

# Georgia Southern University

## Computer Use Policy

**Effective Date: 6/08/2006**

**Last Revised: 5/18/2006**

**Status: Approved**

### **I. Purpose**

The following Computer Use Policy has been developed as a complement to relevant laws and policies to define acceptable and unacceptable computer use practices, to promote an understanding of responsible usage of university computing resources, and to protect and conserve those computing resources. The policy is not intended to be exhaustive, and Georgia Southern University reserves the right to limit, restrict, or extend computing privileges and access to its computing resources.

### **II. Policy Statement**

In support of its mission of teaching, scholarship, and service, Georgia Southern University provides access to computing resources for students, faculty, staff, and other authorized users within institutional priorities and financial capabilities. The computing resources of Georgia Southern University, including facilities, hardware, software, networks, and computer 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. Georgia Southern University requires all persons authorized to use its computing resources to do so responsibly and in compliance with all 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 computing resources must act responsibly to maintain the integrity and security of these resources. Each user of a university computing resource is ultimately responsible for the use of that computing resource and for the use of his or her computer account. Persons misusing the University's computing resources in violation of federal and state laws, Board of Regents and university policies, or this policy are subject to disciplinary actions by the University and/or forfeiture of their computer privileges. In the event such misuse of computer resources threatens to compromise the integrity or jeopardize the security of university computer 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 computer resource or the temporary or permanent termination of a computer account, to protect, investigate, and ensure the security and proper use of computer resources.

1. Use of any university computing 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 attempt an unauthorized use, of any of the University's computers or network facilities.
2. No one shall knowingly endanger the security of any university computing resource, nor willfully interfere with authorized computer usage by circumventing or attempting to circumvent normal resource limits, logon procedures, or security regulations. Furthermore, use of all university computing resources shall be subject to all provisions of the Georgia Southern University Information Technology Security Standards and Guidelines, which are incorporated by reference as part of this Computer Use Policy.
3. No technologies shall be connected to the University's computing resources that interfere with authorized usage of those resources. The University reserves the right to restrict the use of any technologies that may endanger the security and/or integrity of its computing resources. See the Information Technology Security Standards and Guidelines.
4. The University's computing resources shall not be used to attempt unauthorized use, or to interfere with another person's legitimate use, of any computer or network facility anywhere. All users shall share computing resources in accordance with policies set for the computers involved, giving priority to more important work and cooperating fully with the other users of the same equipment. Encroaching on or disrupting another person's use of university computers is prohibited. Examples of such acts include but are not limited to: excessive game playing; sending excessive messages either locally or off campus [including but not limited to electronic chain letters]; initiating denial of service attacks; printing excessive copies of documents, files, data, or programs; modifying system facilities, operating systems, or disk partitions; attempting to crash or tie up a university computer; damaging or vandalizing university computing facilities, equipment, software, or computer files; causing an inordinately large number of requests for files; spamming; sniffing; running scans; reconfiguring; or using an inordinately high percentage of bandwidth.
5. University computing resources and network facilities 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. All computer usage shall be in full compliance with all provisions of the Campus Advertising, Sales and Solicitation Policy and the web-based Financial Transaction Policy.
6. Passwords to any computing resource shall only be issued to authorized users. Password recipients are responsible for the integrity of their password and shall not distribute it to unauthorized users.

