PRINTABLE PDF

Policy 5.1
Information Technology Conditions of Use

Responsible Official: VP for Information Technology & CIO
Administering Division/Department: Office of Information Technology
Effective Date: March 31, 2007
Last Revision: March 29, 2007

Policy Sections:

Overview

This policy sets forth the terms of acceptable use for IT-related systems and services.

Applicability

This policy applies to anyone who connects a personal computer or other electronic device to any networks, applications, systems, or servers at Emory University. It also applies to any user of any Emory-owned equipment.

Policy Details

A. Definitions [moved to new section below]

B. Guarantees and Disclaimers

1. Integrity and Privacy of Information Not Guaranteed

a. The University does not guarantee the security, the confidentiality or the integrity of a user's Information on Electronic Systems (ES). Some portions of the ES are more secure than others. Very high standards of security and integrity prevail in portions of the ES associated with Administrative Systems. In smaller local work group settings, the standards may not be as high. It is the user's responsibility to assess the risk and to use all means appropriate to safeguard Information. You use ES at your own risk. Should you feel appropriate safeguards are not in place, you are advised to not use that portion of the ES and to discuss the situation with the appropriate Electronic System Administrator (ESA). The University will not be responsible for the loss or disclosure of user Information on Electronic Systems.

b. The University, through its employees, will treat all of its Information on students and employees as confidential, disclosing that Information only when authorized by the student or employee in question, approved by the appropriate University Official, or required by local, state or federal law. Student and employee information is accessed by University staff, formally authorized on a need-to-know basis, only for the business purposes of the University. Aggregate information may be released by an appropriate University Official, for example, to respond to a survey.

c. Viruses, Trojan horses, worms, password breakers and packet observer programs are known to exist or have been known to exist on campus. Although reasonable efforts will be made to eradicate dangerous and unethical software, be aware that these programs exist, and take appropriate precautions.

d. Some ESAs have procedures associated with misdirected mail that involve someone acting in a "Postmaster" capacity. The Postmaster may read mail files to the extent necessary to resolve addressing problems for delivery or diagnostic purposes. Typically, someone designated by each ESA has permission to look at any file on that associated portion of the ES for diagnostic purposes only.

2. Exposure to Offensive Material

The University has no control over the content of Information servers on External Electronic Systems or the Internet. This is to inform you that some Information may be offensive to you and/or unsuitable for certain audiences.

3. Liability for Loss or Damages

The University will not be liable for any losses, including lost revenues, or for any claims or demands against the user of an ES by any other party. In no event will the University be liable for consequential damages, even if the University has been advised of the possibility of such damages. The University will not be responsible for any damages due to the loss of output, loss of data, time delay, Electronic Systems performance, software performance, incorrect advice from a consultant, or any other damages arising from the use of the University's Electronic Systems and Information. The University will attempt to correct conditions and restore Information losses.

4. Ownership of Information

a. Information created using or stored in University Electronic Systems is subject to the Emory University Copyright Policy, which covers copyright issues pertaining to University faculty, staff and students, as well as commissioned works of non-employees.

b. ES users, as a condition of ES use, recognize that the University may do as it sees fit with its owned and copyrighted Information. ES users, as a condition of ES use, grant the University permission to copy or delete Information they have created or stored in ES. Some ESA's have procedures associated with the management of computer storage space that could result in Information being arbitrarily removed from an ES. An example would be a policy of automatically deleting unread electronic or voice mail after a set period. Un-accessed computer files might be moved to off-line storage and eventually erased. Contact the appropriate ESA for current storage management procedures, if any.

c. ES users, as a condition of use, recognize that when they leave the University (cease to be an enrolled student or an employee of the University), their Information may be removed from University ES without notice. ES users must remove their Information or make arrangements for its retention prior to leaving the University. Specific ES policies on retention and removal may vary by system.

