



THE GEORGE  
WASHINGTON  
UNIVERSITY  
WASHINGTON DC

**Responsible University Official:**  
Vice President and Chief Information Officer  
**Responsible Office:** Information Systems and Services  
**Origination Date:** June 4, 2003

## NETWORK USAGE AND SECURITY POLICY

### Policy Statement

Use of the University network constitutes consent to the University’s [Code of Conduct for Users of Computing Systems and Services](#), as well as other University policies and laws regarding use and security of University information and systems. Network users and administrators are responsible for following the security requirements set forth in this policy, and for immediately reporting suspected security violations to the Chief Information Officer.

### Reason for Policy/Purpose

The University network is critical to the University’s mission, goals and operations. The purpose of this policy is to establish requirements for use and protection of the University network and the information transmitted via that network.

### Who Needs to Know This Policy

Faculty, staff and students

### Table of Contents

### Page #

Policy Statement .....	
Reason for Policy/Purpose .....	
Who Needs to Know This Policy.....	
Table of Contents .....	
Policy/Procedures .....	
Website Address .....	
Contacts.....	
Definitions.....	
Related Information .....	

# NETWORK USAGE AND SECURITY POLICY

Appendices.....  
Who Approved This Policy .....  
History/Revision Dates .....

---

## Policy/Procedures

---

The University network refers to those devices and communication pathways that form the campus computer and data communications infrastructure. University departments and individuals that make use of the University network and computing equipment connected to the networks are responsible for keeping the network and departmental workstations secure in accordance with this policy.

### I. Role and Authority of Information Systems and Services

Due to the critical nature and function of the University network, the design, operation and maintenance of the network is delegated exclusively to Information Systems and Services (ISS). For further information on Information Systems and Services Roles and Authority with respect to network security, see Appendix A.

### II. User Responsibilities

#### A. Basic Security Measures

All network users are responsible for implementing the following basic security measures with respect to their workstations:

- Installing a current version of anti-virus software;
- Running an operating system that has been recently updated and patched;
- Uploading all vendor-recommended security updates to GW-owned computers when prompted to do so by Patchlink;
- Utilizing a personal firewall is recommended;
- Users of the University’s Virtual Private Network or Wireless Network must implement anti-virus software, an updated and patched operating system, and a personal firewall;
- Following all security measures and requirements as set forth in the [Information Security Policy](#) and the [Data Classification Security Policy](#); and
- Encrypting laptop computers and other mobile devices containing confidential information in accordance with the [Mobile Device Security Policy](#).

#### B. Additional Security Requirements for Wireless Network and Virtual Private Network Usage

Security threats increase when using remote access such as a Wireless Network or the Virtual Private Network (VPN). Thus, all wireless and VPN connections and transmissions are logged by ISS, and are subject to scanning by ISS-approved officials.

## NETWORK USAGE AND SECURITY POLICY

Wireless Network and VPN users must maintain the workstation security measures identified under User Responsibilities, above. In addition, VPN users may use the VPN only under the following stipulations:

- ISS shall limit access to the VPN to individuals who have a justifiable administrative, business, academic or research need to access University-owned systems from a remote or wireless location.
- VPN users who require privileged access to administrative University systems must receive written approval from their department head before access to the VPN service will be granted.
- VPN users must use the VPN client in accordance with all University policies.
- VPN users must use the standardized VPN client offered by ISS and may not reconfigure the VPN client. They must not allow others who have not received written permission from their department head or other University-authorized official to use the VPN client.

Upon graduation or termination of employment with the University, all VPN users must uninstall the VPN client, return all University equipment (if applicable) and refrain from further accessing any system via VPN unless the user has ongoing permission to access University-owned systems. VPN user accounts will be deleted after 90 consecutive calendar days of inactivity. The VPN user's department head must again provide written permission for the user's account to be reinstated.

### **B. Unauthorized Access and other Network Security Violations**

It is a violation of this policy for any user connected to the University network to allow an unauthorized individual to use the network. Other network security violations include but are not limited to routing between networks, using networks in a manner that degrades quality of network service, stealing an Internet Protocol (IP) address, "spoofing," "phishing," using peer-to-peer (P2P) or other similar file sharing technologies without approval of the Vice President and CIO, or using network resources in violation of applicable laws or University Policies. The University network and users use thereof are subject to monitoring by ISS.

