Northern Light Health℠

Title: IS Network Connection	
Policy/Procedure #: 22-012	**Date Posted: 12/09/2025**
Initial Effective Date: Earliest Confirmed, 11/2006	Date Last Revised: 12/09/2025
Author: Christie Polley, VP & Chief Information Security Officer	
Executive Sponsor: SVP & Regional President – IT Executive Sponsor	Final Approver: SVP & Regional President – IT Executive Sponsor
Supersedes: 22-012	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 22-007, Anti-Malware Software
System Policy 22-011, Mobile Devices
System Policy 22-028, Information System Product Standards, Core Vendors and Application Rationalization

DEFINITIONS

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

PURPOSE

To provide for secure connections to the Northern Light Health network while protecting the network from malware and intrusions.

POLICY

To minimize risk to the Northern Light Health network from malware and intrusions, connections are limited to only those devices which meet minimum requirements for security. Failure to meet minimum standards will result in being disconnected from the network.

PROCEDURE

1. All hardware connecting directly to the Northern Light Health internal network is to be operated by Northern Light Health; under no circumstances are personally-owned devices to be directly connected.
   a. Approved employees will be enabled to access the "Employee Wireless Network" with personal devices.
   b. Northern Light Health devices will be made available to non-Northern Light Health Users if access to the network is needed for demonstration purposes.

2. Current requirements are outlined in Schedule I - Requirements Schedule, which may change from time to time.

3. All Users connecting to the internal Northern Light Health network are required to authenticate first using Northern Light Health provided unique User ID and password combinations.

4. Northern Light Health Hardware:
   a. No modification in connectivity will be made to a Northern Light Health device, computer, or infrastructure unless approved by Northern Light Health Information Systems staff**.**

5. Non-Northern Light Health Hardware:
   a. Vendor supplied hardware permanently placed on the Northern Light Health network must be configured to prevent both disruption of network traffic and introduction of vulnerabilities, exploits and/or malware to the Northern Light Health network as specified in the attachment to this Policy.

6. Remote Connections by non-Northern Light Health networks to the Northern Light Health network:
   a. All connections must be via a Northern Light Health approved Virtual Private Network (VPN).

b. The outside network must have in place a Northern Light Health approved firewall for VPN connection.
c. Northern Light Health reserves the right to disconnect any non-Northern Light Health connection that presents a risk to the operations of Northern Light Health.
d. All connections to the Northern Light Health network must be covered by a Business Associate Agreement or an agreement approved by Northern Light Health Senior Vice President and Chief Legal Officer.

7. Northern Light Health device standards for connection to the Northern Light Health network are subject to change, as determined by the Northern Light Health Chief Digital Officer, to reflect current industry guidelines and current security requirements for the Information Systems of Northern Light Health. The Northern Light Health Information Systems will communicate a change in standards for device connection to impacted Users as soon as is practicable following any change.

REFERENCES
None.

ATTACHMENTS
Schedule I – Requirements Schedule, linked above this Policy as a Related Document

This document was approved by the committee(s) noted below on the date(s) as noted:
Leadership Council, 11/2006, 4/14/2009
Information Security Council, 10/25/2018, 11/24/2020, 12/17/2021, 11/10/2022, 8/15/2023, 05/21/2024, 2/21/2025
Compliance Committee, 11/9/2022, 8/9/2023, 5/8/2024, 2/12/2025, 11/12/2025
Compliance Task Force, 5/24/2016, 2/28/2017, 8/28/2018, 12/11/2019, 2/23/2021, 12/14/2021
IS Vice Presidents, 10/22/2019
ERM Compliance Task Force, 9/23/2013, 9/22/2015