Virtual Private Network (VPN) Policy

Policy 912

1 Introduction

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

2 Scope

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

3 Definitions

3.1 VPN

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

3.2 VPN Concentrator

A device in which VPN connections are terminated.

3.3 VPN Client

A device, usually a single computer running client software.

4 Policy and Procedure Statements

4.1 Policy

4.1.1 Approved Appalachian State University 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.

4.1.2 Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Appalachian State University 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 Appalachian State University ITS office.
5. All computers connected to Appalachian State University 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 ASU Technical Support (phone: 828.262.6266, email: techsupport@appstate.edu); this includes personal computers.
6. All computers connected to Appalachian State University internal networks via VPN must have the latest operating system security patches applied. Information on these patches can be obtained from ASU Technical Support or your college computer consultant.
7. Users of computers that are not Appalachian State University-owned equipment must configure the equipment to comply with Appalachian State University's VPN and Network 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 Appalachian State University's network, and as such are subject to the same rules and regulations that apply to Appalachian State University-owned equipment, i.e., their machines must be configured to comply with all Appalachian State University Security Policies.
10. Peer-to-peer software is not allowed over VPN.
11. Computer with multiple user accounts (ie 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.

4.2 Enforcement

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

5 Additional References

6 Authority

7 Contact Information

8 Original Effective Date

This policy was approved by the Provost on July 19, 2005

9 Revision Dates