Policy 64

Governors State University

Networking and Computing, Network Security, and Wireless Computing

1. Purpose

This policy is in effect for all users of University networking and computing resources. Governors State University (GSU) computing services are provided to support education, research and the public service mission of the University, and their use is limited to those purposes. This policy covers responsibilities of network users and those managing the network, addresses network security and provides the minimum guidelines for security, data security, and wireless computing on-campus.

2. Underlying Principles

Principles of academic freedom and the laws that govern "Fair Use" apply in full to electronic information and communications.

All users will comply with the Family Educational Rights and Privacy Act of 1974, as amended (FERPA), which affords students specific rights with respect to their educational records.

GSU's computing equipment, software and network access services are subject to applicable State, Local, and Federal laws.

3. Use of the GSU Network

All users of the GSU network are subject to the terms set forth in the GSU Acceptable Use Policy and any other computer policies in place at the University.
Individual campus units and departments that provide access to the GSU network are responsible for ensuring that use is consistent with University policies and contractual obligations governing the software and/or services offered on the GSU network.
The network may not be used for commercial or political purposes and may not be used by non-University entities, except as specified by contract.

4. Responsibilities of GSU Network Users

Users will use their University provided account(s) and network access primarily in conjunction with their University-related activities.
Any account owner who is logged into the GSU network is responsible for ensuring that the system is not used by any other individual through that account.

5. Responsibilities in Managing the GSU Network

a. **Resource consumption:** Any use of the GSU network that consumes so many resources as to noticeably degrade services to others will be reviewed by the administrator of the department where the problem is occurring and Information Technology Services (ITS). Exceptional measures, such as suspension of accounts

or lowering the service priority of the offending application may be initiated, if needed, to protect the quality of service to others.

b. **Websites**: All web pages must contain an electronic means by which users are able to contact an individual who is able to respond to messages concerning the page's content.
c. **Copyright:** Unauthorized materials and/or software in violation of copyright will be removed from the network. See the Policy on Fair Use of Copyrighted Material for additional information.
d. **Monitor network:** ITS in collaboration with other network administrators will monitor all use of the GSU networks.
e. **Violations and Appeal:** Suspected illegal activities will be investigated. Where GSU finds, there is reasonable evidence that University resources are being used illegally or contrary to University policy, ITS may limit or revoke access to the GSU network, network services, or campus computers. Individuals who have had their access limited or revoked, may appeal to the Information Technology Policy and Planning Council[1].
f. **Domains:** Only ITS approved and registered domains (see Glossary of Terms) may be operated within the GSU network address space.

6. Network Security

The following steps will be taken in response to security threats. Under these circumstances data normally considered private may be collected and examined by the designated ITS security officer and designated ITS administrators. The ITS security officer is the executive director of Information Technology Services.

a. **Security violation:** Any security violation that represents a significant misuse of University resources or violates GSU policies will be brought to the attention of the appropriate authorities.
b. **Security risks:** In the event that ITS judges that a Local Area Network (LAN), server, or system or any portion thereof, presents an immediate security risk to GSU, the network, or any system connected to the network, ITS may terminate or restrict the LAN's network connection without notice. If there is no immediate risk, ITS will bring the matter to the attention of the LAN's administrator. If the LAN's administrator is unable to resolve the problem ITS will contact the unit head.
c. **Account verification:** In the event that ITS judges that an account on one of its multi-user systems presents an immediate security risk, the designated ITS security officer may inactivate the computer account without prior notice.
d. **Scans:** ITS will occasionally scan computers connected to the GSU network for security vulnerabilities using a tool for that purpose. If a security weakness is detected the ITS designated security officer will secure all systems in a timely manner.
e. **Administrator of a server:** The administrator of a server or computer on the GSU network is responsible for the security of that system. The administrator of a

[1] Contact the Information Technology Policy and Planning Council in writing at Governors State University, 1 University Parkway , University Park, IL 60466.

server or computer is any individual in possession of the security rights of said server who can perform tasks to control user account creation, deletion, and changes; including the control of user access to applications and files on a particular server. A GSU network connected server or computer requires unique authentication (userid and password), when accessing protected information, such as but not limited to student information, University financial information, and employee information. The ITS security officer will monitor and log access information that could be useful in establishing the identity of individuals who use the system to breach network security.

f. **Publicly accessible computers:** Departments that operate publicly accessible computers connected to the GSU network must implement ITS approved safeguards against network abuse appropriate to the network access.
g. **Server access:** Any terminal server that grants network access through the phone system must authenticate each user, requiring at minimum a unique userid and password.
h. **Personal use responsibility:** The owner of private/personal equipment, e.g. a desktop, laptop or PDA (personal digital assistant) that is connected to the GSU network is responsible for ensuring that the system is not used by any other individual through his/her connection or account.
i. **Authorized use of software and hardware:** Software and hardware, which permits the capture and examination of GSU network packets, must be used only by authorized personnel. Constraints on the use of these tools include:
    i. Use only with the knowledge of the ITS security officer.
    ii. Only the minimum information required to solve the problem will be collected.
    iii. All data collected must be destroyed as soon as it has served its purpose.
j. **Confidentiality:** Information collected in response to a security threat must be considered confidential. No disclosure can be made without approval of the GSU General Counsel.
k. **Data collection:** Administrators of a server may log and monitor connections and user activity only of the servers they administer. This will be done only after obtaining appropriate administrative authorization or in response to an appropriate request to do so by a law enforcement agency.
l. **Departmental units:** Campus units that operate their own computers or networks may add, with the approval of the unit head, individual guidelines that supplement this policy.

