Policy 64
Effective 2/02/06
Revised 9/25/06
Revised 4/25/16
Revised 03/28/18

Governors State University
Acceptable Use Policy for Computing and Networking, Network Security and Wireless Computing

I. PURPOSE

This policy is in effect for Governors State University (GSU) community using the University networking and computing resources. 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 GSU Community, addresses network security, and provides the minimum guidelines for security, data security, and wireless computing on-campus.

II. 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.

All users will comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

All users will comply with the Illinois Identity Protection Act (5 ILCS 179/1, et seq.).

All users will comply with the Illinois Personal Information Protection Act (815 ILCS 530/1).

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

III. USE OF THE GSU NETWORK

All users of the GSU network are subject to the terms set forth in this 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.

IV. 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.

V. 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 the Institutional Policy Committee.

F. **Domains:** Only ITS approved and registered domains (see Glossary of Terms) may be operated within the GSU network address space.

VI. 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 administrator.

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 administrator 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 administrator 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 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 (user ID and password), when accessing protected information, such as but not limited to student information, University financial information, and employee information. The ITS administrator 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 remote, internal or external, connection which grants network access, directly or indirectly, must authenticate each user against GSU's Network Directory Service whereupon at minimum a unique user ID and password is required.

H. **Personal use responsibility:** The owner of private/personal equipment, e.g., a desktop, laptop or other mobile device 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 administrator.
    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.

VII. 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 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 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. Minimum password length 8 characters long
   ii. Maximum password length 16 characters long
   iii. Cannot contain your account name or parts of full name
   iv. Must be a unique password going back 6 previous passwords
   v. Must contain one character from each of the following categories;
      1. Uppercase characters (A thru Z)
      2. Lowercase characters (a thru z)
      3. Numeric characters (0 thru 9)
      4. Non alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
   vi. Passwords expire every 180 days for employees and 180 students
   vii. Number of password incorrect attempts before lockout will be 5
   viii. Length of password log out time is 30 minutes of inactivity

F. **Firewall:** Access to GSU internal network is protected by network firewall technology in which may block inappropriate content or information, which might represent a risk to GSU.

G. **Known security breach:** All compromised machines will be completely rebuilt (i.e. erase the hard drive and reinstall). Any web-based operating system 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.

I. **Recommended Travel Guidelines**: Anyone taking any electronic devices that can store or communicate data, such as laptop computers, compact and portable storage devices, GPS systems, phones, mobile devices, and their associated software to another country should contact ITS staff to ensure devices are in a "clean" state as defined by federal regulation (U.S. Treasury Department's Office of Foreign Assets Control – OFAC).

VIII. 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.

IX. 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 network 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.

X. LAPTOP DATA ENCRYPTION

All laptop computers provided by GSU will be encrypted with data encryption technology in which will require a user to sign onto the laptop with his/her GSU network username and password. The data on the laptop's hard drive will be encrypted with a random security code generated at the time of encryption technology installation on the laptop.

XI. MOBILE DEVICES, REMOVABLE DEVICES, AND SENSITIVE DATA

Any GSU sensitive data in which might resided, either temporarily or permanent, on a mobile or removable device must be encrypted using GSU encryption technology or ITS approved encryption solutions. It is highly recommend that any sensitive data in computer files have file level encryption as well, thus providing addition security.

XII. EMAIL OR DISTRIBUTION OF SENSITIVE DATA

Communicating GSU sensitive data via email body, email attachments, file storage technologies, or device sharing technologies must be encrypted using GSU approved encryption technologies or application encryption methods. GSU sensitive data is to reside and be communicated between GSU provided devices. Storing GSU sensitive data on private/public computers, networks, or mobile devices is prohibited. If storing of Sensitive Data is required outside of GSU network or on a public/private device, a request can be made to Information Technology Services (ITS) for evaluation and approval of appropriate GSU management.

XIII. GLOSSARY OF TERMS

A. **Academic Freedom –** Academic freedom gives both students and faculty the right to express their views — in speech, writing, and through electronic communication, both on and off campus — without fear of sanction, unless the manner of expression

substantially impairs the rights of others.

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. FERPA link
F. **GSU Network –** The machines, servers, communication equipment and software that provide access to and compute information for the University.
G. **GSU Community** - Faculty, staff, students and guests of the University
H. **Health Information Portability and Accountability Act (HIPAA), also known as Public Law 104-191, –** HIPAA link
I. **Illinois Identity Protection Act (5 ILCS 179/1, et seq.), (IPA)** IPA link
J. **Illinois Personal Information Protection Act (815 ILCS 530/1), (PIPA)**PIPA link
K. **Mobile Devices** - Any device which is easily portable of which includes, but not limited to laptops, tablets, and smartphones.
L. **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 difficult to remember. They are what computers understand and use to route traffic on the Internet.
M. **Websites –** Websites are HTML/HTM documents, Internet web pages and documents that are viewable through browsers by accessing a domain name over the Internet.