Trusted Access Policy

Policy 911

1 Introduction

1.1 The purpose of this Policy is to establish standards for Trusted Access (defined below) to devices on the Appalachian State University Network. Effective implementation of this Policy will minimize unauthorized access to Trusted Devices. This Policy will help protect Appalachian State University proprietary information and technology and individual personal computers from malicious intent (a.k.a. hacking or cracking) from Untrusted Users.

2 Scope

2.1 This Policy applies to all network access directly or indirectly connecting to devices on Appalachian State University networks.

3 Definitions

3.1 Definition phrase or word

   Definition summary

3.2 Remote or Outside User

   Any user or device not directly connected to the Appalachian State University campus network.

3.3 Trusted Access

   Network connection to the Trusted Network (defined below). Or connections to device(s) in the Open_Servers VLAN that are privileged. i.e. Root/Administrator level access.

3.4 Trusted Device

   A device connected to the on campus network that has been registered for Network use by or for a staff or faculty member using their University Computer User Account. Or devices located in special ITS managed subnets.

3.5 Trusted User

   Devices registered using Appalachian State University Staff and Faculty Computer User Accounts. Remote or Outside User connections authenticated as Trusted Users via VPN. Also with limitations, Third Parties who have executed a Third Party Connection Agreement authenticated via VPN.

3.6 Trusted Network

   All devices registered by a Trusted User and other devices registered in special Trusted VLANs such as Special Purpose and University Administrative subnets.

3.7 Untrusted Network

   All devices not defined under Trusted Network, including but not limited to Internet devices.

3.8 Untrusted Users

   Devices on campus not registered by a Trusted User or off campus connections not authenticated via a VPN connection as a Trusted User.
3.9 VLAN
Virtual Local Area Network.

3.10 VPN
Virtual Private Network. A way to extend the Trusted Network using authentication and encryption.

4 Policy and Procedure Statements

4.1 General

4.1.1 All internal computing devices deployed at Appalachian State University must be registered by an operational group or individual that is responsible for system administration and or operation. The default registration zone for devices registered by faculty and staff using their University Computer User Account is in the Appalachian State University Trusted Network. The Trusted Network is made up of devices whose business mission does not require access to be initiated to the device from the Untrusted Network.

1. Access to the Appalachian State University Trusted Network will only be allowed to be initiated from Trusted Devices and other special ITS administered subnets.
2. Remote or outside Trusted Users (defined below) may gain access to local Trusted Device(s) in one of three ways:
   1. The outside Trusted User must initiate a connection and authenticate to the Appalachian State University VPN endpoint (see VPN_Policy) using their Appalachian Computer User Account and password. Special username and password pairs will be distributed by Network Infrastructure and Control Systems (NICS) to Third Parties upon receipt of a valid executed Third Party Connection Agreement. Currently Windows 9x, NT, 2000 and XP platforms using the Enterasys VPN client are supported. NSS will make client software available upon request.
   2. The Appalachian State University inside Trusted Device that requires the connection must initiate the connection. In other words, the connection must be made from the on campus Trusted Device to the other 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). Note: The Open_Servers VLAN is in the Untrusted zone and is provided minimal enterprise security.
3. Access will not be allowed to be initiated from Untrusted Users in the Untrusted Network (including the Internet) to the Trusted Network.
4. All connectivity to devices in the Trusted Network, and/or Root/Administrator privileged connectivity to Open_Servers VLAN devices by a Third Party must be preceded by the execution of a Third Party Connection Agreement. Note: PCAnywhere connections constitute Root/Administrator privilege.

4.2 Compliance

4.2.1 Special firewall rules will be put in place to block access attempts from being initiated from the Untrusted Network to the Trusted Network. This limits the Trusted Device’s exposure to malicious activities that will come from the Untrusted Network, including the worldwide Internet.

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