Northern Light Health

Title: Internet Access and Use	
Policy/Procedure #: 22-030	**Date Posted: 02/04/2026**
Initial Effective Date: Earliest Confirmed Date, 11/2007	Date Last Revised: 02/04/2026
Author: Kurt Anderson, Chief Information Security Officer	
Executive Sponsor: SVP & Regional President – IT Executive Sponsor	Final Approver: SVP & Regional President- IT Executive Sponsor
Supersedes: 22-030	Dated: 02/27/2025

APPLICABILITY

☒ Northern Light Health adopts the following (and any Attachment(s)) for all its Member Organizations, specifically including, but not limited to, those listed below:

☐ Northern Light Health adopts the following (and any Attachment(s)) for its Member Organizations selected below:

- ☐ Northern Light Acadia Healthcare
- ☐ Northern Light Acadia Hospital
- ☐ Northern Light AR Gould Hospital
- ☐ Northern Light Blue Hill Hospital
- ☐ Northern Light CA Dean Hospital
- ☐ Northern Light Eastern Maine Medical Center
- ☐ Northern Light Health Foundation
- ☐ Northern Light Health Home Office
- ☐ Northern Light Home Care & Hospice
- ☐ Northern Light Maine Coast Hospital
- ☐ Northern Light Mayo Hospital
- ☐ Northern Light Medical Transport
- ☐ Northern Light Mercy Hospital
- ☐ Northern Light Pharmacy
- ☐ Northern Light Sebasticook Valley Hospital
- ☐ Work Health
- ☐ Other (list): _____

SCOPE

This Policy applies to all Users of Northern Light Health information systems.

RELATED POLICIES/PROCEDURES

System Policy 22-004, Information Systems Acceptable Use
System Policy 22-009, Email Encryption
System Policy 22-017, Northern Light Health Computer Information Security Standards
System Policy 22-020, eMail and Electronic Communication Systems
System Policy 23-105, Patient Access to Own Health Information
System Policy 23-118, Information Classification

DEFINITIONS

Confidential: Information that is classified as Confidential as determined by System Policy 23-118, Information Classification.

Users: The person for whom a hardware or software solution has been designed and created to carry out job related functions.

PURPOSE

To provide guidance for the appropriate use of the Internet by Northern Light Health Users.

POLICY

In order to protect Northern Light Health's internal network (Intranet) from the risks of the Internet, all connections to the Internet from Northern Light Health and Member Organizations computers must be properly screened, managed and maintained.

Northern Light Health Information Security places a high priority on addressing security risks to Northern Light Health and Member Organization information systems. Protecting our information systems maintains the confidence of our patients and the communities we serve. For this reason, the specifics of security problems should not be discussed widely, but should instead be shared on a need-to-know basis within Northern Light Health and its Member Organizations.

PROCEDURE

1. Information Movement

    a. If Users need to download nonstandard software for legitimate business use, they may contact the Northern Light Health Help Desk at 1-888-827-7728 or 973-7728.

    b. Users may not place information belonging to Northern Light Health or any Member Organization in consumer file sharing services outside of the Northern Light Health network without the prior approval of the Northern Light Health Compliance Department.

    c. Users are prohibited from being involved in any way with exchanging, accessing or downloading material that is inconsistent with Northern Light Health or Member Organization business use or incidental personal use or otherwise prohibited under System Policy 22-004, Information Systems Acceptable Use.

    d. Users may not email Confidential information or information for Northern Light Health/Member Organization official use to a personal Internet address unless (1) a patient directs that their PHI be emailed in this manner, and such request is made and documented according to System Policy 23-105, Patient Access to Own Health Information; or (2) such activity has been approved by the User's manager, Privacy Officer and the Northern Light Health Chief Information Security Officer and appropriate protections are in place for that information.

e. Emails containing Confidential information must be encrypted according to System Policy 22-009, Email Encryption.

f. The use of Northern Light Health and Member Organization information systems to participate in activities meant to circumvent software licenses, including but not limited to, the pirating of software is prohibited.

2. No Expectation of Privacy

a. Northern Light Health Information Security uses software that filters and logs all Internet activity.

b. Filtering of permitted sites that may pose a risk to the organization will be vetted by the Enterprise Risk Management Council.
   (1) Users may recommend appropriate web sites to their management for approval and inclusion on the "permitted list."
   (2) Northern Light Health Information Security may provide usage reports and User destinations on the Internet to the User's manager at any point.
   (3) Manager requests for usage activity reports must be directed to and approved by Human Resources before being sent to Northern Light Health Information Security.
   (4) In the event material in violation of Section 1 of this Policy is accessed, reports will be provided to the appropriate manager(s) for review.

3. Access Control

a. All Users wishing to establish a network based connection to Northern Light Health or a Member Organization must log in with a Northern Light Health supplied unique user ID and password before gaining access to the private internal network.

b. Users may not establish Internet or other external network connections that could allow non-Northern Light Health users to gain access to Northern Light Health or Member Organization systems and information. These connections include the establishment of VPN connections other than those designated by Northern Light Health Infrastructure and Northern Light Health Information Security.

c. Users are prohibited from using a Northern Light Health or Member Organization Internet connection to establish personal business channels. Prohibited examples include electronic data interchange (EDI) arrangements, setting up or promoting personal business ventures, on-line database services, etc.

d. Users must not "test the doors" or probe security mechanisms at either Northern Light Health/Member Organization Intranet sites or other Internet sites.

4. Reporting Security Problems

    a. Users must immediately notify the Northern Light Health Help Desk at 1-888-827-7728 or 973-7728 of any potential IS security concerns. The Northern Light Health Help Desk must immediately notify the Information Security Team if any of the following events occur:

        (1) Confidential information belonging to Northern Light Health or a Member Organization is lost or accessed by unauthorized parties, or is suspected of being lost or accessed by unauthorized parties;
        (2) Any actual or suspected unauthorized use of Northern Light Health/Member Organization information systems;
        (3) Passwords or other system access control mechanisms are lost, stolen, or inappropriately disclosed, or are suspected of being lost, stolen, or inappropriately disclosed; or
        (4) Any unusual system behavior which may indicate a malware infection.

5. Exceptions

    a. The Chief Information Security Officer, with the approval of the Northern Light Health VP/Chief Compliance and Internal Audit Officer, may grant exceptions to the policy for the purpose of conducting security testing and for security-related reasons.

REFERENCES
None.

ATTACHMENTS
None.

This document was approved by the committee(s) noted below on the date(s) as noted:
Leadership Council, 11/2007
Information Security Council, 4/25/2018, 11/24/2020, 10/14/2022, 7/21/2023, 05/21/2024, 2/21/2025
Compliance Committee, 10/12/2022, 7/12/2023, 5/8/2024, 2/12/2025, 1/14/2026
Compliance Task Force, 10/25/2016, 3/27/2018, 12/11/2019, 2/23/2021, 12/14/2021
IS Vice Presidents, 10/22/2019