### **III. Administrator Responsibilities**

#### **A. System Security**

The administrator of a server for University network-connected computers is responsible for the security of that system. The administrator must monitor and log accesses and keep other system logs that could be useful in establishing the identities and actions of people, programs and processes that might use the system to breach network or system security. All servers that provide access to the University network or Internet services must require user authentication in order to restrict access. Units that operate publicly accessible computers connected to the University network must implement safeguards

## NETWORK USAGE AND SECURITY POLICY

against network abuse appropriate to the network access available to users of those systems.

### **B. Information Security**

Data that is considered confidential as defined by the [Data Classification Security Policy](#) must not be publicly accessible. System administrators are responsible for reasonably securing these systems so as to reduce the threat to the University as a whole.

As network data transmissions are not secure, confidential data should either be encrypted separately before transmission, or a secure network transmission protocol that provides encryption automatically should be used. Contact ISS at (202) 994-7803 or at [infosec@gwu.edu](mailto:infosec@gwu.edu) for further encryption information and resources.

Departments may elect to require individual users to be responsible for their own machines, or hire a Local Support Partner or other technical support person to assist in fulfilling these requirements in accordance with the [Local Support Partner \(LSP\) Policy](#).

### **IV. Reporting Security Violations**

Due to the interconnections provided by University network, a security violation on one machine can threaten security of other systems on the network. Accordingly, any suspected instances of security violations must be reported immediately to the Chief Information Officer at (202) 994-0599.

---

## **Website Addresses for This Policy**

---

[GW University Policies](#)

---

## **Contacts**

---

<b>Subject</b>	<b>Contact</b>	<b>Telephone</b>	<b>Email Address</b>
Encryption/Protection	ISS	(202) 994-7803	<a href="mailto:infosec@gwu.edu">infosec@gwu.edu</a>
General Inquiries	Director, IT Services	(202) 994-0102	
Network Problems	ISS Help Desk	(202) 994-5530 Option 2	<a href="mailto:ithelp@gwu.edu">ithelp@gwu.edu</a>
Security Violations	Chief Security Officer	(703) 726-4412	<a href="mailto:krizi@gwu.edu">krizi@gwu.edu</a>

## Definitions

---

<b>Firewall</b>	A set of related programs that protects the resources of a private network from users from other networks.
<b>Internet Protocol Address</b>	A IP address is a number that uniquely identifies each sender or receiver of information that is sent across the Internet.
<b>Local Area Network</b>	A LAN is a group of computers that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area.
<b>Operating System</b>	A program that serves as an interface between a system user and computer hardware that manages all the other programs in a computer (e.g. Windows XP or ME, or Mac OS X)
<b>Patch</b>	A quick-repair job for a program. Even after a software product has been formally released, problems (called bugs) will almost invariably be found. A patch is the immediate solution that is provided to users; it can often be downloaded from the software maker's Web site.
<b>Server</b>	A computer program or system that provides services to other computer programs or systems
<b>Spoofing</b>	The forging of information used to identify a communication transmission (an e-mail header, e.g.) so that the message appears to have originated from someone or somewhere other than the actual source.
<b>University Network</b>	A series of devices and communication pathways that make up the campus computer and data communications infrastructure. This includes the campus Backbone Network, the local Area Networks, the Virtual Private Network, all Wireless Networks, and all equipment connected to those networks. It also includes all platforms (operating systems, such as DOS or Windows), all computer sizes (laptops, desktops and mainframes), and all application systems (including but not limited to <i>Oracle</i> , <i>Banner</i> and <i>Blackboard</i> ).
<b>Virtual Private Network</b>	A VPN is the use of telecommunication infrastructure to provide remote offices or individual users with secure access to the organization's network.
<b>Wireless Network</b>	A network in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.

