WASHINGTON STATE UNIVERSITY
EXECUTIVE POLICY MANUAL
Executive Policy #16
Approved September 3, 2003

University Network Policies

BACKGROUND

Washington State University's network infrastructure and network services are vital to carry out the mission of the University. Policies are needed to ensure the continued integrity of these assets.

Three areas have been identified which require policy statements:

Network Protection – Protection of the physical network infrastructure.

Network Devices and Services – Management responsibility for devices connected to the network infrastructure and services offered over the network.

Network Information Services Access – Access to network information services provided by WSU.

Also refer to:

Electronic Publishing Policy: Policy on Electronic Publishing and Appropriate Use of Computing Resources, Information Technologies, and Networks (*Executive Policy* 4)

University Data Policies (*Executive Policy* 8)

Wireless LAN Policy (*Executive Policy* 13)

University Antivirus Policy (*Executive Policy* 14)

DEFINITIONS

Network infrastructure is the collection of elements that provide the mechanism to carry out electronic data, voice, and video communications. This includes cabling, switches, routers, computers, software, other network components for wide-area/local-area, and wireless network hardware such as wireless access points and their associated components operated within the boundaries of WSU.

WSU **network information services** are the information and transactional services that WSU makes available for use via the WSU network and/or the Internet. Examples include central and local e-mail services, self-service Web applications, online course management systems, e-commerce sites, etc.

A **public service** may be accessed by anyone without supplying personal identification that is associated with appropriate authorization.

Access to a **nonpublic service** is restricted and cannot be gained without proper identification and authorization.

For purposes of issue and complaint investigation and resolution, "WSU" is defined as Information Technology and/or the system/network administrators at the local department or college level working in concert with the Information Technology unit at that campus.

University Network Policies

Network Protection Policy

PURPOSE

Washington State University must have a stable and reliable environment for all students, faculty, staff and affiliates to conduct computing and communication activities. This network protection policy is intended to protect and preserve the physical network infrastructure over which these activities are conducted.

NETWORK PROTECTION POLICY STATEMENT

The WSU network infrastructure shall be protected from accidental or malicious destruction or modifications and from activities that impair network usability and performance.

ACCESS TO THE WSU NETWORK INFRASTRUCTURE

Access to the physical network infrastructure behind the faceplate connections shall be limited to only those individuals authorized by central information technology departments (WSU IT in Pullman, Information Services in Spokane, Tri-Cities, Vancouver, ICN, etc), hereafter referred to collectively as Central IT/IS. This includes access to telecommunications closets, access to and use of telecommunications pathways (cable trays, horizontal distribution conduits, riser systems, etc.), and access to and use of telecommunications media (fiber strands, copper pairs, etc.). Access to the above facilities by Facilities Services, Operations staff is permitted when performing maintenance in the facilities or when completing work orders that are requested or approved by authorized Central IT/IS.

Wireless access points, installed and/or maintained by Central IT/IS, are considered to be a part of the physical infrastructure and therefore access is restricted to designated individuals.

Access via network or other data connection to the management features of any electronic network infrastructure equipment owned and/or managed by Central IT/IS shall be limited to Central IT/IS staff or their designated representative.

Central IT/IS is responsible for the telecommunications infrastructure space and equipment and shall insure that these spaces are safe and secure. Therefore physical access to these spaces will be strictly controlled. To ensure the safety and accessibility of the communications infrastructure, communications closets must be single-purpose facilities and cannot be utilized as auxiliary space for purposes such as storage, janitorial closets, etc.

Unauthorized modifications to or tampering with the physical network or electronic network equipment will be considered inappropriate use and may be subject to disciplinary and/or criminal action. (See also University Appropriate Use Policy, *Executive Policy* 4)

University Network Policies

Network Protection Policy (cont.)

DEPARTMENTAL EXTENSIONS TO THE WSU NETWORK

Departments may extend the WSU network with small intra-office networks to accomplish local goals provided these networks do not require access to the physical WSU network infrastructure as described above. Furthermore, these networks must not impair the usability or performance of the WSU network in any way beyond the usual network traffic resulting from additional devices being attached to the network extension. All departmental components (switches, cables, connectors, etc.) must meet current industry performance standards and be of sufficient quality to maintain overall network performance. Installation of departmental cabling must meet National Electrical Code (NEC) standards, Washington State Department of Labor and Industries standards and licensing requirements, and Electrical Industries Alliance/Telecommunications Industries Alliance (EIA/TIA) telecommunications cabling specifications.

Extensions to the WSU network using wireless technologies must comply with the Wireless LAN Policy (*Executive Policy* 13). Privacy and confidentiality issues must be considered before utilizing wireless technologies.

Departments are encouraged to contact IT for a review of their plans for installing network extensions to ensure that network performance will not be impaired by the installation and that the extension does not violate State of Washington Codes.

WSU reserves the right to review any departmental network extensions and disconnect those components that impair network usability, performance or security.

