STATEMENT OF POLICY AND PROCEDURE
Section: 1:3X.1 | Chapter: | Page(s): 6
Subject: INFORMATION TECHNOLOGY – MEMBER LIBRARIES |
Reviewed: NEW | Revised: NEW | **Effective:2024/09/11**

Part 1 – Interpretation and Application

Definitions

1. In this policy, any word or expression mentioned hereinafter has its statutory meaning unless otherwise specified, and:
    a. **"NLLS"** refers to the Northern Lights Library System and its staff.
    b. **"Endpoint"** refers to any technology capable of connecting to the internet, including, but not limited to: computers, tablets, phones, printers, and self-checkout machines.
        - **"Approved Endpoint"** refers to any endpoint approved for use on an NLLS network by NLLS.
        - **"Unapproved Endpoint"** refers to any endpoint not approved for use on an NLLS network by NLLS.
    c. **"External Party"** refers to any group or individual without a formal staff or volunteer arrangement with a Member Library or NLLS.
    d. **"Member Library"** refers to a library or service point served by NLLS and/or one or more staff members who are employed by, or volunteer at, a Member Library and acting under its representation.
    e. **"Network Equipment"** refers to any piece of technology that is used to create and/or facilitate an internet-based network, including, but not limited to, firewalls, switches, and wireless AP units.
    f. **"Staff Member"** refers to any individual formally employed by or volunteering at a Member Library, such as board members.

Part 2 – Policy Compliance

Exceptions

2. Any exception to this policy must be authorized in writing by NLLS prior to any action being taken on behalf of the Member Library or NLLS staff.

Non-Compliance

3. Failure to follow this policy without prior exception may result in the immediate and unannounced partial or full revocation of the Member Library's access to technology-based services. In such situations, NLLS will notify the Member Library of the revocation and provide reasonable steps for the Member Library to regain access to services.
4. If a cybersecurity incident is directly attributable to the proven and continued non-compliant actions of a Member Library, the library may be held liable for recovery and/or reconstruction efforts.

Part 3 – User Account Management

Login Credentials

5. The sharing of assigned desktop and/or Polaris login credentials with another staff member and/or external parties is strictly prohibited.

Desktop Login Credentials

6. All staff members accessing an endpoint on the Staff Network must access the endpoint through a desktop login credential assigned by NLLS that accurately identifies the staff member through a combination of first, middle, and/or last names.

Polaris Login Credentials

7. All staff members accessing Polaris must access the application through a login credential assigned by NLLS that accurately identifies the staff member through a combination of first, middle, and/or last names, in addition to the Member Library in which they are primarily employed and/or volunteer.

Departure of a Staff Member

8. If a staff member departs a library under any circumstances, including, but not limited to, resignation, retirement, or termination, NLLS must be notified of the date and end time of the staff member's last shift prior to, when possible, its occurrence so that access to the account may be appropriately restricted.
9. Member Libraries may keep the accounts of former staff members active for reasons of business continuity. In these cases, the password must be changed to a password other than that used by the staff member during their employment, no later than the end time of their last shift.
10. NLLS will delete all accounts of former staff members 365 days after their last working day or upon request by the Library Manager or Director, whichever occurs sooner.

Part 4 – Acceptable Use

Internet Usage

Internet Browsing and Content Filtering

11. NLLS will not apply content filters to the internet connection at Member Libraries, either by its own accord or at the request of a Member Library.
12. Staff members must follow safe browsing practices when accessing the internet, including, but not limited to, only visiting trusted websites and avoiding potentially dangerous websites such as those classified as 'dark web'.
13. It is the responsibility of the Member Library to ensure that staff members are not accessing content that can be reasonably believed to have a likelihood of compromising the network.

Downloads from the internet

14. All endpoints operating on an NLLS network (with the exception of the BYOD Wireless Network and the Public Wireless Network) must operate software provided by NLLS that restricts the download of files commonly associated with a high level of risk to the organization's cybersecurity.
15. Staff members must follow safe downloading practices when downloading files from the internet, including, but not limited to, only downloading files from trusted websites.

16. Under no circumstances are staff members permitted to download files or programs obtained illegally or that infringe copyright.

Endpoint Usage

17. NLLS will not impose restrictions on the usage of endpoints for staff members over and above what is already stated in this policy.

