Policy 914

1 Introduction

2 Scope

3 Definitions

4 Policy and Procedure Statements

4.1 Network Infrastructure and Control Systems

4.1.1 Network Infrastructure and Control Systems has been mandated by the University to manage the campus network ? ?from the wall-plate to the Internet,? in order to ensure reliability, security, integrity and interoperability on the network backbone infrastructure. It is also the responsibility of Network Infrastructure and Control Systems to ensure the integrity, security and appropriate use of the campus ??radio space?? in terms of wireless networking. Even more so than with traditional wired networking technology, 802.11 wireless networking has a multitude of issues that can ??step on?? or conflict significantly with campus services and policies. Channel allocations, device placement, information exposure and access point configuration all have the potential to disrupt critical campus services or inadvertently distribute private or sensitive information protected by law.

4.1.2 Consequently, just as is the case with the campus wired network infrastructure, schools and departments at Appalachian State University are not permitted to install their own wireless infrastructures without meeting certain requirements.

4.1.3 Wireless requirements and information follows:

4.1.3.1 ?Sniffing? or listening in on wired or wireless LANs is expressly prohibited except as a trouble-shooting procedure by Network Infrastructure and Control Systems personnel and/or designated information security officer.

1. Any school or department wishing to pursue 802.11 wireless networking within their building or for their department should call 828.262.6266 and have a RightNow Remedy ticket submitted to Network Infrastructure and Control Systems, in order to arrange for an appropriate site survey that will assess the requirement for wireless connectivity, determine how many access points/radios are needed and where the optimum location for placement of these radios would be.
2. If the purpose of the wireless connectivity is for departmental administrative/faculty/staff connectivity, the department is responsible for all costs associated with the equipment and any wiring that might be required; however, Network Infrastructure and Control Systems will provide all installation, configuration, maintenance and management of the access point(s) at no charge to the department. Network Infrastructure and Control Systems will provide specific details as to what would need to be purchased and from where.
3. Central funding for classroom wireless is not available at this time.
4. The University has established the Aruba Network product line as the standard for 802.11 wireless access points; access points from any other vendor are not acceptable. If any non-standard access points are identified, they will lose connectivity from the network. Wireless gateways (NAT routers) are not allowed.

5. Because of network security concerns, State rules do not permit individuals or departments to have wireless Network Access Points (that do not meet these restrictions) attached to the University production network. If such ?rogue? devices are detected by state or local auditors during regular audits, a ?finding? may be forwarded to the Chancellor. If the findings are not rectified, they can result in lost privileges for the University.
6. Even if a school or department purchases an Aruba Network access point, it must be administered by Network Infrastructure and Control Systems.
7. All wireless access for official University business and student access must be WPA/WPA2/802.11i encrypted. .
8. The asu-visitor SSID is for University visitors that do not have a University Computer Userid. This SSID is not encrypted and will be very restricted and should NOT be used for official University business including student access.
9. The ?asu? and ?asu-? ssids are reserved for use only on Appalachian State University owned Access Points.

4.1.3.2 Failure to follow these wireless networking policies and procedures will result in any non-compliant devices losing network connectivity until there is compliance.

4.1.3.3 It is important to keep in mind that wireless technology is, and will for the foreseeable future be, a shared bandwidth technology (like old shared Ethernet hubs). As such, services that rely on appropriately configured switched electronics, like IP Multicast, will not effectively work in a wireless environment.

4.1.3.4 Also, special considerations must be given to using wireless for sensitive applications.

4.1.3.5 If you have any specific questions not addressed above, please contact the Technical Support Center at 828.262.6266 for further assistance.

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