Objective:

The purpose of this document is to define which Network Access Control (NAC) policies will be implemented on the DHE network. The objectives of NAC are to:

- Define expected security posture of assets connecting to the DHE network
- Determine compliance to defined posture
- Enforce policy based on an asset's posture compliance by granting an asset the appropriate network access based on the asset's posture compliance

Scope:

The NAC policies are applied to all computing and mobile devices that connect to the DHE network, including wired, wireless, and virtual private networks based on device management.

Glossary:

The definitions for the following Terms used within this document are located in the **DHTS Glossary of Terms.**

Term
Duke Health Enterprise (DHE)
Guest
Guest Network
IT Managed Device
NAC Policies
NAC Profiles
Network Access Control (NAC)
Network Segment
Patient Care Devices
Quarantine Network
Remediation Network
User Managed Device
Whitelist

Policy:

At the time of NAC policy enforcement, the following will be implemented on the DHE networks. See DHE IT-STD-3483 Smartphone and Tablet Standard and DHTS SEC-STD-3522 Network Access Control Standard for technical standard information.

- **IT Managed Devices**
  - IT Managed Devices on the network will have full network access in the appropriate Network Segment if posture checks (NAC agent installed, supported Operating System, Asset Management, and Endpoint Protection) are met. If posture checks are not met, then the device will be placed in a Remediation Network with limited access for user and/or DHTS Service Desk to resolve

compliance. If the device poses an immediate risk, it will be placed in a Quarantine Network for incident response and forensics.

- **User Managed Devices**
  - User Managed Devices on the network may have full network access in the appropriate Network Segment if posture checks (NAC agent installed, supported Operating Systems, and Endpoint Protection) are met. If posture checks are not met, then the device will be placed in a Remediation Network with limited access for the user and/or DHTS Service Desk, or other IT support personnel to resolve the compliance issues.

- **Patient Care Devices**
  - When possible, NAC Profiles are assigned to Patient Care Devices. If a Profile cannot be created, the device will be documented in a Whitelist managed by the IT support group and approved by the ISO. These devices will have full network access in the appropriate Network Segment. If the device poses an immediate risk, it will be placed in a Quarantine Network for incident response and forensics.

- **Guests**
  - Upon first connection to the Guest Network, users are presented with the Acceptable Use Policy. Once acknowledged, they will have Internet-only access. This network is for devices that have no requirement to access Duke Health network resources.

REFERENCES

Audience: Application IT Support Staff & ISO

Policies:
DHE IT-STD-3483 Smartphone and Tablet Standard
DHTS SEC-STD-3522 Network Access Control Standard

Authoritative Sources:
NA

Attachment Names:
NA

Note: DHTS QSD Policies are reviewed at least every two years; however, a review cycle that is more frequent may be requested. All DHE Workforce members are expected to adhere to this policy and all other relevant procedural documents. If the Policies cannot be met, the Business Owner, Service Owner, or designee, is responsible for documenting an eGRC Exception Request

and taking any necessary steps to mitigate risk. (For an Exception Request, refer to DHE SEC-SOP-2239 Information Security Exception Request Management Procedure. For a Planned Deviation, refer to DHTS QA-SOP-2224 DHTS Deviations Management Procedure.)

Revision History (Since Last Version):

Section(s) Affected	Summary of Changes
Glossary	Added link to DHTS Glossary of Terms; removed definitions.
Policy	Review completed; grammatical updates; no content updates.

Author(s) and Approvals

Author(s):
Kimberly Catron

Approver(s) and Quality Reviewer:
Cicely Samuel (04/14/2021), Randall Arvay (04/09/2021)

QSD Policy Template, *QA-T1-2153, V3 Mar 2021*