

Mathematics Department Computer Use Policies

Purpose of the Policy

The following departmental Computer Use Policies have been developed as a means to emphasize and enforce the existing university policies that can be located via the web at: <http://academics.georgiasouthern.edu/provost/policies/computeruse.html>. All departmental Faculty and Staff are required to read Georgia Southern's "Computer Use Policies", "Information Technology Security Standards and Guidelines", and the "Incident Response Procedures". Full compliance at the departmental level is mandatory.

Policy Statement

The senior administrative staff of Georgia Southern University have read and approved the computing policies that were set forth by the University's IT Services. These policies are not voluntary. The Mathematics Department will operate within the requirements and guidelines of existing university policies pertaining to the usage of university computing resources. It is at the discretion of the department chair to determine when it may be necessary to add to the existing university policies, but at no time will the department circumvent or otherwise diminish the authority or direction of university policy. The chair, as well as the departmental administrators, will work in unison with the university's IT Services to ensure that the university's computing policies, standards, and procedures are strictly enforced at the departmental level.

1. The computing resources of Georgia Southern University, including facilities, hardware, software, networks, and computer accounts, are the property of Georgia. The use of these resources is a privilege granted by Georgia Southern University to authorized users only.
2. Under no circumstances should personal passwords be shared. If passwords must be written down in order to be remembered, the document should be kept on one's person, such as in a wallet or purse. Passwords should also be changed on a monthly basis. Some advice for selecting "strong" passwords; use at least 8 characters, use a combination of upper and lowercase letters, include some punctuation characters (&*^%\$#@><:"',etc), ensure the password is not in the dictionary (all languages), do not use simple patterns (123456, abcde, 112358, etc.), and do not base your password on personal information (your name, birth date, pet names, address, etc.). Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

3. It is ultimately the responsibility of the individual computer user to ensure that their office computer's operating system and anti-virus software is kept up to date. In the event that a faculty or staff member is not familiar with the process, the departmental administrators can be called on for assistance and will make every attempt to ensure that the end user is familiar with the correct procedure to guarantee that all software is kept up to date. The campus policy concerning software updates is to perform the process monthly. The departmental policy concerning updates is to perform the process daily. This is easily achieved by using the automatic update features contained within Windows 2000, Windows XP, and Symantec Anti-Virus CE. The entire process can be done with no participation from the end user. Once again, if a faculty or staff member is not familiar with the procedure of updating system software, a departmental administrator should be contacted.
4. 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. 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.*
5. In the event that a computer resource threatens to compromise the integrity or jeopardize the security of University computer resources or harm authorized users of those resources, the departmental administrators will work with IT Services 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. In the event that it is deemed necessary to confiscate a computer resource, the user of that resource will have the option of directing departmental administrators in the copying of crucial data from that resource before it is presented to IT Services for further investigation. This will only be done if the copying of data will not hinder further investigation of the resource. A temporary replacement of the confiscated resource will then be supplied for the faculty or staff member to continue work.
6. No technologies shall be connected to the University's computing resources that interfere with authorized usage of those resources. These technologies include, but are not limited to: hubs, switches, access points, etc. Prior approval from IT Services must be obtained in order to use these devices. These devices accomplish something practical, but they can hinder network

performance if not used properly. For instance: a hub connected to another hub can cause substantial amounts of unnecessary traffic and hinder overall network performance. Although a switch alleviates the hub's broadcasting effect, prior approval must be obtained before using these types of devices. 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.

7. 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.
8. 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.
9. 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 shall refer all disciplinary matters to appropriate authorities.

Responsible Office:

This Computer Use Policy shall be administered and enforced by the Department Chair or his or her duly authorized designee.