Policy 908

1 Introduction

1.1 The purpose of this Policy is to define standards for connecting to Appalachian State University's network from any remote host, untrusted host, and remote network, including untrusted hosts on Appalachian State University?s intranet. These standards are designed to minimize the potential exposure to Appalachian State University from damages, which may result from unauthorized use of Appalachian State University resources. Damages include the loss of sensitive or university confidential data, intellectual property, damage to public image, damage to critical Appalachian State University internal systems, etc.

2 Scope

2.1 This Policy applies to all Appalachian State University employees, students, contractors, vendors and agents with an Appalachian State University-owned or personally owned computer or workstation used to connect to the Appalachian State University network. This Policy applies to remote access connections used to do work on behalf of Appalachian State University, including but not limited to, reading or sending email and viewing intranet web resources.

2.2 Remote access implementations that are covered by this Policy include, but are not limited to, dial-in modems, DSL, VPN, SSH, and cable modems, etc.

3 Definitions

3.1 Cable Modem

Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

3.2 Closed Network

Networks that are located on the University Trusted Core Network.

3.3 Dial-in Modem

A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "http://policy.appstate.edumodem"http://policy.appstate.edu for modulator/demodulator.

3.4 Dual Homing

Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Administrative network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on an Appalachian State University-provided Remote

Access home network, and connecting to another network, such as a spouse's remote access.

3.5 DSL

Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

3.6 Internet

All networks external to Appalachian State University.

3.7 Intranet

All networks internal to Appalachian State University.

3.8 Remote or Outside User

User connecting to Appalachian State University from the Internet or Untrusted VLANs on Appalachian State University?s intranet.

3.9 Remote Access

Any access to Appalachian State University's administrative network through a non-Appalachian State University controlled network, device, or medium.

3.10 Split-Tunneling

Simultaneous direct access to a non-Appalachian State University network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Appalachian State University's trusted administrative network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "http://policy.appstate.edutunneling"http://policy.appstate.edu through the Internet.

3.11 Trusted User

Appalachian State University Staff, Faculty, or Third party contractors who have executed a Third Party Connection Agreement.

3.12 VLAN

Virtual Local Area Network.

4 Policy and Procedure Statements

4.1 General

1. It is the responsibility of Appalachian State University employees, students, third party contractors, vendors and agents with remote access privileges to Appalachian State University's campus networks to ensure that their remote access connection is given the same consideration as the user's on-site connection to Appalachian State University.
2. General access to the Internet for recreational use by immediate household members is discouraged through the Appalachian State University Dial-in Modem Network. The Appalachian State University employee is responsible to ensure the family member does not violate any Appalachian State University policies, does not perform illegal activities, and does not use the access for outside business interests. The Appalachian State University employee bears responsibility for the consequences should the access be misused.
3. Access to the Appalachian State University Trusted Network will only be allowed from Trusted Users and other special ITS administered subnets.
4. Remote or outside Trusted Users (defined below) may gain access to Trusted hosts in one of two ways:
    1. The outside Trusted user will initiate a connection and authenticate to the Appalachian State University VPN endpoint (see VPN_Policy). Username and password pairs will be distributed to Third Parties upon receipt of a valid Third Party Connection Agreement. Currently Windows 9x, NT, 2000 and XP platforms are supported. Network Infrastructure and Control Systems will make client software available upon request.
    2. The Appalachian State University inside Trusted device to be connected must initiate the connection. In other words, the connection must be made from the on campus Trusted device.
    3. If these methods are not suitable or are not technically feasible, the Appalachian State University device will need to be moved to the Open_Servers VLAN (see Open_Servers VLAN Policy). The Open Servers VLAN is in the Untrusted zone. Furthermore, if Remote Access of the Open_Servers VLAN device is used for system administration functions (Root Access), the user performing these functions must be defined by the "http://policy.appstate.eduTrusted User definition"http://policy.appstate.edu, defined below.
5. Please review the following policies for details of protecting information when accessing the administrative network via remote access methods, and acceptable use of Appalachian State University's network:
    1. Acceptable Use Policy (Policy on the Use of Computers and Data Communications)
    2. Virtual Private Network (VPN) Policy
    3. Trusted Access Policy

4.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via password authentication.
2. At no time should any Appalachian State University employee or student provide his or her login or email password to anyone, not even family members.
3. All hosts that are connected to Appalachian State University internal networks via remote access technologies must use the most up-to-date anti-virus software. Information on this software can be obtained from the ASU Technical Support group (phone: 828.262.6266, email tech support; this includes personal computers.
4. Where possible use secure methods for remote access. I.E. Use SSH in place of Telnet, secure web servers, SCP in place of FTP.
5. Direct access (initiated from the Internet) will not be allowed to machines registered as regular staff, faculty or student.

4.3 Enforcement

4.3.1 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