UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS

Virtual Private Network (VPN) Policy

Policy #510

Source of Authority: N.C.G.S. § 116-34(a)
UNC Code § 502(A)

Revision Authority: Chancellor

History: **First Issued:** February 17, 2011

Related Policies: IT Account Management Policy #503;
Technology Use Policy #508;

Responsible Offices: Chancellor

Effective Date: February 17, 2011

I. Purpose

This Policy provides guidelines for Remote Access Virtual Private Network ("VPN") connections to the UNCSA trusted administrative network.

II. Scope

This Policy applies to all UNCSA employees, contractors, consultants, temporary employees, and other workers including all personnel affiliated with third parties utilizing VPNs to access the UNCSA network.

This Policy applies to implementations of all VPN that are directed through any type VPN Concentrator.

III. Definitions

A. "**User Managed Service**" means the that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

IV. Policy

A. Approved UNCSA employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are "user managed" services.

B. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to UNCSA internal networks via their VPN.

C. VPN use is to be controlled using password authentication.

D. Only VPN clients approved by UNCSA's Information Technology Department ("IT") may be used.

E. By using VPN technology with personal equipment, this personal equipment is a *de facto* extension of UNCSA's network, and as such is subject to the same, policies, rules, and regulations that apply to UNCSA-owned equipment.

F. All computers, including personal computers, connected to UNCSA internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the administrative standard.

G. All computers connected to UNCSA internal networks via VPN must have the latest operating system and security patches applied.

H. Users of computers that are not UNCSA-owned equipment must configure the equipment to comply with the UNCSA Technology Use Policy.

I. Peer-to-peer software is not allowed over VPN.

J. Anyone found to have violated this Policy may have their network access privileges temporarily or permanently revoked.

V. Revision History

A. February 17, 2011 – Adopted by Board of Trustees as part of UNCSA Policy Manual

UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS

Virtual Private Network (VPN) Procedures

Procedure #510

I. Requesting Access. To request VPN access, the employee must complete the VPN access request agreement form and submit it to the CIO. The agreement is available at www.uncsa.edu/informationtechnologies/UNCSA-VPN-Agreement-Form.pdf**.**

II. VPN Operations

A. When actively connected to the administrative network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

B. VPN gateways will be set up and managed by the UNCSA IT Department.