Area:	Basic Policies and Appointment	Number:	2050
Subject:	Information Technology Appropriate Use Policy	Issued:	11/11/2010
Applies To:	Faculty and Staff	Revised:	
Sources:	USG Board Policy	Page(s):	1 of 8

I. Purpose

This Information Technology Appropriate Use Policy is authorized by the Board of Regents, Appropriate Use Policy (2009-014) which charges each University System of Georgia institution to develop policy that, at minimum, includes the Board policy guidelines. These guidelines establish that the institution and its users have an obligation to abide by the following standards of appropriate and ethical use:

- Use only those IT resources for which you have authorization
- Protect the access and integrity of IT resources
- Abide by applicable local, state, federal laws, university policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted material
- Use IT resources only for their intended purpose
- Respect the privacy and personal rights of others
- Do no harm

Therefore, the following Information Technology (IT) Appropriate Use Policy statement (AUP) defines acceptable technology and information use practices, promotes an understanding of responsible use of university IT resources, seeks to protect the University's IT resources, and preserves the relevant policies, regulations and laws. The policy is not intended to be exhaustive, and Georgia Southern University reserves the right to limit, restrict, or extend privileges and access to its information technology resources.

II. Policy Statement

In support of its mission of teaching, scholarship, and service, Georgia Southern University provides access to IT resources for students, faculty, staff, and other authorized users within institutional priorities and financial capabilities. The IT resources of Georgia Southern University, including but not limited to, facilities, hardware, software, networks, data, information, and user accounts are the

property of the State of Georgia. The use of these resources is a privilege granted by Georgia Southern University to authorized users only.

This AUP incorporates all applicable policies and regulations of the Georgia Southern University and the University System of Georgia as they related to administration, instruction, research and scholarly pursuits, including but not limited to, the Information Technology Security Standards and Guidelines, the Intellectual Property Policy, the Misconduct in Research, and prior Institutional approval through the University's Institutional Review Board for surveys and other projects utilizing human subjects.

Georgia Southern University requires all persons authorized to use its IT resources to do so responsibly and in compliance with all local, state and federal laws, all contractual and license agreements, and all policies of Georgia Southern University and the Board of Regents of the University System of Georgia. Authorized users of the University's IT resources must act responsibly to maintain the integrity and security of these resources.

Each user of a university IT resource is ultimately responsible for the use of that resource and for the use of his or her access credentials. Persons violating this AUP are subject to disciplinary actions by the University including, but not limited to, forfeiture of their privileges.

In the event that misuse of IT resources threatens to compromise the integrity or jeopardize the security of university resources or harm authorized users of those resources, the University's Chief Information Officer, or his or her designee, is authorized to take any and all necessary actions, including the immediate confiscation and/or disabling of a university resource or the temporary or permanent termination of user access credentials, to protect, investigate, and ensure the security and proper use of IT resources.

All of Georgia Southern University IT resources and network facilities are subject to the provision of the Georgia Open Records Act, O.C.G.A. Sections 50-18-70 *et seq*. Therefore, users of University IT resources shall have no expectation of privacy of materials stored on or transmitted by University IT resources. The University cannot and will not guarantee the privacy or confidentiality of computer files, electronic mail, or other information stored or transmitted by its IT resources. The University reserves the right to access and examine any of its IT resources or devices attached to the University network upon reasonable belief that federal or state laws have been violated, where the University's contractual obligations or its operations may be impeded, to preserve the integrity of the system, to cooperate with internal investigations, in compliance with lawfully issued subpoenas or civil discovery, and in cases of emergency.

Students, employees and service providers are required to affirm their recognition of this policy at the beginning of their relationship with the University and periodically thereafter as determined by the Chief Information Officer.

III. User Responsibilities

The use of IT resources is granted based on acceptance of the following specific responsibilities:

1. **Use only those computing and IT resources for which you have authorization.**

    a. Misrepresenting a person's identity or relationship to the University when obtaining access privileges or using technology is prohibited.

    b. Use of any university information technology resource is restricted to those having proper authorization to use that particular resource. It is a violation of the law and university policy to assist in, encourage, or conceal from authorities any unauthorized use, or attempted unauthorized use, of any of the University's computers or network facilities.

    c. Passwords to any information technology resource shall only be issued to authorized users. Password recipients are responsible for the protection of their access credentials (passwords) and shall not distribute them to other users.

    d. Only those persons with proper authorization shall modify or reconfigure any university information technology resource or network facility.

