Georgia State University Policy

7.20.07 Minimum Information Security Environments and Data Classification

Policy Summary

The university has both the right and the obligation to manage, protect, secure and control the electronic information resources of the university.

Full Policy Text

The university has both the right and the obligation to manage, protect, secure and control the electronic information resources of the university.

Administration of Policy

Mandating Authority:
Administrative Council

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

The Associate Provost for Information Systems and Technology, as Chief Information Officer, is responsible for ensuring that Georgia State University has adequate information security in order for systems and data to be available for appropriate purposes. The basic standards and guidelines described in this policy provide for the minimum acceptable environment for operating and accessing information systems.

Additional Information

Standards
**Authorized Access to Information Systems (Accounts)** Authorized access to the university’s information systems is the granting of authority to approach, enter, make use of, and exit the university’s information systems. Access is accomplished via an account, which is a record kept by operating systems for each authorized user of information systems for the purpose of identification, administration and security. Users are required to obtain proper authorization prior to accessing the university’s information systems.

Guidelines establishing eligibility to receive authorized access:

a) Every university employee or student eligible to register may be granted access to university information systems
b) Users shall not be granted access in excess of the level required to perform their job responsibilities
c) Individuals providing services to the university may with appropriate authorization be granted access to university information systems
d) Users shall not misrepresent their identify or relationship to the university when accessing the information systems
e) Users shall not access information systems that they are not authorized to access.

**Configuration for Network Connection** Configuration refers to the version of operating system that is installed on your workstation, desktop or laptop computer. As each operating system version may handle other applications in a different manner, users must ensure that they check the current procedure for securing each device to determine the correct accompanying versions of networking software, e-mail, AntiVirus and VPN client needed for access to the Georgia State Network. Users should be aware that a local decision to continue use of a non-supported version of operating system could result in denial of network connection due to increased risk of new security holes that will not be addressed by the software vendor.

**Passwords and Userids (Authentication Methods)** A userid and password is one method (and the one most commonly recognized by the average user) of authentication. A userid is the name by which the person is known and addressed on the University’s information systems. The password used in conjunction with the userid is a unique string of characters that a user enters as an identification code. Users must follow standards for creating passwords as defined in the "Create or Change a Password" document (see link in Procedures section). Other recognized forms of authentication include, but are not limited to, smart cards, swipe cards, one-time passwords, digital signatures, and/or digital keys and biometrics. Users must have a valid method of authentication before they will be authorized to access the information systems.

Guidelines regarding the use of userids and passwords:

a) Users must not use accounts or passwords that they have not been authorized to use, or have not been assigned to them
b) Users shall not give passwords to unauthorized users
c) Users shall not share userids and passwords
d) Users must effectively control the creation, use and maintenance of passwords in order to prevent unauthorized access and destruction, modification or deletion of sensitive data
e) Users are responsible for securing their passwords from inadvertent disclosure
f) Users are responsible for any activity carried out under their account identification.

**Secure Disposal or Re-use of Information Systems Equipment** Prior to disposal or re-use, equipment containing storage media should be cleansed to prevent unauthorized exposure of data. Disposal of equipment shall be done in accordance with all applicable state or federal surplus property and environmental disposal laws, regulations or policies.

**Software Licensing** Valid licenses are required for each end user for all commercially developed software operating on systems used by that user. Responsibility for centrally managed and distributed software lies with IS&T. Colleges and operating departments are responsible for approving and retaining documentation on software (other than centrally managed) installed on devices within their areas of responsibility. As a minimum, colleges and operating departments
should be able to show original licensing materials (packaging, hologram software seal, authorization codes, etc.), date of installation and serial number of equipment (or Georgia State University inventory number) that the software was installed on. Colleges and operating departments are responsible for developing and managing their own procedures for collecting and maintaining licensing records.

**Physical Security** Physical security refers to the protection from harm or loss of the pieces of equipment that constitute an information system environment or personal computing device. Information systems must be safeguarded in a way that minimizes the risk of abuse, theft and destruction.

Guidelines regarding physical security: a) Users must implement appropriate protection measures including physical barriers, environmental detection and protection, insurance and/or other risk management techniques b) Users must not leave mobile computer systems unattended for extended periods of time and shall utilize locking devices responsibly c) Users shall protect information systems by utilizing protective measures such as locked screens and password-protected screen savers

**Securing University Information Systems** Securing systems refers to the protection of a computer system and its data from harm or loss, particularly the prevention of access by unauthorized individuals. Users are responsible for properly securing their information systems.

Guidelines for securing systems: a) Users shall not knowingly defeat or attempt to defeat the security of information systems b) Users must take reasonable precautions in ensuring that they do not disseminate viruses and malicious programs to other users c) Users must configure University mail servers to prevent them from being used as third party mail relays d) Users are responsible for monitoring the security of their own information systems e) Users who are permitted to provide network or computer-based services are required to take reasonable precautions to ensure that information systems being used for this purpose are not compromised or used by unauthorized users; see the Sensitive Information Protection Policy for guidelines

**University Information Security Officer (ISO)** The Information Security Officer (ISO), as designated by the Associate Provost for Information Systems and Technology, has responsibility for developing and publicizing university information security policies as well as monitoring compliance with those policies and all applicable laws, rules and regulations. The ISO coordinates the standards, procedures and guidelines necessary to administer access to university information resources. The ISO works in conjunction with information resource owners, the university data administrators and functional users to develop this material.

Contact the Responsible Office for procedures.

Policy originally approved and made effective by Administrative Council January 6, 2004

**Additional Helpful Resources**