

**AUSTIN PEAY STATE UNIVERSITIES
POLICY AND PROCEDURES MANUAL**

Policy Number: 4:033	Supersedes Policy Number: N/A
Date: April 4, 2008	Dated: November 11, 2005
Subject: Connecting Network Extension Devices and Server Services to the campus and residence network	Mandatory Review Date: April 4, 2013
Initiating Authority: Vice President of Finance and Administration	TBR Policy/Guideline Reference: 1:08:00:00
Approved: President: signature on file	

I. PURPOSE

The purposes of this policy include:

- A. to articulate the rights and responsibilities of persons using information technology resources owned, leased, or administered by Austin Peay State University (APSU)
- B. to protect the interests of users and APSU
- C. to facilitate the efficient operation of APSU information technology resources

This policy is not intended to discourage computer use, but to promote and maintain a reliable computer network for the entire university community to use.

II. GENERAL

It is the responsibility of the Austin Peay State University Office of Information Technology (OIT) to provide security, ensure appropriate use, and allocate access to network resources and bandwidth in an equitable manner to the campus community. Thus, the university has established several guidelines to manage the specifics regarding connecting network devices and installing network server services to the campus network as well as the residence hall network.

APSU reserves the right to remove any network equipment or server services at any time. APSU reserves the right to disable any network port that is causing disruption to any or all parts of the campus and residence hall networks until the cause of the disruption is removed.

III. RESTRICTIONS ON CAMPUS NETWORK

- A. The campus network includes all academic and administrative buildings on the APSU main campus, Fort Campbell, Public Square as well as administrative and academic use areas (offices, labs, etc) in the residence halls.
- B. Only network devices (including but not limited to devices such as hubs, switches, routers, and wireless access points) approved by OIT will be allowed for use on the campus network.
- C. Only network server services (including but not limited to DHCP, DNS, SMTP, WINS, and routing services) approved by OIT will be allowed for use on the campus network.
- D. University faculty, staff, and students are not permitted to attach personal network devices or install network server services in any campus locations including but not limited to classrooms, labs, offices and public areas.
- E. Departments wishing to extend their network connectivity, implement wireless networking or install network services should contact OIT.

IV. RESTRICTIONS ON RESIDENCE HALL NETWORK

- A. The residence hall network includes all residence halls on the APSU main campus with the exception of administrative and academic use areas (offices, labs, etc) in the residence halls.
- B. One network port per student is provided in residence hall rooms. One network port per apartment is provided in married student housing. This is sufficient for connecting one computer to the network at a time.
- C. Some students in the residence hall network may wish to extend the network in their room to allow the connection of more than one computer or other network devices such as printers or game consoles in addition to their primary computer.
- D. If more than one network connection is desired, routers, switches and hubs in the residence halls are permitted, but only on a *“use at your own risk”* basis and as long as these devices are not capable of providing wireless services. Improper installation and management of these devices may cause disruption of network services to the student’s port. If use of these devices does cause disruption to the student’s port, the student will be required to remove the equipment causing the disruption before network services can be re-enabled.
- E. Students may not install other network extension devices (including but not limited to wireless access points) in their residence hall rooms.

- V. Students may not install network servers that provide network services (including but not limited to DHCP, DNS, SMTP, WINS, and routing services) in their residence hall rooms.

VI. CONSEQUENCES

- A. All users shall comply with the Tennessee Board of Regents Policy (TBR) 1-08-00-00, Information Technology Resources, which may be found at: http://www/tbr/state/tn.us/policies_guidelines/goverance_policies/1-08-00-00.htm. Said TBR policy (and any subsequent versions thereof) is hereby fully incorporated and made a part of this university policy.
- B. The installation of unauthorized network extension devices and server services are known to interfere with the operation of the APSU network. Operation of these devices and services is a violation of University policy, and will result in loss of network access and/or disciplinary action. Intentional interruption of APSU network services will result in further disciplinary action and/or prosecution. Visit these policies for further computer usage information:
- 3:013 - “Student Code of Conduct”
<http://www.apsu.edu/policy/pdf/3013.pdf>
 - 4:032 - “Acceptable Use of Information Technology Resources”
<http://www.apsu.edu/policy/pdf/4032.pdf>