VPN Access and Procedures

Authority: CIO

History: Effective date: 18-January-2008

Sources of Authority:
Responsible Office(s): ITS

I. Purpose

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

II. Scope

This Policy applies to all UNCA employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the UNCA network. This Policy applies to implementations of all VPN that are directed through any type VPN Concentrator.

III. Policy

Approved UNCA 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. Further details may be found in the Remote Access Policy.

Additionally,

1) It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to UNCA internal networks via their VPN.
2) 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.

3) Dual (split) tunneling is NOT permitted; only one network connection is allowed.

4) VPN gateways will be set up and managed by the UNCA ITS office.

5) All computers connected to UNCA 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 UNCA User Support, this includes personal computers.

6) All computers connected to UNCA internal networks via VPN must have the latest operating system security patches applied. Information on these patches can be obtained from UNCA User Support or your college computer consultant.

7) Users of computers that are not UNCA-owned equipment must configure the equipment to comply with UNCA Usage (#72) and Network Security (#78) Policies.

8) Only ITS approved VPN clients may be used.

9) By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of UNCA’s network, and as such are subject to the same rules and regulations that apply to UNCA-owned equipment, i.e., their machines must be configured to comply with all UNCA Usage (#72) and Network Security (#78) Policies.

10) Peer-to-peer software is not allowed over VPN.

11) Computer with multiple user accounts (i.e. true multiuser hosts) are not allowed to create VPN connections to the trusted network for the entire host and its users. Note: At this time we know of no way to allow single user VPN connections on multiuser computers.
IV  Procedures
   1) To request VPN access, the employee must complete the VPN access request agreement form and forward it to their supervisor. The agreement is available at www.unca.edu/compcenter/policies/ITS_VPN_Agreement.pdf

V  Enforcement

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

VI. Definitions

**VPN**  Virtual Private Network, a way to extend the corporate/production (trusted) network using authentication and encryption.

**VPN Concentrator**
   A device in which VPN connections are terminated.

**VPN Client**
   A device, usually a single computer running client software.

6.0 Revision History

________________________________________________________