform the physical destruction, providing written confirmation of completion of the task.

GP11. Security training shall be integrated into existing library training programs such as orientation programs for new employees, volunteers, or patrons in the use of computers, software, and network information resources.

GP12. Incident logs and subsequent security reports must be generated and reviewed on a regular basis.

Specific Responsibilities for Ensuring Shenandoah Public Library LAN Security:

1. Public Users

Public Users are expected to be knowledgeable about and adhere to the Library's Computer and Internet Use Policy. Users are ultimately responsible for their own behavior. User responsibilities include:

PU1. Understanding and respecting relevant Federal and State laws, Shenandoah Public Library policies and procedures, and other applicable security procedures and practices established for the Shenandoah Public Library network.

PU2. Using network resources in accordance with terms specified in the Library's Computer and Internet Use Policy, and being aware of activities disallowed and the consequences of engaging in such unauthorized use.

PU3. Being aware of privacy issues related to their use of network resources and protecting the confidentiality and integrity of their own information.

PU4. Notifying a staff member if a security violation or breach is observed or detected.

PU5. Reporting any signs of abnormal or suspicious activity to library staff.

Specific Responsibilities for Ensuring Shenandoah Public Library LAN Security:

2. Staff Users

Staff Users are expected to be knowledgeable about and adhere to the Library's Network Security Policy and Computer and Internet Use Policy. Users are ultimately responsible for their own behavior. User responsibilities include:

SU1. Adhering to guidelines set forth for Public Users (PU1-PU4).

SU2. Selecting and maintaining strong passwords as outlined in the Library's password policy. Specifically, users must not disclose passwords to others.

SU3. Notifying a local administrator when security procedures are not followed-for example, when a previous user leaves a workstation without logging off or when passwords are written and left in open view.

SU4. Notifying a local administrator or network management if a security violation or breach is observed or detected.

SU5. Being familiar with how malicious or virus-infected software is distributed and observing practice that minimizes the risk of damage due to the introduction of such software.

SU6. Reporting any signs of abnormal or suspicious activity to the Teen & Technology Librarian.

SU7. Ensuring that his/her workstation is left on as scheduled so the hard drive may be backed and virus checks run, according to Library procedure.

Specific Responsibilities for Ensuring Shenandoah Public Library LAN Security:

3. Library Managers

Library managers, with guidance or direction from the City of Shenandoah, are responsible for developing and implementing effective security policy. They are ultimately responsible for ensuring that the objectives of library policy and individual responsibilities are clearly communicated to staff and end users and adequately followed. Specific responsibilities of library managers include:

LM1. Effectively analyzing potential security risks in order to formulate an appropriate security policy. This risk management requires:

- identifying the assets to be protected
- assessing potential vulnerabilities
- analyzing the risk of exploitation
- implementing cost-effective safeguards

LM2. Providing training, or at least written training materials, to all staff, volunteers, and patrons in the appropriate use of the network, awareness of the possible effects of misuse or unauthorized use of network resources, and the consequences of any unauthorized use.

LM3. Ensuring staff and patrons understand the danger of malicious software, how it is generally spread, and the technical controls used protect against it.

LM4. Informing local administrators and network management of the change in status of staff or contract workers who utilize the Shenandoah Public Library network. This could include a position change (providing greater or more restricted access privileges) or termination of library employment.

Specific Responsibilities for Ensuring Shenandoah Public Library LAN Security:

4. Network Managers

Network management includes the Technology & Teen Librarian, the Library Director or contracted support and is expected to implement and maintain security measures enforcing local security policies, to archive critical programs and data, and to control access and protect physical network facilities. Specifically, network management is responsible for:

NM1. Rigorously applying available security measures enforcing local security policies.

NM2. Developing procedures that promote security in daily operations.

NM3. Advising library management on the effectiveness of the existing policies and technical considerations that may lead to improved practices.

NM4. Responsible for securing the local network and its borders with outside networks.

NM5. Responsible for responding to security breaches or violations in a timely and effective manner.

> NM5.1. Notify local administrators if a break-in is in progress and assist other local administrators in responding to security violations.
>
> NM5.2. Cooperate with local administrators in tracking/monitoring violators and assist in enforcement efforts.

NM6. Configuring audit logs and using network monitoring tools to aid in the detection of security violations.

NM7. Conducting timely audits of network server logs.

NM8. Remaining informed on outside policies and recommended practices and, when appropriate, informing library management of new developments.

NM9. Exercising the powers and privileges inherent in network administration with caution and discretion.

NM10. Identifying, recommending, installing, and configuring software providing:

- intrusion detection
- monitoring of unauthorized activity
- removal of malicious software

NM11. Developing procedures that allow users and local administrators to report security violations, and notifying library management and possibly outside agencies of any threats.

NM12. Promptly notifying designated personnel of all computer security incidents.

NM13. Providing assistance in tracking the source of malicious software or computer viruses and determining the extent of contamination.

NM14. Removing malicious software or viruses.

NM15. Conducting periodic audits to ensure proper security practices are followed.

NM16. Performing security testing/audit of the network every 3 years.

NM17. Maintaining user privacy.

NM18. Overseeing the update of anti-virus signatures on all local workstations and servers and for scanning server hard drives regularly.

NM19. Maintaining network documentation, including the Network Diagram, list of IP addresses, firewall rule set, Access Control List, and Computer/Electronics Inventory.

Specific Responsibilities for Ensuring Shenandoah Public Library LAN Security:

5. Local Administrators

Local administrators are staff who assist in the daily maintenance of security services and who support and enforce applicable security policies and procedures. Specifically, local administrators are responsible for:

LA1. Managing all users' access privileges to data and programs.

LA2. Monitoring security-related events and following up on any actual or suspected violations, where appropriate; notifying network management of reported security incidents and assisting in investigating them.

LA3. Maintaining and protecting server software, relevant files, and media using specified security mechanisms and procedures.

LA4. Notifying network management of any pending updates required.

LA5. Leaving workstations on and unlocked to receive critical updates per library procedure.

LA6. Promptly notifying network management and library management of all computer security incidents;

> LA6.1. Notify the network management if a break-in is in progress; assist other local administrators in responding to security violations.
>
> LA6.2. Cooperate with network management in tracking violators and assisting in enforcement efforts.

Sources: The Texas State Library and Archives Commission (https://www.tsl.texas.gov/ld/pubs/compsecurity/ptthreesecpol.html) and Mark Brophy (https://www.iltanet.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=65dfd8dc-8920-4d58-bbe2-843bfb88eba0&forceDialog=0&ssopc=1)