Governors State
UNIVERSITY

Acceptable Use Policy for Computing and Networking (64)

Re-Approved by:	President Green	
History:	Issued 02/02/2006	
	Revised /11/06/2023	
	Last Reviewed – 05/06/2024	
Related Policies:	61, 75, 80, 88, 89, 91, 92	
Additional References:	N/A	
Policy Owner: **Contact Person:**	Information Technology Services – Director of Information Security	

I. Policy Statement

The GSU Network is provided to support education, research, and the public service mission of the University, and its use is limited to those purposes. This policy describes the base responsibilities required of GSU Network users.

II. Purpose

This purpose of this policy is to establish guidelines to support the usability, safety, and security of the GSU Network.

III. Scope

This policy is in effect for all users of the Governors State University (GSU) Network.

IV. Roles and Responsibilities

Individuals are required to comply with the components of this policy as applicable.

V. Credit and Source

This policy was developed internally.

VI. Definitions

A. **Individual -** Any person that accesses or consumes technology services (data, systems, printers, and other resources) provided by the University.

B. **GSU Network (the Network)** – The data, data storage, communication, and computing systems established, maintained, and or administered by the University.

C. **Security Risk** – Something that could compromise the confidentiality, integrity, or availability of University data.

D. **Application Owner** – The GSU individual or department responsible for a specific application.

E. **Server Administrator** – The GSU individual or department responsible for the operation and maintenance of a specific server.

F. **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.

G. **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.

H. **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.

Mobile Devices - Any device which is easily portable of which includes, but not limited to laptops, tablets, and smartphones.

VII. Policy

I. **ADHERENCE TO OTHER POLICIES**

All users must adhere to applicable university policies and procedures regarding the use and security of the GSU Network.

J. **LAWS AND REGULATIONS**

i. Individuals will comply with applicable laws and regulations. Examples include the following:

1. The Family Educational Rights and Privacy Act of 1974 (FERPA)
2. The Health Insurance Portability and Accountability Act (HIPAA) of 1996
3. The Illinois Identity Protection Act (5 ILCS 179/1, et seq.)
4. The Illinois Personal Information Protection Act (815 ILCS 530/1)

K. **INFORMATION SECURITY**

i. **Security Awareness Training** – Access to the Network will only be granted to individuals that have taken University-provided security awareness training within the previous 12 months. Access to the Network may be suspended if an individual fails to complete training within 12 months of the previous training.

ii. **Security Risks** - In the event of a suspected security risk, ITS may take appropriate action including revoking access to the Network. Suspected security risks may be investigated and reported to the appropriate authorities.

iii. **Compromised Devices** – Any device suspected of having its security compromised will be immediately removed from the Network and completely erased prior to being returned to service. Potentially compromised devices may also be forensically imaged and/or retained for additional investigation before being returned to service.

iv. **Confidentiality** – Data collected in response to a suspected or confirmed security incident is classified as 'restricted' under the GSU Data Classification Policy. No disclosure of this data can be made without the approval of the GSU General Counsel.

v. **Application Owner and Server Administrator Responsibilities –** Application owners and Server administrators are responsible for the security of the systems and data under their control and must follow all established rules to ensure the confidentiality, integrity, and availability of the information contained or processed therein.

L. **ACADEMIC FREEDOM**

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

M. **GSU NETWORK ACCESS**

i. 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.

ii. 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.

N. **REMOTE ACCESS**

i. Remote access to the GSU Network is provided as needed via a virtual private network (VPN). All VPN users must utilize their University-provided account and multi-factor authentication.

    ii. Remote access granted to third parties must be disabled when not actively used and must be actively monitored while in use.

O. **ACCOUNTS AND PASSWORDS**

    i. Except where not possible and explicitly authorized, access to any Network resource, server, application, and/or service must utilize the University's Single Sign-On service and multi-factor authentication.
    ii. Except where required for public access or otherwise explicitly authorized, access to the Network will require a unique account for each individual.
        1. The University will provide Individuals with an account for the purposes of accessing the Network in conjunction with their University-related activities.
        2. Accounts may not be used by anyone aside from the individual to which the account is assigned.
        3. Individuals must choose a password for their account. Password requirements are located in the Policy 64 Procedures document.
        4. Accounts will be temporarily locked after a certain number of incorrect authentication attempts.
        5. Passwords may not be shared or disclosed to others.

P. **RESOURCE CONSUMPTION**

Any use of the GSU Network that noticeably degrades services to others will be reviewed by 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.

Q. **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.

R. **DOMAINS**

Only ITS approved and registered domains may be operated within the GSU Network address space.

S. **MONITORING AND SCANNING**

To ensure security, availability, and compliance with policies, procedures, laws, and other regulations:

    i. Network and system activity may be logged and monitored.
    ii. Devices connected to the Network may be scanned for enumeration and vulnerability management.

T. **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).

U. **DATA SECURITY**

i. All University owned laptops and mobile devices must be encrypted using approved encryption technology.
ii. Non-public University data must be encrypted during transmission.
iii. Non-public University data may not be stored on unencrypted removable media.
iv. Non-public University data may only be stored or processed on devices, storage media, or services owned or explicitly authorized by the University.
v. The transmission of non-public University data to third parties is prohibited unless explicitly authorized by the University.
vi. The use of unauthorized applications and third-party service providers to store or process non-public University data is prohibited.

V. **UNAUTHORIZED WIRELESS NETWORKS**

Wireless Networks implemented and/or maintained by departments or individuals are not permitted.

W. **VIOLATIONS AND APPEALS**

Suspected unauthorized activities will be investigated and ITS may limit or revoke access to the GSU Network. Individuals, who have had their access limited or revoked, may appeal the Institutional Policy Committee.