7. Misrepresenting a person's identity or relationship to the University when obtaining or using university computer or network privileges is prohibited.
8. Accessing, reading, altering, or deleting any other person's computer files or electronic mail without specific authorization is prohibited.
9. Copying, installing, distributing, infringing, or otherwise using any software, data files, images, text, or other materials in violation of copyrights, trademarks, service marks patents, other intellectual property rights, contracts, or license agreements is prohibited. All usage of computing resources shall be in compliance with federal and state copyright laws and in full conformance with the Regents Guide to Understanding Copyright and Fair Use.
10. Creating, installing, or knowingly distributing a computer virus, "Trojan horse," or other surreptitiously destructive program on any university computer or network facility, regardless of whether any demonstrable harm results, is prohibited.
11. Only those persons with proper authorization shall modify or reconfigure any university computing resource or network facility.
12. Users of university computing resources shall have no expectation of privacy of materials stored on those resources. The University reserves the right to access any of its computer resources when federal or state laws or university policies may have been violated or where university contractual obligations or university operations may be impeded or when deemed in the best interest of the University. Computer users should not place confidential information in computers without protecting it appropriately. The University cannot and will not guarantee the privacy or confidentiality of computer files, electronic mail, or other information stored or transmitted by its computers. All computer usage on Georgia Southern University computing resources and network facilities is subject to the provisions of the *Georgia Open Records Act, O.C.G.A. §§ 50-18-70 et seq.*
13. Authorized computer users shall take full responsibility for messages that they transmit through the University's computing resources. The University's computing resources shall not be used to transmit any communications prohibited by law, including but not limited to fraudulent, harassing, obscene, or threatening messages.
14. System administrators shall perform their duties fairly, in cooperation with the Georgia Southern community, their administrative supervisors, university policies, and funding sources. System administrators shall respect the privacy of others to the extent allowed by law and University policy. System administrators shall refer all disciplinary matters to appropriate authorities.

### **III. Sanctions:**

Violations will be classified as major or minor based on the following considerations:

- Intent of the person committing the violation
- Sensitivity of resource compromised
- Effect on the University community

Based on these considerations, the following example situations would be classified as major violations (these are not all-inclusive):

1. An intentional hack into a campus server.
2. A weak password in a user account that has access to social security numbers, medical information, credit cards, or other data classified as sensitive.
3. A failure to update a server's operating system that results in a denial of service attack that brings down the entire campus network.

Classification of a violation will be proposed by the Information Technology Services Security Administrator and/or the CIO, and approved by the appropriate Vice President.

### **First /minor violation**

If a person has violated the Computer Use policy or Security Standards Policy, and (1) the violation is deemed minor by IT Services, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the IT Services or department level. The offender will be notified of the offense and how to come back into compliance with the University's policy. The offender will also be furnished a copy of the Computer Use Policy and the Security Standards Policy, and will sign a form that indicates the person has read the two policies and agrees to conform to the policies.

An e-mail that includes a description of the violation and a copy of the incident report will be sent to the employee's immediate supervisor and their respective Vice President. For students the Vice President of Student Affairs and the Office of Judicial Affairs will be notified with a description of the violation and a copy of the incident report.

### **Subsequent and/or major violations**

The offender will be notified of the offense and how to come back into compliance with the University's policy. The offender will also be furnished a copy of the Computer Use Policy and the Security Standards Policy, and will sign a form that indicates the person has read the two policies and agrees to conform to the policies.

Reports of subsequent or major violations will be forwarded to the employee's Office of the Vice President for the determination of sanctions to be imposed. For staff employees, consult the Office of Human Resources regarding appropriate action or See Human Resource's policy on Counseling and Disciplinary Action:

<http://jobs.georgiasouthern.edu/p&p/Counseling%20and%20Disciplinary%20Action.htm>

For Faculty employees, see the Faculty Handbook:

<http://academics.georgiasouthern.edu/provost/handbook/facultyhandbook.pdf> .

For students, the Vice President of Student Affairs and the Office of Judicial Affairs will be notified of the violation for determination of sanctions to be imposed.

### **Range of disciplinary sanctions**

Use of Georgia Southern University computing resources in violation of the University's Computer Use Policy and the Security Standards and Guidelines Policy may result in loss of computing privileges and other disciplinary action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Security Act, the Copyright Act, and other local, state, and federal laws; 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.

### **IV. Responsible Office:**

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

### **V. Definitions:**

Computing Resource Computing 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 computing network facilities accessed by anyone from anywhere.

Authorized Use Authorized use of Georgia Southern University computing resources is use of computer resources that is consistent with the education, research, and service mission of the University and consistent with this Computer Use Policy.

Authorized User Authorized users are as follows:

1. current faculty, staff, and students of Georgia Southern University;
2. any person connecting to a public information service housed on a computing resource; and
3. others whose access furthers the mission of the University and whose usage does not interfere with other users' access to computing resources.

Each user of a computing resource must be specifically authorized to use that particular computing resource by the university unit responsible for maintaining and operating the resource.

Revision history: 2/22/2006  
3/07/2006  
5/16/2006  
5/18/2006