Usage by External Parties

18. The Member Library is responsible for ensuring that external parties utilizing an endpoint connected to an NLLS network employ safe browsing practices.
19. It is strongly recommended that external parties not be given access to an endpoint connected to the Staff Network or Staff Wireless Network. If this is required, external parties must be actively monitored by a staff member when utilizing the endpoint.
20. Under no circumstances are any personal devices belonging to external parties permitted to connect to an NLLS network other than wirelessly through the Public Wireless Network.
21. Under no circumstances are any personal devices belonging to external parties permitted to connect to a printer operating on an NLLS network, other than wirelessly.

Usage of the Public Network and Public Wireless Network

22. NLLS will not impose content, usage, or download restrictions on devices connected to the Public Network beyond those mentioned in this policy.
23. Users must agree to the *NLLS Public Wireless Hotspot Connection Conditions and Terms of Agreement* before connecting to the Public Wireless Network.
24. The Member Library is responsible for enforcing the *NLLS Public Wireless Network Hotspot Connection Conditions and Terms of Agreement* for users accessing the Public Wireless Network in the library.
25. If a Member Library has a concern about a user's activity while using an endpoint connected to the Public Network, it is the responsibility of the Member Library to report this concern to NLLS.

Connection of Personal Devices to the Network

26. Member Library staff members are not permitted to connect personal devices to an NLLS network other than the BYOD Wireless Network or the Public Wireless Network.

Part 5 – Password and Access Management

27. Password management is a critical component of ensuring the cybersecurity of NLLS and its Member Libraries. Poor password management practices increase the organization's vulnerability to malicious cyber activity which poses significant risk of lost personal and/or business data. To protect against this, all staff members must:
    a. Change temporary passwords provided to them by NLLS upon first login.
    b. Use a unique password for every application. The reuse of passwords is strictly prohibited.
    c. Employ complex passwords and follow the recommendations of the entity requiring login credentials. If password recommendations are not provided, employees must create a complex password no fewer than 14 characters, inclusive of at least one number and one special character. Passwords must also not include any words or terms associated with the Member Library or the workplace, such as the library name or digits of a workplace phone number.
    d. Not divulge passwords to external parties.

e. Ensure that passwords are securely stored in a password management application. The digital storage of passwords in unsecured documents and the physical storage of passwords outside of locked places, such as locked rooms or cabinets, is strictly prohibited.

Part 6 – Network Access and Configuration

Network Configuration

28. NLLS administers two separate networks for each Member Library: the Staff Network and the Public Network. Both networks serve a distinct purpose and carry their own policies and procedures regarding access.
29. In unique situations, NLLS may set up an additional network at a Member Library that will carry its own set of unique policies and procedures.
30. Member libraries are not permitted to connect network equipment to any NLLS network without the express permission of NLLS.

Staff Network Access

31. The Staff Network is reserved for the use of Approved Endpoints requiring a hardwired internet connection that are to be used exclusively by staff members.
32. If an endpoint is required to connect to the Staff Network, NLLS must be contacted before connection.
33. NLLS maintains the right to refuse to allow an endpoint to connect to the Staff Network if it is reasonably believed to have a likelihood of compromising the network or degrading network performance. Due to this, it is recommended that Member Libraries contact NLLS staff before purchasing new endpoints.
34. It is not permitted to connect computers that do not operate on the NL.ORG domain to the Staff Network without the express permission of NLLS. This includes computers owned by the Member Library that do not yet operate on NL.ORG, such as public access computers.
35. If an Unapproved Endpoint is found to be connected to the Staff Network, NLLS will remotely revoke the endpoint's access to the network until the Member Library obtains approval for the endpoint from NLLS.

Public Network Access

36. The Public Network is reserved for the use of Approved Endpoints requiring a hardwired internet connection to facilitate the offering of public access computers to external parties.
37. If an endpoint is required to connect to the Public Network, NLLS must be contacted before connection.
38. NLLS maintains the right to refuse to allow the connection of an endpoint to the Public Network if it is reasonably believed to have a likelihood of compromising the network or degrading network performance. Due to this, it is recommended that Member Libraries contact NLLS staff before purchasing new endpoints.
39. If an Unapproved Endpoint is found to be connected to the Public Network, NLLS will remotely revoke the endpoint's access to the network until the Member Library obtains approval for the endpoint from NLLS.
40. Personal computers belonging to staff members and external parties are not permitted to connect to the Public Network, including via a network-connected printer. These endpoints are only permitted to connect to the Public Network via the Public Wireless Network or the BYOD Wireless Network for staff members.

