



**University of North Carolina School of the Arts
Information Technologies Policy**

Title:

VPN Access Policy

Purpose:

The purpose of this Policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the UNCSA trusted administrative network.

Scope:

This Policy applies to all UNCSA employees, contractors, consultants, temporaries, 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.

Policy:

Approved UNCSA employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally,

- 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.
- VPN use is to be controlled using password authentication. 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.
- VPN gateways will be set up and managed by the UNCSA IT office.
- All 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. Information on this software can be obtained from UNCSA Desktop Support, this includes personal computers.
- All computers connected to UNCSA internal networks via VPN must have the latest operating system security patches applied. Information on these patches can be obtained from UNCSA Desktop Support.
- Users of computers that are not UNCSA-owned equipment must configure the equipment to comply with UNCSA Technology Use Policy.

- Only IT approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of UNCOSA's network, and as such are subject to the same rules and regulations that apply to UNCOSA-owned equipment.
- Peer-to-peer software is not allowed over VPN.
- Anyone found to have violated this Policy may have their network access privileges temporarily or permanently revoked.

Procedures:

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/UNCOSA-VPN-Agreement-Form.pdf.

Distribution:

Distribution to department heads
UNCOSA's website

Executive Council Approval/Revalidation Date:

December 17, 2009