2. **Protect the access and integrity of computing and IT resources.**

    a. Accessing, reading, altering, or deleting information or data of any kind without authorization is prohibited.

    b. Users must take appropriate steps to secure protected, confidential and sensitive information including personal identifying information such as social security numbers and birth dates.

    c. No person shall circumvent or attempt to circumvent any system, resource limits, access procedures, or security regulations established by the Chief Information Officer or his or her designee.

    d. Only authorized devices shall be connected to the University network and no device shall be connected to the University's network or otherwise used in a manner that interferes with the authorized use of university resources. The University reserves the right to restrict the use of any technologies that may endanger the security, integrity or fair use of its information technology resources.

e. The University's information technology resources shall not be used to attempt unauthorized use, or to interfere with another person's legitimate use, of any computer, network facility or other technology resource.

f. All computers that utilize campus network resources must have approved antivirus software that utilizes current virus definition files. These computers include all University owned computers and all computers owned by faculty, students and staff that are used on the campus networks. The removal, modification, or disabling of antivirus software on University owned computers without written consent by the Chief Information Officer or his or her designee is prohibited.

g. Third-party, hosted services or systems operated on behalf of the University must meet University security guidelines and provide assurances that the protection of University information assets conforms to institutional standards, Board of Regents policy, Federal and State laws.

h. Users have an obligation to report suspected violations of this policy. Reports should be directed to a University official such as the Information Technology Services Security Administrator, University Auditor, University Police or the head administrator of the unit responsible for the particular system involved. Reports may also be provided to the Ethics and Reporting Hotline at: http://services.georgiasouthern.edu/internalaudit/contact.php

3. **Abide by applicable laws and USG policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.**

a. Copying, installing, distributing, infringing, or otherwise using any software, data, images, video, text, or other materials in violation of copyrights, trademarks, service marks patents, other intellectual property rights, contracts, or license agreements is prohibited.

b. All use of information technology resources shall be in compliance with federal and state copyright laws and in full conformance with the Georgia Regents Guide to Understanding Copyright and Fair Use.

4. **Use computing and IT resources only for the intended purposes.**

a. University information technology resources shall not be used for commercial purposes without specific authorization from the Vice President for Business and Finance or his or her duly authorized designee.

b. All technology use shall be in full compliance with all provisions of the Campus Advertising, Sales and Solicitation Policy and Financial Transaction Policy.

c. University information technology resources shall not be used for personal political gain or as a vehicle of election to a public office.

5. **Respect the privacy and personal rights of others.**
   a. Authorized users shall take full responsibility for messages that they transmit through the University's information technology systems. The University's information technology resources shall not be used to transmit or participate in any communications prohibited by law, including but not limited to fraudulent, harassing, obscene, or threatening messages.

   b. It is a violation of this policy to tap a phone line or run a network sniffer or vulnerability scanner without authorization of the CIO.

   c. It is a violation of this policy to access, attempt to access or use another person's access credentials or data without explicit authorization of the CIO.

   d. It is a violation of this policy to access or copy another user's electronic mail, data, programs, or other files without explicit authorization of the CIO.

   e. The unauthorized disclosure of information about employees or students is prohibited.

   f. Users should use only those systems officially licensed or sanctioned by the University. Users are cautioned about using free software or social internet sites for conducting University business. There are substantial risks to the privacy and protection of information on such sites.

6. **Do no harm.**
   a. Technology shall be disposed of according to established procedures. No technology shall be implemented, used or disposed of in such a way that causes harm to persons or animals, or violates environmental protection laws.

   b. Technology used in research will conform to conditions of institutional approval through the University's Institutional Review Board for projects utilizing human and animal subjects.

   c. Persons shall not create, install, or knowingly distribute a virus, key logger, malware or other surreptitiously invasive program on any university information technology facility.