7. Minimum Guidelines for Network Security

The following guidelines address minimum requirements and recommendations to decrease the opportunities for breach of network security.

a. **Antivirus:** All desktop computers will have the GSU version of antivirus software and will retain the setting that schedules regular updates of virus definitions from the central server.
b. **University computers:** When a university owned computer is configured, all operating system updates and patches will be applied. In addition, operating system updates and patches must be applied regularly. An automated setting to include checking for updates on a daily basis, is set as the default. Users should not change that setting.
c. **Server level security:** Whenever possible, security policies will be set at the server level and applied to the desktop machines.
d. **Login:** All campus desktop computers will have a mandatory network login. See the items below for additional information.
e. **Secure password:** The password will be a "strong" password, defined as:
    i. must be 6-8 characters in length
    ii. must include punctuation such as ! $ % & * , . ? + - =
    iii. must start and end with letters
    iv. must not include the characters # @ ' " `
    v. must be new, not used before
    vi. passwords expire every 65 days

f. **Firewall:** New machines will activate the built-in firewall. All other users will consider use of a free firewall.
g. **Known security breach:** All compromised machines will be completely rebuilt (i.e. erase the hard drive and reinstall from installation disks).
Microsoft IIS should not be installed or have its functions enabled .
h. **Recommended Guidelines**: ITS recommends a regular backup strategy in addition to the above minimum guidelines. It will be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will limit the damage caused by the loss of a machine.

8. Data Security

a. ITS is responsible for securing critical data as it travels across the network. The user must insure that every precaution is taken to secure data when moved from the network. Local or desktop storage of sensitive data is discouraged.
b. The transfer of any critical data directly from GSU server(s) or workstation to another device, which is not administered by an employee of GSU, can only be authorized with written permission by the ITS department.

9. Wireless Computing

Wireless networking uses the shared resource of the unlicensed radio frequencies to support the implementation of wireless access across campus.

The use of the campus wireless LAN shall be subject to the University policies and guidelines consistent with the wired network.

a. **Wireless service considerations:** The wireless network shall be viewed as augmenting the wired network, to provide more flexible network use. Applications that require large amounts of bandwidth, or are sensitive to changes in signal quality and strength may not be appropriate for wireless access.
b. **Sensitive data:** Wireless LAN will not be used to access student sensitive data unless the appropriate levels of encryption and tools as determined by ITS are used to secure the data transmission.
c. **Independent wireless network products:** Wireless networks are inherently less secure than wired networks. Only by proper implementation and operation can effective security be maintained. A network-wide approach should be taken to keep interference to a minimum, secure the campus wireless networks and insure the integrity of the campus computing systems connected to these networks. If individuals or units/departments deem it necessary to independently deploy wireless networking products, they must collaborate with ITS for implementations. ITS will work with any University department wishing to install wireless networking in their area.

10. Glossary of Terms

a. **Academic Freedom –** The freedom of the members of the university community to express their ideas in school without restrictions.
b. **Computing Services –** The facilities, computers, software and support materials that provide access to and support the services of the GSU network.
c. **Critical Data** - Critical data is defined as any and all data sets required in the execution of the university functions.
d. **Fair Use –** Under the "fair use" rule of copyright law, an author may make limited use of another author's work without asking permission. The fair use privilege is perhaps the most significant limitation on a copyright owner's exclusive rights.
e. **Family Educational Rights and Privacy Act (FERPA) –** The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.
f. **GSU Network –** The machines, servers, communication equipment and software that provide access to and compute information for the University.
g. **Registered Domain –** Computers connected together via the Internet are able to send information back and forth because each connected machine (often referred

to as a host) possesses a unique address. Each Internet Protocol (IP) address takes the form of four sets of numbers, separated by periods, or dots. The IP number system is coordinated by, and numbers are assigned under the authority of, the Internet Assigned Numbers Authority (IANA) which receives its charter from the Internet Society and the Federal Network Council. These IP numbers are long and hard to remember. They are what computers understand and use to route traffic on the Internet.

h. **Websites –** Websites are HTML/HTM documents, Internet web pages and documents that are viewable through browsers by accessing a domain name over the Internet.

Effective 2/02/06
Revised 9/25/06