5. Safeguarding Activity in Shared Systems

a. Unrestricted ES access is granted only to immediate Electronic System staff by the appropriate ESA. These authorized individuals are responsible for the integrity and safeguarding of the Electronic Systems and the Information within them. They are expected to respect the privacy of Information within the ES and are not exempt from this policy.

b. To protect the integrity of the Electronic Systems against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the University reserves the right to limit permanently or restrict any user's ES usage; to inspect, copy, remove, or otherwise alter any Information or system resources that may undermine the authorized use of that Electronic System; and to do so with or without notice to the user. However, no such action will be taken without specific authorization from the appropriate ESA. The University, through authorized individuals, also reserves the right to periodically check and monitor its Electronic Systems, and reserves any other rights necessary to protect the Electronic Systems.

c. The University disclaims responsibility and will not be responsible for loss or disclosure of user Information or interference with user Information resulting from its efforts to maintain the privacy, security, and integrity of its Electronic Systems and Information. Most ESAs have backup procedures that periodically save user Information. Backup copies may be stored off-site and may be retained for long periods of time. The intent is to be able to recover the Information in case of system disaster. ES backup procedures and backup retention periods differ by individual ESA policy. You may or may not be able to recover lost information. The University retains the right to review Information contained in backups in conjunction with its ES integrity and safeguarding activities or as part of an official investigation of alleged violation of University Policy.

d. The University reserves the right to take emergency action to safeguard the integrity and security of Electronic Systems. This includes but is not limited to the termination of a program, job, or on- line session, or the temporary alteration of user Access Codes. Such emergency action will be taken on the authorization of the appropriate ESA. The taking of emergency action does not waive the rights of the University to take additional actions under this policy.

C. Responsibilities and Requirements of Users and ES Administrators

Users of Emory University's electronic systems are expected to abide by their local departmental policies; university policies and guidelines; local, state, and federal laws; and all other applicable policies. Contact your local ESA for departmental policies and view it.emory.edu/policies for a listing that includes other, but not all, applicable policies and laws.

1. Access Code and Password Usage

a. Access to Information and Electronic Systems is a privilege that has an accompanying responsibility to protect those systems. In general, you are responsible for all usage done under your Access Codes. Should you choose to disclose your Access Codes to others, you will be held responsible for the resulting usage. In particular, you should never disclose Access Codes which were intended to provide you alone with personal access to University Electronic Systems. You should avoid disclosing your ES Access Codes, even when requested to by someone who says it is necessary to work on a problem. Disclosure may put you and/or the person to whom you have disclosed your Access Codes in violation of an applicable license or contract. You should take all reasonable precautions, including but not limited to password changes and other file protection measures, to prevent unauthorized use of the systems and software accessible by means of your Access Codes.

b. You should only use ES Access Codes that you are authorized to use. You should not try in any way to obtain ES Access Codes in an unauthorized or fraudulent manner. This includes, but is not limited to, providing false or misleading information for the purpose of obtaining Access Codes, capturing of Access Codes or theft of Access Codes. It is unethical to engage in activity that is intended to produce entry into an ES by persuading ES users to reveal their access codes.

c. Although you have a right to access the Information for which you are authorized, you should not attempt to circumvent Access Codes or Information protection schemes or uncover security loopholes or attempt to break authentication procedures or encryption protocols. This is sometimes called "hacking" or "cracking." Using loopholes in ES or EES security systems to access your own data is inappropriate and may be hazardous. Using loopholes in ES or EES security systems for unauthorized access or activities is unethical and in some cases illegal. These activities include, but are not limited to, the unauthorized changing of access rights, privileges, ownership, resource allocations, or quotas. You should refrain from experiments that attempt to find or demonstrate ES or EES vulnerabilities without the prior permission of the appropriate ESA. In particular, you should not use University Electronic Systems to "hack" or "crack" External Electronic Systems. It is also expected that you will respect the financial structure of the Electronic Systems by not intentionally developing or using any unauthorized mechanisms to alter or avoid charges levied for ES access or use. If you find that you have unintentionally gained unauthorized access, stop. Take no further action on the system and immediately contact the appropriate ESA.

2. Anonymous Activity

a. Sending Information, especially electronic mail, that does not correctly identify the sender can be

unethical. Unless the recipient expressly accepts anonymous Information, you should not disguise or attempt to disguise your identity or the identity of the part of the Electronic System you are using.

b. It is also the responsibility of the ESA to ensure that Electronic Systems do not use "public" Access Codes which permit the anonymous distribution of arbitrary Information. For example, it would be fine to allow access to public domain software or documentation through a public "Guest" Access Code, but would be inappropriate to allow "Guests" to send electronic mail to just anyone. It would also be inappropriate for the ESA to allow "Guests" to access resources outside the domain of his or her ES. For example, it would be improper to provide "Guests" with general access to the Internet.

c. ESAs should refrain from setting up "generic" or "project" computer IDs with the intent to grant the same ES Access Code to multiple people. Multiple access can obscure anonymous activity and other technical solutions should be explored.

d. Setting up an ES to "masquerade" as another ES for the purpose of anonymous activity is unethical.