IV. Information Technology Administrators and Technician Responsibilities

Information technology administrators and technicians are granted significant privileges and trust to use their authorization appropriately for the intended purpose of establishing and maintaining the operation and integrity of IT resources. As such, system Administrators and technicians have the additional responsibility of protecting the confidentiality, integrity, and availability of the resources they are managing or servicing. These additional responsibilities include, at a minimum:

1. System administrators and technicians shall respect the privacy of others to the extent allowed by law and University policy. Any private information seen or otherwise obtained in carrying out duties must be treated in the strictest confidence, unless it relates to a violation of policy, law or threatens the security of IT resources.

2. System administrators and technicians shall immediately refer all violations of policy or law to appropriate authorities.

3. System administrators and technicians shall cooperate at all times with University Police, University Auditor, Environmental safety officers, the Associate Vice President for Legal Affairs, the IT Services Security Officer, and the Chief Information Officer.

V. Sanctions:

Violation of the University's Information Technology Appropriate Use Policy may result in loss of information technology privileges and other disciplinary action. Some violations may constitute criminal offenses, and in such cases, the University will carry out its responsibility to report such violations to the appropriate authorities. Nothing in this policy is intended to limit the authority of supervisors to impose disciplinary sanctions on employees.

Policy violations will be classified as major or minor by the Information Technology Services Security Administrator or the Chief Information Officer, with the approval of the appropriate vice president or their designee.

1. First or minor violations

Violations of this policy that are deemed minor may be dealt with by the Chief Information Officer or within the appropriate department if the violator has not committed prior violations of the policy. Violators will be notified of the nature of the violation and advised how to reestablish compliance with the policy.
For violators who are employees, a description of the violation and a copy of the incident report prepared by Information Technology Services will be sent to the employee's immediate supervisor and the appropriate vice president or their designee. For violators who are students, a description of the violation and a copy of the incident report will be sent to the Dean of Students, Office of Judicial Affairs.

2. Subsequent or major violations

Violations that are deemed major and violations involving violators who have previously violated the Appropriate Use Policy (including prior versions of the policy) will be referred to the appropriate vice president for imposition of sanctions in accordance with Human Resource policies, which for employees could include termination of employment. Sanctions are imposed against student violators for subsequent or major violations in accordance with the Student Conduct Code.

Violators will be notified of the nature of the violation and advised how to reestablish compliance with the policy. In addition, violators will receive a copy of the Appropriate Use Policy and any other policy violated, and will be required to certify in writing that they have read and understand the policies, and agree to abide by the policies in the future.

VI. Responsible Office:

This Information Technology Appropriate Use Policy shall be administered and enforced by the University's Chief Information Officer or his or her duly authorized designee.

VII. Definitions:

Information Technology Resource - Information technology resources comprise all computers and electronic data storage, transmission, and manipulation devices owned and/or controlled by any part of Georgia Southern University or connected to the University's communication facilities, including departmental computers and the University's information technology network facilities accessed by anyone from anywhere.

Authorized Use - Authorized use of Georgia Southern University information technology resources is use of computer resources that is consistent with the education, research, and service mission of the University and consistent with this Appropriate Use Policy.

Authorized User – An Authorized user is:

1. A person who has truthfully identified themselves and to whom access credentials have been granted to Georgia Southern University IT resources; or
2. any person connecting to a public information service operated by Georgia Southern University.

Sensitive Information – All information that should remain private as designated by the University including, but not limited to educational records, social security numbers, credit card numbers, bank-related information, and health-related information.

Technicians – Employees who have the responsibility of maintaining, configuring, and repairing desktop and laptop computing resources.

System Administrators – Employees who have the responsibility of configuring and maintaining servers and systems used by authorized users.

IX. Publication:

1. This policy will appear in the student handbook and other appropriate publications accessible to student readership.

2. This policy will appear in employee handbook and other appropriate publications available to employees.

X. Revision history: Adapted from Computer Use Policy July, 28, 2010
Approved by Presidents Cabinet on 11/11/2010.