ITPC 04-1
Approved 3-17-05

Information Technology Policy Committee
Network Monitoring and Access Guidelines

Information Technology Services (ITS) Network Support monitors IPFW network traffic to discover and address network usage and quality of service issues. Although traffic is not being monitored for content, content may be viewable. ITS is authorized to monitor network traffic without prior permission under the provisions of the Wiretap Act, the Pen Register, and the Trap and Trace "Provider Exception" clauses. ITS Network Support will also limit bandwidth availability for uses which are not considered part of the university mission, such as gaming and non-instructional use of music and video.

IPFW Network Access for Computer Servers

ITS is authorized to approve each request to connect a workstation to the IPFW network for use as a server. Servers which will be managed by any department or office other than ITS will not be permitted to use the DNS, DHCP, and SMTP protocols.

Due to possible interference with the campus wireless system, any non-ITS wireless device that will function as a wireless access point, router, or server should be approved by ITS.

Any workstations, servers, or devices that are performing the function of a server, not managed by ITS, but connected to the IPFW network must have up-to-date virus protection, current operating system patches, and a configuration that disables unnecessary ports and services. In addition, the server administrator is responsible for compliance with all federal and state laws and all university policies concerning data security and confidentiality. Additional information is available at http://www.its.ipfw.edu/regs/policies/networkmonitoring.html .

If any server is found to be inadequately configured or appears to be negatively affecting the IPFW network, ITS will notify the person or department responsible and allow 48 hours to bring the server up to current standards. If the device does not meet standards within this time period, it will be disconnected from the IPFW network until ITS can verify that the problem has been resolved. If a server is found to be having a severe impact on the network, ITS may immediately disconnect the device from the network.

IPFW Network Access for Computer Workstations

Computer workstations to be connected to the IPFW network using wired connections must meet the current hardware standards specified on the Minimum Networked Workstation/Printer Standards Web page found at http://www.its.ipfw.edu/regs/policies/workstations.html . ITS must be provided access to the workstation for installation of current network protocols, and each user will be required to establish an IPFW network account.

Wireless access to the IPFW network is restricted to users with a valid network account.