3. Backups

If you use a "personal" system, even if it is provided by the University, it is your responsibility to insure that the system is properly backed up and that the Information contained in that "personal" system is safeguarded. Contact your local ESA for assistance if necessary.

4. Communication Tampering and Monitoring

a. It is unethical and may be criminal to attempt to monitor other people's communications without their permission. Likewise, you should not view, read, listen to, copy, change, execute or delete another user's Information without that user's or the owner's permission. This includes but is not limited to monitoring, reading, or tampering with electronic-mail of which you are neither the author nor the addressee. Exceptions for legitimate purposes should be obtained from the Vice Provost for Information Technology.

b. ESAs may authorize ES "postmasters" to read electronic mail files as necessary in order to correct addresses on "dead letters" or perform other diagnostic tasks.

c. The unauthorized physical connection of monitoring devices to the ES which could result in the violation of University policy or applicable licenses or contracts is unethical. This includes but is not limited to the attachment of any electronic device to the ES for the purpose of monitoring data, packets, signals or other Information. Authorization to possess and use such hardware for legitimate diagnostic purposes must be obtained from the appropriate ESA.

5. Copying, Installing, and Using Software

a. In order to receive user support from the University or vendors, you may be asked to produce the manuals, original diskettes, serial number, or other proof of proper software licensing. In addition, vendors may require proof of purchase to upgrade to a new version of the product. It is the responsibility of the appropriate ESA, which is often the user in the case of a "personal" system, to insure that proper documentation and records are maintained.

b. You should be aware of and abide by the university policy on Copying and Using Computer Software. Most software that resides on Electronic Systems is owned by the University or third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements. You are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on Electronic Systems or for distribution outside the University; against the resale of data or programs, or the use of them for non-educational purposes or for financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization. University employees who develop new packages that include components subject to use, copying, or redistribution restrictions have the responsibility to make any such restrictions known to the users of those packages.

c. You should not knowingly possess, give to another person, install on any Electronic System, or run, programs or other Information which could result in the violation of any University policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers, and packet observers. Authorization to possess and use Trojan horses, worms, viruses and password breakers for legitimate research or diagnostic purposes can be obtained from the Vice Provost for Information Technology. Authorization to possess and use packet/data observation software for diagnostic purposes may be obtained from the appropriate ESA.

6. Copyrights and Plagiarism

a. Respect for intellectual labor and creativity is essential to academic discourse. This tenet applies to works of all authors and publishers in all media. It includes respect for the right to acknowledgement and right to determine the form, manner, and terms of publication and distribution. If copyright exists, as in most situations, it includes the right to determine whether the work may be reproduced at all. Because electronic Information is volatile and easily reproduced or altered, respect for the work and personal expression of others is especially critical in ES environments. Viewing, listening to or using another person's Information without authorization is unethical. Ethical standards apply even when this Information is left unprotected.

b. For Information which the individual or the University does not hold the copyright, written permission from the copyright holder is required to duplicate any copyrighted material. This includes duplication of CDs, DVDs, audio tapes, videotapes, photographs, illustrations, computer software and all other Information for educational use or any other purpose. Exceptions to this policy must be obtained in writing from University Counsel.

c. With a greater emphasis on computer based assignments, students need to be especially cognizant of ES ethics. In particular, academic dishonesty or plagiarism in an ES student assignment may be suspected if the assignment calling for independent work results in two or more solutions so similar that one can be converted to another by a mechanical transformation. Academic dishonesty in an ES assignment may also be suspected if a student who was to complete an assignment independently cannot explain both the intricacies of the solution and the techniques used to generate that solution. Suspected occurrences of academic dishonesty are referred to the Honor Council of the student's school or college.

7. Harrassment

a. The University has a policy prohibiting sexual and discriminatory harassment. The University Policy Statement on Discriminatory Harassment covers all forms and means of sexual discriminatory harassment, including any such activities using Electronic Systems. ES usage or Information that is perceived by its recipient as sexual or discriminatory harassment as defined by University policy may be considered a violation.

b. The display of offensive material in any publicly accessible area is likely to violate University harassment policy. There are materials available on the Internet and elsewhere that some members of the University community will find offensive. The University can not restrict the availability of such material, but it considers its display in a publicly accessible area to be unethical. Public display includes, but is not limited to, publicly accessible computer screens and printers.

