NOLS
NORTH OLYMPIC
LIBRARY
SYSTEM

Policy 5.3
Computer Security

Adopted by the Library Board of Trustees: 06/25/2015

The North Olympic Library System's (NOLS') local area networks are critical to the provision of information services to NOLS staff and customers. NOLS' Integrated Library System (ILS) processes sensitive and valuable information. Stringent safeguards of network use and resources are necessary to protect the confidentiality of transactions being processed on NOLS' networks, and to keep critical systems operational.

1. **Purpose.** This policy defines operational practices, and assigns specific responsibilities required to secure networked information resources.

   This policy covers all electronic information resources in the library. It applies equally to hardwired and wireless networks, network servers, staff and public workstations, network equipment, telecommunications equipment, and peripherals, such as printers and scanners, within the library. This policy applies to all who utilize, manage, or administer library computers or networks in any way, including library customers, library staff, vendors and contractors.

2. **Security Program.** NOLS' security program is designed to ensure the availability of networked resources, and the integrity and confidentiality of data transmitted over and stored on the networks. Specifically the goals of the program include:

   A. Ensuring library networks have sufficient security measures applied to protect the integrity of their data, the privacy of information transactions, and the availability of their resources;

   B. Ensuring the cost of security measures implemented is commensurate with the risks present on the networks;

   C. Ensuring appropriate budgetary and technical network support is available and maintained;

   D. 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;

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

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

   G. Ensuring that all applicable organizational policies and procedures are applied and practiced; and

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

3. **General Responsibility for Network Security.** Responsibility for implementing and maintaining the Library's network security goals is divided among four identified groups.

   A. **Library Management -** the Library Board of Trustees, Director, and Management Team, who have functional responsibility for the library. Library management is responsible for informing staff about this policy, assuring that each person has access to it,, and interacting with staff, volunteers and customers regarding security issues.

   B. **Network Administrators** – IT staff and contractors involved in the technical support, management, and operation of NOLS networks. Network management must ensure the continued operation of all networks and is responsible for implementing appropriate network security measures as indicated in this security policy.

   C. **Site Facilitators -** library staff responsible for ensuring that end users have access to needed network resources available through the library's servers and internet access. Site Facilitators provide day-to-day maintenance of network security in accordance with this security policy. Site Facilitators are responsible for reporting observed breaches of security policy to network and library management.

   D. **End Users -** library staff, volunteers, and library customers who have access to NOLS networks. End users are required to use the network resources responsibly in accordance with the provisions of this security policy and Policies *4.4: Public Computing* and *4.5: Public Use of the Internet*. All users of data and network services, including the internet, are responsible for complying with security protocols established by NOLS, and for reporting to library and network management any actual or suspected breach of security.

4. **Access to physical facilities.** Access to the server room, server closets, and other secure areas housing information systems and networking infrastructure is restricted to authorized personnel only and requires authorization by the IT Manager or Library Director. Visitors to these restricted areas, including contractors, service vendors, utilities staff and others must be authorized by the Library Director or IT Manager and escorted at all times. Logs of visitor access will be maintained.

5. **Established security standards.**

   A. All NOLS workstations, regardless of whether they are on the staff, public or wireless networks, must be configured with NOLS settings and applications. All workstations will receive regular security patch updates in accordance with established practices.

   B. Obsolete computer equipment will be disposed of according to NOLS Policy *5.9: Surplus Materials*. Prior to disposal, hard drives will be destroyed.

C. If end users fail to comply with this policy, NOLS information, while stored, processed or transmitted on NOLS networks, 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 the Library Director for action. Violations by any end user may result in termination of rights to use any NOLS network. In the case of NOLS employees, violation may also result in disciplinary action up to and including termination of employment.

D. Staff who manage workstations and/or servers shall be trained so they can follow all policies and procedures effectively.

E. 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.

F. Server security shall be exclusively controlled by network management. Access to server security mechanisms by all other staff, volunteers, or public users shall be considered unauthorized access.

G. For network security and to ensure that service remains available to all library users, NOLS electronically monitors network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage. Anyone using the NOLS website expressly consents to such monitoring. Except for the above purposes, or if required by law, no other attempts are made to identify library users or their internet activity.

H. Each staff member, volunteer, and contract worker will be assigned a unique User ID and initial password according to established procedure. Public users will use unique or generic User IDs and passwords to gain access to network resources. Users must not share or disclose unique User IDs and passwords. All users must be authenticated to the network before accessing network resources.

I. The State of Washington’s Records Retention Schedule shall govern the storage of data on NOLS networks.

J. Incident logs and subsequent security reports will be generated and reviewed by Library and Network Management on a regular basis.