## **Related Information**

---

[Application and System Access Policy](#)  
[Code of Conduct for Users of Computing Systems and Services](#)  
[Data Classification Security Policy](#)  
[GW NetID: Individual Accounts Policy](#)  
[Information Security Policy](#)  
[Local Support Partner \(LSP\) Policy](#)  
[Mobile Data Device Security Policy](#)  
[Security Breaches Involving Confidential Personal Information](#)

Computer Fraud and Abuse Act, 18 U.S.C. §1030

---

## **Appendices**

---

**Appendix A            Information Systems and Services Roles and Authority**

---

## **Who Approved This Policy**

---

Louis H. Katz, Executive Vice President and Treasurer

---

## **History/Revision Dates**

---

**Origination Date:**            June 4, 2003  
**Last Amended Date:**        November 19, 2008  
**Next Review Date:**         December 1, 2009

## **Appendix A**

### **Information Systems and Services Roles and Authority**

ISS is responsible for the design, operation and management of the computing and network communications services provided at the campus level. Responsibilities include the selection, purchase, setup and maintenance of all network equipment, the choice of protocols supported by the network, and the definition of campus standards necessary for efficient operation of the network or for the security of transmitted, stored and processed data and networked computers or other equipment.

#### **I. Network Design**

ISS has sole authority to purchase network equipment and to build and maintain the University's network infrastructure, except where ISS has delegated specific authority to a local network administrator for an area of the University. All systems and equipment connected to the network must be approved by ISS, including but not limited to switches, hubs, routers and wireless devices.

#### **II. Protocols**

A "protocol" is a set of rules used when exchanging information between points on a network or over the Internet. ISS shall dictate the protocols and services present on the University's network. At the present time the campus backbone universally supports the "Internet Protocol (IP) address." The University primarily uses Dynamic Host Control Protocol (DHCP) to dynamically assign IP addresses to workstations as needed. The DHCP is a communications protocol that lets network administrators manage centrally and automate the assignment of IP addresses in an organization's network. ISS also shall determine the specific routes that network traffic will take across the University.

IP addresses shall not be assigned from within the University IP address space for individuals or organizations that are not affiliated with the University. In requesting an IP address, each requesting person, organization, or service agrees to abide by all applicable University policies and agrees not to give access to the University networks (through their connected machine) to others who are not affiliated with the University.

#### **III. Domain Name Standards (DNS)**

A "domain" is a group of network addresses identified by a name. The Domain Name System translates internet domain names (for example "[www.gwu.edu](http://www.gwu.edu)") into the corresponding IP addresses (such as 128.164.127.251) for that site. Only ISS-approved domains may be operated within the University network address space. According to the University's Domain Name System Standards (refer to <http://dns.gwu.edu> for a detailed version of the DNS standards) all services that are provided by members of the University Community as part of their official functions and as part of the mission of the

## NETWORK USAGE AND SECURITY POLICY

institution will be registered within the “gwu.edu” domain. All services provided by members of the University Community that are not part of their official functions as members of the community or as part of the mission of the institution will be registered outside the gwu.edu or the gwumc.edu domain. Domain names outside gwu.edu will not be allowed on the University network (within the 128.164.x.x or the 161.253.x.x IP address ranges). Very rare exceptions may exist with approval from the Vice President and Chief Information Officer.

### **IV. Patchlink Usage**

Patchlink shall be used to provide and distribute vendor recommended security updates to GW owned PCs. Patchlink usage, outside of the normal distribution of security patches for PCs operated by university faculty members, must be approved by the Research and Instructional Technology Committee (RITC). Local Support Partners (LSPs) shall make use of Patchlink to provide security updates to PCs that they support including the support of PCs in the academic departments. In instances where ISS is contractually obligated to provide comprehensive desktop management to non-academic administrative departments and units, Patchlink shall be used to manage hardware and software in addition to security patch distribution. ISS shall train LSPs on the proper use of Patchlink.

ISS will not use Patchlink to deploy any application to PCs that do not have a support agreement for desktop management in place. Patchlink will not be used to examine user filenames or the content of data files on machines.

### **V. Management of Security Violations**

In the event ISS judges that a LAN, a network device, or an individual user presents an immediate security risk to the University network equipment, software, or data, ISS may terminate or restrict network connection without notice.

Attacks on the University network or systems are detected by University network and system administrators. Severe or ongoing attacks (such as an onslaught of unsolicited mail) may require that the source of the attack be blocked from the University network. ISS may block a specific network address, port or application in order to protect the University against attack, or take other action as it deems necessary.