41. Member Libraries are not permitted Administrator access to endpoints connected to the Public Network.

Part 7 – Wireless Network Access and Configuration

Wireless Network Configuration

42. NLLS administers three separate wireless networks for each Member Library: the Staff Wireless Network, the BYOD Wireless Network, and the Public Wireless Network. Each wireless network serves a distinct purpose and has its own set of policies and procedures regarding access.
43. In unique situations, NLLS may set up an additional wireless network at a Member Library that will carry unique policies and procedures.

Staff Wireless Network

44. The Staff Wireless Network ("Library Staff") is reserved for using Approved Endpoints requiring a wireless connection.
45. If an Unapproved Endpoint is found to be connected to the Staff Wireless Network, NLLS will remotely revoke the endpoint's access to the network until the Member Library obtains approval for the endpoint.
46. If an endpoint is acquired that must connect to the Staff Wireless Network to function, such as a traffic counting device or security cameras, NLLS staff must be contacted before connection to build the appropriate isolated network lock-out.
47. NLLS maintains the right to refuse to permit an endpoint to connect to the Staff Wireless Network if it is reasonably believed to have a likelihood of compromising or degrading network performance. Due to this, it is recommended that Member Libraries contact NLLS staff before purchasing new technologies.
48. Divulging the Staff Wireless Network password to external parties is strictly prohibited.

BYOD Wireless Network

49. Staff members may bring their personal endpoints to work and connect to the BYOD Wireless Network ("Library BYOD").
50. Divulging the BYOD Wireless Network password to external parties is strictly prohibited.

Public Wireless Network

51. The Public Wireless Network ("Library Wireless") is reserved for external parties to use via their own endpoints or through unsupervised use of Approved Endpoints, including public access computers.

Part 8 – Stewardship of Network Devices

52. All network equipment found at a Member Library is the property of NLLS and provided on loan to Member Libraries to facilitate a network connection.
53. All network equipment must be physically secured in a locked space approved by NLLS.
54. NLLS must be provided access to network equipment upon request and within a reasonable timeframe in consideration of a Member Library's opening hours.
55. Staff members are not permitted to unplug, move, or otherwise interact with network devices at the Member Library without prior approval from NLLS.
56. Member Libraries must not permit any external party from unplugging, moving, or otherwise interacting with network devices at the Member Library without prior approval from NLLS.

57. Member Libraries are responsible for maintaining the network capabilities of their building and/or space to the minimum standard of being able to support modern network equipment, including, but not limited to, ensuring network cabling is of a current recommended specification.

Part 9 – Endpoints

Minimum Computer Configuration

58. All computers must be provided to NLLS to configure to the following minimum configuration before being permitted to connect to an NLLS network:
    a. Each computer is required to have the following applications installed:
        - Endpoint Detection and Response (EDR) software
        - Remote support software
        - Software capable of automatically updating and patching other software
    b. All computers connected to the Staff Network must operate on NL.ORG
    c. All computers connected to the Public Network must utilize software to wipe the user's data at the end of each session.
    d. All computers must operate a modern operating system specified by NLLS.
59. If a computer cannot meet the minimum computer configuration, it will not be permitted to connect to an NLLS network.

Part 10 – Data Backups

60. NLLS will back up the Outlook and OneDrive data of Library Managers and Library Directors at Member Libraries via off-site backups without charge to the Member Library.
61. Upon request from a Member Library, NLLS will backup staff members' Outlook and OneDrive data at cost.
62. Data integrity during and/or after a cybersecurity incident is not guaranteed.

Part 11 – Cybersecurity Incidents

63. In the case of a cybersecurity incident – either speculated or confirmed – NLLS will take all measures necessary to isolate the cause, reduce the spread, and protect our digital assets, up to and including assuming immediate and unannounced absolute control of the network at each Member Library and each endpoint connected to it without concern for data preservation.

NLLS Executive Board Chair

September 11, 2024

Date of Approval