6. Specific Responsibilities for Ensuring Network Security.

A. **Responsibilities of End Users** (staff, volunteers and public). Users are expected to be knowledgeable about and adhere to the Library's security and acceptable use policies. Users are ultimately responsible for their own behavior. Specific User responsibilities include:

a) Understanding and respecting relevant federal and state laws, NOLS policies and procedures, and other applicable security procedures and practices established for NOLS' networks.

b) Using network resources in accordance with Library policies, and being aware of prohibited activities and the consequences of engaging in such unauthorized use. Applicable policies include, but are not limited to: Policy 4.1: Basic Rule of Conduct, 4.4: Public Computing, 4.5: Internet Policy; and in the case of NOLS employees, also HR 8.1:Code of Employee Conduct, HR 8.5: Limits to Personal Business Conducted on Duty, HR8.6: Professional Ethics, and HR 8,.11: Computer Security Awareness and Acceptable Use

c) Being aware of privacy issues related to the use of network resources, such as knowledge of passwords, confidential credentials and/or information about network infrastructure, and protecting the confidentiality and integrity of such information.

d) Selecting and maintaining strong passwords as outlined in the Library's password guidelines. Users must not disclose unique User IDs or passwords to others. NOLS' guidelines regarding creation, communication, and documentation of passwords must be followed at all times.

e) Notifying site management when security procedures are not followed, for example, when a previous user leaves a workstation without logging off or when passwords are written down and left in open view.

f) Notifying network management if a security violation or breach is observed or detected.

g) Being familiar with how malicious or virus-infected software is distributed and following practices that minimize the risk of damage due to the introduction of such software.

h) Reporting any signs of abnormal or suspicious activity to an appropriate Library staff member; Library staff should report to their Library Manager and/or IT staff.

i) Refraining from install hubs, wireless access points, terminal services, or other equipment that extends the network or accessing, altering, removing, connecting to, or otherwise tampering with any equipment managed by NOLS in any manner other than those authorized.

j) Insuring that computers are secured, when not in use, according to established rules and guidelines.

k) For staff only: Ensuring that one's workstation is left on as scheduled so system updates, backups and maintenance can occur, according to NOLS practice.

B. **Responsibilities of Library Management.** Library managers, with guidance or direction from NOLS' IT Manager and the Library Director, are responsible for developing and implementing this policy and other security policies and practices. They are ultimately responsible for ensuring that the importance of computer security and individual responsibilities for computer security are clearly communicated to staff and end users, and are adequately followed. Specific responsibilities of library managers include:

a) Effectively analyzing potential security risks to formulate appropriate security policies and practices. This risk management requires identification of the assets to be protected, assessment of potential vulnerabilities, analysis of the risk of exploitation; and the implementation of cost-effective safeguards.

b) 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.

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

d) Informing Network Management of the change in status of staff, volunteers, contract workers and any others who have unique User IDs who use NOLS networks. This could include a position change (providing greater or more restricted access privileges) or termination of library employment.

C. **Responsibilities of Network Administration.** Network management is mainly handled by NOLS staff but contracted support is also involved. NOLS staff and contractors are expected to implement and maintain security measures enforcing NOLS security policies and practices, to archive critical programs and data, and to control access and protect physical network facilities. Specifically, Network Administration is responsible for:

a) Rigorously applying available security measures enforcing local security policies and practices;

b) Advising library management on the effectiveness of existing policies and technical considerations that may lead to improved practices;

c) Assigning a unique User ID and initial password to new users according to established procedures;

d) Securing local networks and their borders with outside networks;

e) Ensuring that all software installed on servers and workstations is approved for use and is licensed properly;

f) Installing all new software and software updates and backing up server and workstation drives;

g) Responding to security breaches or violations in a timely and effective manner;

h) Notifying Library Management if a break-in is in progress and assisting site facilitators in responding to security violations;

i) Cooperating with site facilitators in tracking/monitoring violators and assisting in enforcement efforts;

j) Configuring audit logs and using network monitoring tools to aid in the detection of security violations;

k) Conducting timely audits of network server logs;

l) Remaining informed of model policies and best practices and, when appropriate, recommending changes to library management;

m) Exercising the powers and privileges inherent in network administration with caution and discretion;

n) Protecting all network access points with a firewall and intrusion prevention system that monitors and controls communications;

o) Preventing traffic matching specific reconnaissance, intrusion or virus patterns from entering or exiting the network;

p) Managing and monitoring all boundary protection systems;

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

r) Identifying, recommending, installing, and configuring software providing: intrusion detection, monitoring of unauthorized activity and removal of malicious software;

s) Developing procedures that allow users and local administrators to report security violations, and notifying library management and, if applicable, outside agencies of any threats;

t) Promptly notifying designated personnel of all computer security incidents;

u) Providing assistance in tracking the source of malicious software or computer viruses and determining the extent of contamination;

v) Promptly quarantining and/or removing malicious software or viruses;

w) Conducting periodic audits to ensure proper security practices are followed; and

x) Maintaining user privacy.

D. **Responsibilities of Site Facilitators.** The Site Facilitator group consists of staff or volunteers who assist in the daily maintenance of security services and who support and enforce applicable security policies and practices. Specifically, site management is responsible for:

a) Managing all users' access privileges to data and programs;

b) 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;

c) Maintaining and protecting server software, relevant files, and media using specified security mechanisms and procedures;

d) Promptly notifying network management and library management of all computer security incidents;

e) Notifying network management if a break-in is in progress; assisting other site facilitators in responding to security violations;

f) Cooperate with network management in tracking violators and assisting in enforcement efforts; and

g) Backing up all data on network servers and workstations according to established schedule and procedure;

7. Exceptions to this policy. Any requests for exceptions must be submitted in writing and in advance to the IT Manager for approval. The IT Manager will retain documentation of currently permitted exceptions and will review them on an annual basis.