

Morgan State University
COMPUTER AND INFORMATION TECHNOLOGY USE
PROCEDURES AND GUIDELINES

I. Introduction.

Morgan State University (hereinafter called the “University”) computer and information technology resources (“computing resources”)¹ are dedicated to the support of the University’s mission of teaching, research and service. In support of its mission, the University provides access to computing and information resources for students, faculty and staff, consistent with institutional priorities and financial capabilities.

The University is responsible for securing its computing resources against unauthorized use modification, destruction, disruption or disclosure, while making them accessible for authorized and legitimate users.

II. Scope of Policy.

The purpose of this Policy is to provide general guidance to University faculty, students and staff regarding the use of the University’s computing resources. It defines the general principles regarding the appropriate use of equipment, software, and networks. It is the Policy of the University that all members of its community act in accordance with these responsibilities, relevant laws, contractual obligations and high ethical standards. This Policy applies to all users of University computing resources, whether accessing those resources on campus or remotely.

Access to the University’s computing facilities is a privilege granted to University students, faculty and staff. The University reserves the right to limit, deny or extend computing privileges and access to its computing resources.

III. Authentication/Security.

The same principles of academic freedom and privacy that have long been applicable to written and spoken communications in the University community apply also to electronic information. The University cherishes the diversity of perspectives represented on this campus and, accordingly, does not condone either censorship or the casual inspection of electronic files.

¹Computing resources include, but are not limited to computers, software, E-mail accounts, Internet access, personal home web pages and similar computing tools.

The University employs various measures to protect the security of its computing resources and of its user accounts. Users should be aware that there is no expectation of privacy of computing resources and that the University cannot absolutely guarantee the privacy or confidentiality of electronic documents. The University has, however, taken reasonable precautions to protect electronic documents containing private and confidential information. The University, its system administrators, technicians, or contractors will not routinely seek access to users' messages or documents except where necessary to:

1. Meet the requirements of the Maryland Public Records Law and/or other statutes, laws or regulations;
2. Protect the integrity of the University's information technology resources, and the rights and other property of the University;
3. Allow system administrators to perform routine maintenance and operations, and respond to emergency situations;
4. Protect the rights of individuals working in collaborative situations where information and files are shared;
5. Retrieve a file by a supervisor or principal investigator of assigned work, when an employee is unavailable; or
6. Monitor general usage patterns, and inspect files for a limited time when there is probable cause to believe a user has violated this Policy.
7. Investigate security violations and unauthorized access.

Under normal circumstances, inspections or monitoring related to violations of this Policy must be authorized in advance by the Vice President for Planning and Information Technology or that individual's designee, in consultation with the General Counsel. Such inspections or monitoring will be conducted with notice to the user, unless, after consultation with the General Counsel, it is determined that notice would seriously jeopardize substantial interests of the University or third parties. However, in the event of unauthorized use of the system, computer staff, without prior authorization, may access user accounts, files, and messages and/or deny access to computing resources if emergency action is deemed necessary to protect documents and files and the systems on which they reside. In such situations, the Vice President for Planning and the General Counsel shall be notified as soon as possible after the fact.

IV. Statement of Responsibilities.

A. University Responsibilities.

The University assumes the responsibility to ensure the integrity of its computing systems, workstations, and lab facilities. The computing systems offers file protection which can only be modified by an authorized user. Since no system is absolutely secure, usage will be monitored periodically to ensure that irresponsible users cannot affect the performance and integrity of other accounts and other users' information.

B. User Responsibilities.

Users of the University's computing resources or facilities, have the following responsibilities:

1. Use the University's computing facilities and resources, including hardware, software, networks and computer accounts, responsibly and appropriately, respecting the rights of other computer users, physical facilities and controls, and respecting all contractual and license agreements. "Inappropriate use" includes but is not limited to:

- a. Insertion of viruses into computer systems;
- b. Tapping a network or running a "sniffer" program;
- c. Email spam, chain letters, threats and harassment;
- d. Destruction of another user's files, lab hardware or software including but not limited to:
 - i. Disconnecting and reconnecting or reconfiguring hardware;
 - ii. Intentionally or knowingly, personally or through any agent, deleting, examining, copying, destroying altering or modifying files and/or data/records or computer programs stored, maintained or produced by a computer without permission, consent, authorization from the owner;
 - iii. Physically damaging hardware or software;
 - iv. Removing computer hardware and/or any internal components;
- e. Unauthorized use of an account-id and /or password;
- f. Unauthorized use and/or copying of software;
- g. Use for personal commercial gain, charitable solicitations unless these are authorized by the appropriate University official, or personal political activities such as campaigning for candidates for public office, or for lobbying² of public officials.

