University of North Dakota Policy

Network Access Control and Authentication

Effective: *September, 2009*
Last Updated: *May, 2010*

Responsible University Officer: Chief Information Officer

Policy Owner: Deputy Chief Information Officer

Policy Contact: Manager of Network Services

Policy Statement

All individuals connecting to the campus network (wired, wireless, or remote access), are required to authenticate through the UND network access control system with an ID that tracks back to the individual. Access logs will be retained in accordance with the campus retention policy. Connecting an unauthorized wireless router or access point to the campus network is prohibited. Attempts to bypass circumvent, or defeat the network access control system is prohibited.

Exclusions

Energy and Environment Research Center and others approved by the CIO.

Reason for Policy

Due to legal and regulatory requirements and NDUS policy, the need to respond to security incidents on campus, and an obligation to protect our valuable network resources, UND must be able to identify every individual who connects to the campus network. For these reasons, UND has implemented a network access control system to be used by all students, employees and others to authenticate for campus network use. This system will also provide a single point for collecting and reporting on user access information for legal or security incident investigations.

Policy Enforcement

Individuals who violate this policy should be reported to the Office of the CIO through which they will be subject to sanctions, including the possible loss of network privileges. Sanctions will be administered through the CIO office and designees.

Contact Information

UND HelpDesk	**777-2222**	**itsshelp@mail.und.edu**

Approved by President Kelley, 9/24/09

Definitions

Authenticate: To authenticate is to determine whether someone or something is, in fact, who or what it is declared to be through the use of an identifier and password or related means.

Campus Network: A campus network is an autonomous network that exists on a university campus connecting local area networks in and among buildings and aggregating traffic to a wide area network.

Network Access Control system: Network access control (NAC), a method of bolstering the security of a proprietary network by restricting the availability of network resources to endpoint devices that authenticate. Additional features include checking for current virus protection and that operating system updates are enabled.

Network Access logs: Information captured upon network access, including identifier, time of connection, network card MAC address, and time of disconnection.

Responsibilities

System / Network Administrator
Allow only authorized and authenticated access to the UND network. Report any security incidents or suspicious activity on the network.

Department or College
Provide or approve sponsored (guest) accounts directly or through referral to ITSS. Ensure that sponsored account users understand and comply with University policies, procedures, and laws relating to conditions of use before authorizing access.

Frequently Asked Questions

http://itss.und.edu/safeconnect.html

Related Information

NDUS Procedures Manual, Section: 1901.2 Computing Facilities
http://ndus.edu/policies/ndus-policies/subpolicy.asp?ref=2551

Approved by President Kelley, 9/24/09