STATEMENT OF POLICY AND PROCEDURE

Section: 1:3X | Chapter: | Page(s): 3

Subject: INFORMATION TECHNOLOGY – NLLS Head Quarters |

Reviewed: NEW | Revised: NEW | **Effective: 2024/09/11**

Part 1 – Interpretation and Application

Definitions

26. 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.
    c. **“External Party”** refers to any group or individual without a formal staff or volunteer arrangement 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 NLLS, such as individuals with an employment contract and board members.

Part 2 – Policy Compliance

Exceptions

27. Any exception to this policy must be authorized in writing by NLLS prior to any action being taken on behalf of a staff member.

Non-Compliance

28. Failure to follow this policy without prior exception may result in disciplinary action, up to and including, termination of the staff member.

Part 3 – User Account Management

Login Credentials

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

Desktop Login Credentials

30. 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

31. 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.

Remote Access

32. All staff members remoting into an NLLS managed endpoint must do so exclusively through tools provided by NLLS. A login credential assigned by NLLS that accurately identifies the staff member through a combination of first, middle, and/or last names must be used, along with multifactor authentication.
33. Under no circumstances are staff members permitted to remote into an NLLS endpoint on an unrestricted wireless network such as those offered by airports and hotels.

Departure of a Staff Member

34. Upon a staff member's departure from NLLS for any reason (resignation, retirement, or termination), their account will be restricted by the end of their final shift to prevent access to NLLS systems.
35. For business continuity, NLLS may keep former staff members' accounts active but must change the password by the end of their last shift.
36. NLLS will delete former staff members' accounts 365 days after their last working day or upon the Executive Director's request, whichever comes first.

Part 4 – Acceptable Use

Internet Usage

Internet Browsing and Content Filtering

37. 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 the 'dark web.'

Downloads from the internet

38. All endpoints operating on an NLLS network (except the BYOD Wireless Network and the Public Wireless Network) will operate software that restricts the download of files commonly associated with a high level of risk to the organization's cybersecurity.
39. Staff members must follow safe downloading practices when downloading files from the internet, including, but not limited to, only downloading files from trusted websites.
40. Under no circumstances are staff members permitted to download files or programs obtained illegally or that infringe copyright.

Endpoint Usage

41. NLLS will not impose additional restrictions on staff members' use of endpoints beyond those already stated in this policy.
42. NLLS does not restrict staff members from using their assigned devices for personal uses outside of work hours, provided that the use does not violate any portion of this policy or jeopardize the security of NLLS, its devices, and its network.

Usage by External Parties

43. 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.
44. 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.

Part 5 – Password and Access Management

20. Password management is critical to ensuring the cybersecurity of the Northern Lights Library System (NLLS) and the smooth operation of system services. Poor password management practices increase the organization's vulnerability to malicious cyber activity and pose significant risks of losing personal and business data.
21. **Use of NLLS Password Management Software**
    - Employees must use the password management software provided by NLLS to store and appropriately distribute passwords securely.
22. **Storage of Passwords**
    - Employees must store and access all business-related passwords using the provided software.
    - Digital storage of passwords using alternative tools or external storage devices is prohibited.
    - Physical storage of passwords, such as written notes, is also prohibited.
23. **Password Sharing Restrictions**
    - Passwords must not be shared with unauthorized individuals under any circumstances to maintain cybersecurity and system integrity.
    - Passwords must not be shared via unsecured platforms such as handwritten notes, email, text messages, or other instant messaging services.
24. **Recovery Tool Management**
    - Physical password recovery tools must be stored in secure, locked storage managed by NLLS.
25. **Password Complexity Requirements**
    - Where a service requiring a password does not have minimum password complexity, passwords must include at least the following:
        - twelve characters,
        - one number and one special character,
        - and be unique and do not contain any words or terms associated with the workplace (e.g., NLLS, Elk Point, company contact information).

Part 6 – Data Backups

26. NLLS will back up staff members' Outlook and OneDrive data via off-site backups.
27. Data integrity during and/or after a cybersecurity incident is not guaranteed.

Part 7 – Cybersecurity Incidents

28. 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 and each endpoint connected to it without concern for data preservation.

NLLS Executive Board Chair

Date of Approval