²For purposes of this Policy "lobbying" does not include individual faculty or staff sharing information or opinions with public officials on matters of policy within their areas of expertise. Faculty and staff consulting that is in conformity with University guidelines is permissible.

- h. Any access and/or use which violate state or federal law is prohibited.
2. Use only those computers and computer accounts for which you have authorization.
 3. Use mainframe accounts only for the purpose(s) for which they have been issued. Use University-owned microcomputers and advanced work stations for University-related projects only.
 4. Avoid copyright and trademark infringement. All members of the University community are responsible for understanding and observing, applicable policies, regulations, state and federal laws in connection with copyright and fair use. Similarly, all members of the University community must respect others' rights in their trade and service marks. Such marks may only be used with the permission of the owner. This also applies to University marks. Students, faculty and staff may not use the University's name in their home pages or in any way that implies University endorsement of another organization's, products or services. They may not use University logos, trademarks or the University seal. Questions regarding permission to use the University name, logos and seal in any way shall be referred to the Office of the General Counsel.
 5. Refrain from excessive personal use. Incidental personal use of computing resources such as Email and Internet access is not considered an excessive use of those resources. Personal use may be excessive if:
 - a. It takes place during regularly scheduled work time;
 - b. It overburdens a network;
 - c. It results in substantial use of system capacity;
 - d. It otherwise subjects the University institution to increased operating costs;
or
 - e. It detracts from the University employee's position, or responsibilities as determined by the employee's supervisor.

Some uses will be excessive in all environments, but the extent to which other uses become excessive may vary among units. In those instances, supervisors will provide more specific guidance to individual users by formulating unit policies or providing advice on a case-by-case basis.

6. Be responsible for all use of your accounts and for protecting each account's password. Do not share or give away computer accounts password or identification. If someone else learns of your password, you must change it so not to give others access.
7. Report unauthorized use of your accounts to your project director, instructor, supervisor, system administrator or other appropriate University authority.

8. Cooperate with a system administrator's request for information about computing activities. Under certain specified circumstances, a system administrator is authorized to access your computer files.
9. Take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on any system, network or server that you operate.
10. Make backup copies of data files, programs, diskettes and tapes.

Each user is ultimately responsible for his or her own computing and his or her own work using a computer. Take this responsibility seriously.

V. Administration and Enforcement.

The Vice President for Planning and Information Technology is charged with communicating this Policy to the user community and for providing educational programs to achieve technical proficiency and appropriate use of the resources. Requests for interpretation of the Policy as applicable to particular situations may be directed to the appropriate University administrator, such as the Vice President for Planning and Information Technology, the Vice President for Student Affairs, the Director of Human Resources or to the Office of the General Counsel.

Reports of apparent violations of the Policy may be made to the Vice President for Planning and Information Technology, to an employee's supervisor and/or, in the case of a student, to the Office of the Vice President for Student Affairs. Where serious or repeated violations are alleged, the University's Public Safety Office and/or the Office of the General Counsel should be contacted. In most instances, concerns of possible violations of this Policy will be addressed informally by discussion or admonition. Where sanctions are appropriate, they may include but not limited to a formal reprimand, loss of user privileges for a definite or indefinite period, termination of employment, or in, the case of a student, probation, suspension, or expulsion from the University.

VI. Disclaimer

The University makes no warranties of any kind, whether expressed or implied, with respect to the information technology services it provides. The University will not be responsible for damages resulting from the use of computer facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions, power outages, or by the user's error or omissions.

Use of any information obtained via the Internet is at the user's risk. The University specifically denies any responsibility for the accuracy or quality of information obtained

through its electronic communication facilities and services, except materials which are presented as an official University record. The University also does not accept responsibility for removing material that some users may consider defamatory or otherwise offensive. Users should be advised however, that dissemination of such material may subject them to liability in other forums.

VII. Other Policies and Procedures.

Individual units within the University may develop written guidelines regarding the use of computing resources under their control. Such guidelines must be consistent in principle with this Policy, but may provide additional detail, guidelines or restrictions. Prior to implementation, such guidelines shall be submitted to the Vice President for Planning and Evaluation for review.

This policy is authorized by action of the Morgan State University Board of Regents, February 2001. Comments concerning this policy should be directed to the Vice President for Planning and Information Technology.

Latest Update: February 2001