Georgia State University Policy

7.20.05 Information Systems Ethics

View Archive

Policy Summary

Georgia State University's information system resources shall be made available only for appropriate uses, and will be used in a manner that protects both personal privacy and equitable availability across the university.

Full Policy Text

Georgia State University´s information system resources shall be made available only for appropriate uses, and will be used in a manner that protects both personal privacy and equitable availability across the university.

Administration of Policy

Mandating Authority:
None Identified

Responsible Office(s):
Information Systems and Technology, 13th floor, Commerce Building, 3-4357

Responsible Executive(s):

Policy History

Approving Body: Administrative Council

Rationale or Purpose

In order to further the university's academic, research and service missions, a quality computing environment must be maintained. This environment ensures availability and equitable distribution of resources across the campus. Limited resources should not be used for purposes that are not directly related to the business of the university nor should they be used in a manner that would violate the personal privacy of faculty, staff or students associated with the university.

Additional Information

Standards Appropriate Use. Appropriate use of information systems is that which supports the university´s objectives of teaching, research and extension of knowledge to the public. Guidelines for the appropriate use of information systems: a) Users shall not provide network or

computer-based services using university information systems without prior written approval and registration

b) Users shall not use information systems for non-university business

c) Users shall not use information systems to engage in harmful activities; such activities include, but are not limited to, Internet Protocol (IP) spoofing, creating and/or propagating viruses, port scanning, disrupting services, damaging files, purporting or representing one´s self as someone else, or intentional destruction of or damage to equipment, software or datad)

d) Users shall not impede, interfere with, impair or otherwise cause harm to other users´ legitimate use of information systems

e) Users shall not use information systems in such a way that violates local, state or federal laws, including copyright laws

f) Users shall be responsible for ascertaining that the use of information systems complies with all university policies

g) Users shall not use information systems in such a way that violates the University´s contractual obligations, including limitations defined in software or other licensing agreements

h) Users shall not use information systems to transmit communications that are fraudulent, defamatory, harassing, obscene, threatening, that unlawfully discriminate or that are prohibited by law

i) Users must comply with the regulations and policies of newsgroups, mailing lists and other public forums through which they disseminate their messages and comments

j) Users shall not perform security scanning, probing or monitoring services without appropriate permission.

University Access to User´s Information (Privacy).

University access to a user´s information systems includes any access by the university to approach, enter, or make use of the information stored on the university´s information systems. To the extent permitted by law, the university seeks to preserve an individual´s information or data from unsanctioned intrusion. Electronic and other technological methods must not be used to infringe upon a user´s privacy.

Guidelines concerning access to user information:

a) The university seeks to preserve individual privacy and does not routinely monitor individual usage; however, the university may in accordance with state and federal law, access and monitor information systems when:

1) Users have voluntarily made them accessible to the public 2) It reasonably appears necessary to do so to protect the integrity, security or functionality of the university or to protect the university from liability 3) When necessary for the normal operation and maintenance of the information systems, or to identify or diagnose systems or security vulnerabilities and problems 4) There are reasonable grounds to believe that a violation of law or a significant breach of university policy may have occurred 5) An account appears to be engaged in unusual or unusually excessive activity as indicated by monitoring of general activity and usage patterns 6) It is required by federal, state or local law or administrative rules.

Any such access, other than what is made accessible by the user, required by law or necessary to

respond to emergency situations, must be authorized in advance by the Provost, the Associate Provost for Information Systems and Technology, or the Office of Legal Affairs. Depending on the circumstances, the university will make a reasonable attempt to notify the user of any such action.

b) Users understand that by attaching personal computing devices to the University information systems, they consent to the university´s monitoring of their information systems for maintenance and security purposes

c) Electronic mail messages are not secure and therefore should not be assumed to be private

Policy originally approved and made effective by Administrative Council January 2003

Additional Helpful Resources

Request Authorization to Probe or Monitor University Information Systems
Request Authorization to Access Users´ Information