8. Notification of Violation

All students, faculty and staff share responsibility for seeing that Electronic Information Technology Systems are used in an ethical manner. Please notify the appropriate ESA of any suspected violation of this policy. You may be asked to cooperate with the University should an investigation into the abuse of an Information Technology system arise. You are also encouraged to report any information relating to a flaw in, or bypass of, Electronic Systems security to the appropriate ESA.

9. Unrelated Use

a. Electronic Systems are provided by the University for the sole purpose of supporting its mission. Without permission from the appropriate ESA, it is unethical to use Electronic Systems for:
1) solicitation not related to official University business,
2) commercial gain or placing a third party in a position of commercial advantage
3) any non-University related activity, including non-University related communications
This applies to each segment of the Electronic System utilized by such activity, and specifically to the Campus-Wide Data and Voice Network. Permission from the Vice-Provost for Information Technology must be obtained before using any portion of the Campus-Wide Data or Voice Network for these activities. This paragraph is not intended to restrict free speech or to restrict casual, personal communications between consenting parties.

b. General University policy prohibits non-University use of University facilities. This does not prohibit the University, through its ESAs, from setting up Information servers or other ES specifically designated for the purpose of fostering an "electronic community". These designated Information servers may or may not conform to the guidelines in the previous paragraph. These designated Information servers or other ES are not exempt from any other portion of this policy.

10. Wasting Resources

a. It is unethical to deliberately perform any act which will impair the operation of any Electronic System or deny access by legitimate users to any Electronic System. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of an Electronic System.

b. The willful wasting of ES resources is unethical. Wastefulness includes but is not limited to passing chain letters, willful generation of large volumes of unnecessary printed output or disk space, willful creation of unnecessary multiple jobs or processes, or willful creation of heavy network traffic. In particular, the practice of willfully using Electronic Systems for the establishment of frivolous and unnecessary chains of communication connections is an unethical waste of resources.

c. Game-playing outside of an educational context is generally permitted insofar as such activities do not adversely impact others or violate other provisions of these Guidelines. "Game-playing" is developing or executing a computer program which primarily provides amusement or diversion. Game-playing may be restricted or banned by the appropriate (usually local) ESA.

d. The sending of random mailings ("junk mail") is discouraged but generally permitted insofar as such activities do not violate the other guidelines set out in this document. It is poor etiquette at best, and harassment at worst, to deliberately send unwanted mail messages to strangers. Recipients who find such junk mail objectionable should contact the sender of the mail, and request to be removed from the mailing list. If the junk mail continues, the recipient should contact the appropriate ESA.

Definitions

Access Codes: any form of Information used to authenticate, secure or control electronic information technology systems. This includes, but is not limited to, logon ID's, passwords, keys, and account numbers.

Electronic Information (Information): includes all material stored in or moved by electronic information technology systems including, but not limited to data, records, files, data bases, electronic mail, text, digital images, video images, digital sounds, voice mail, discussion group postings, electronic bulletin board discussions, software, programs, codes and electronic procedures.

Electronic Information Technology Systems (Electronic Systems, ES): include, but are not limited to, computers, computer peripherals, communication devices, cell phones, personal digital assistants (PDAs), telephones and telecommunications equipment, fax machines, computer data networks, video equipment and video networks, photocopying machines, computer software, supporting documentation, supplies, storage media, support facilities and energy sources. Electronic Systems are limited to those leased, rented, owned by, or loaned to the University.

ES Administrator (ESA): is the person responsible for the administration and use policy for a particular portion of Electronic Systems. The University Information Technology environment is a collection of separately administered and often interconnected Electronic Systems. A portion might be a departmental local area network, including local servers, printers, etc. connected to a University backbone network. In this case the ESA might be the department or division head. A portion might also be shared central computers, the telecommunications network or the campus-wide video network. A notable portion of the ES is the backbone data network, or Campus-Wide Data Network.

Related Links

- Current Version of This Policy: http://policies.emory.edu/5.1

Contact Information

Subject	Contact	Phone	Email
Interpretation of Policy	Jay Flanagan	404-727-4962	jay.d.flanagan@emory.edu

Revision History

No previous versions of this policy were found.