University Network Policies

Network Devices and Services Policy

PURPOSE

The WSU network and the network services made available thereon are vital resources for the successful operation of the University. This network devices and services management policy is intended to protect the integrity of the WSU network and its constituent elements and thereby ensure the continued availability of all services provided via the WSU network.

NETWORK DEVICES AND SERVICES POLICY STATEMENT

All devices that are connected to the WSU network and all WSU-provided services available via the WSU network shall be actively managed to ensure the integrity, performance, and availability of the network and availability of WSU network services.

NETWORK DEVICE AND SERVICE MANAGEMENT RESPONSIBILITY

Deans/directors, system administrators, all individual computer users, and third-party vendors are responsible for actively managing the network devices and/or services under their control. This includes protecting the devices and services from accidental or malicious service outages and disruptions by exercising appropriate precautions. See Appendix A for a Best Practices guideline.

Also see University Antivirus Policy (*Executive Policy* 14) for protecting computer operations and resulting performance of the network.

WSU reserves the right to review any device or service attached to the WSU network (public or nonpublic) for vigilant management, adequate security, and appropriate representation of the University as defined in the Electronic Publishing Policy: Policy on Electronic Publishing and Appropriate Use of Computing Resources, Information Technologies, and Networks (*Executive Policy* 4). WSU reserves the right to deny access to the WSU network by any device or service that is deemed to be a significant security risk.

University Network Policies

Network Information Services Access Policy

PURPOSE

Some services provided by WSU and its affiliates via the WSU network are available to the public, i.e., they may be accessed by anyone without supplying personal identification that is associated with appropriate authorization. These are *public services*. However, most WSU network services are nonpublic, i.e., access to the service is restricted and cannot be gained without proper identification and authorization. These are *nonpublic services*. This network services access policy is intended to ensure that all nonpublic network services provided by WSU are accessible only by the appropriate persons.

NETWORK SERVICES ACCESS POLICY STATEMENT

Each nonpublic network service shall ensure that access is provided only to the appropriate individuals by using the WSU Network Authentication Service or equivalent departmental authentication system.

NETWORK AUTHENTICATION SERVICE

The WSU Network Authentication Service provides verification of a user's identity for access to nonpublic WSU network services. All WSU entities are encouraged to use the Network Authentication Service to control access to any nonpublic services that they might provide via the WSU network.

NETWORK SERVICE USER IDENTIFICATION

The WSU Network Authentication Service manages user identification for individuals in the University community to access nonpublic WSU network services. Students, employees, and others approved by the University are eligible to obtain a unique WSU network user identification called a *Network ID*.

- Each individual may select his/her own Network ID, however WSU reserves the right to refuse acceptance or require replacement of a Network ID.
- Each individual is responsible for any and all use of the WSU network or network services obtained under his/her Network ID.
- Network ID passwords must not be shared or transferred to others.
- Possession of a valid Network ID and password does not necessarily imply any right or privilege.

Departments using alternative identification systems are strongly encouraged to promote security by establishing and publishing similar guidelines for their services.

University Network Policies

Network Information Services Access Policy (cont.)

NETWORK SERVICE USER AUTHORIZATION

A nonpublic service on the WSU network may require additional authorization procedures to determine the user's authority and/or level of privileges in using that nonpublic service.

NETWORK SERVICE USER EXPIRATION

Any provider of a nonpublic WSU network service must maintain a list of authorized users or other authorization information. The provider of that service must review and update those authorizations on a regular basis including expiration/removal of authorization for those individuals no longer eligible for access to that particular service. These include faculty and staff that have left the University, students who are no longer enrolled at the University, and third parties that are no longer under contract or other relationship to the University. Care should be taken to specifically preserve access using the WSU Network ID for retirees to services related to retirement and benefits information.

Deans/directors, personnel officers, system administrators and others that grant access to nonpublic systems must ensure that this access is removed when no longer needed for business or academic purposes.

University Network Policies

Appendix A:
Best Practices Guidelines

In order to maintain appropriate network security and integrity it is strongly suggested that all workstations, servers and other network equipment be continually maintained in the following areas:

- Apply the latest software and firmware updates/patches in a timely fashion.
- Install and maintain antivirus software as required by the University Antivirus Policy. See *Executive Policy* 14.
- Disable unnecessary services/daemons such as mail relay (SMTP), SNMP, telnet, ftp, etc.
- Disable or otherwise protect vulnerable TCP/IP ports.
- Take appropriate steps to physically secure servers from theft or damage.
- Regularly review activity logs for evidence of break-ins and take the appropriate corrective actions.
- Maintain regular system backups to facilitate disaster recovery.
- Prevent creation and use of passwords that can be easily cracked, e.g., 12345, a single letter or number repeated, a dictionary word, drowssap (password spelled backwards), etc.
- Remove or disable unused accounts.
- Keep informed of current industry security standards and apply them as appropriate.