Acceptable Use of Information Technology Resources Policy Interpretation Guidelines

These guidelines are meant to assist the university community in the interpretation and administration of the Acceptable Use of Information Technology Resources Policy. They outline the responsibilities each member of the community (client) accepts when using computing and information technology resources. This is put forth as a minimum set of standards for all areas of the

Related Topics

UMass Amherst Acceptable Use of Information Technology Resources Policy

Rights and Responsibilities for Acceptable Use of Information Technology

university and may be supplemented with unit specific guidelines. However, such additional guidelines must be consistent with this policy and cannot supersede this document.

1. CLIENT (USER) RESPONSIBILITIES

Use of University of Massachusetts Amherst Information Technology (UMass Amherst IT) resources is granted based on acceptance of the following specific responsibilities:

Use only those computing and information technology resources for which you have authorization.

For example, it is a violation:

- To use resources for which you do not have authorization
- To use someone else's information technology credentials (NetID and password), or to share yours with someone else (in other words, NEVER share your password; use mail forwarding or role subsidiary accounts for the sharing of information technologies necessary to conduct institutional business)
- To access files, data, or processes without authorization

- To purposely look for or exploit security flaws to gain system or data access

Protect the access and integrity of computing and information technology resources.

For example, it is a violation:

- To use excessive bandwidth
- To release a virus or worm that damages or harms a system or network
- To prevent others from accessing an authorized service
- To send email that may cause problems and disrupt service for other users
- To attempt to deliberately degrade performance or deny service
- To corrupt or misuse information
- To alter or destroy information without authorization

Abide by applicable laws and university policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.

For example, it is a violation:

- To download, use or distribute copyrighted materials, including pirated software
- To make more copies of licensed software than the license allows
- To operate and participate in pyramid schemes
- To distribute pornography to minors
- To upload, download, distribute or possess child pornography

Use computing and information technology resources only for their intended purposes.

For example, it is a violation:

- To use computing or network resources for advertising or other commercial purposes
- To distribute copyrighted materials without express permission of the copyright holder
- To send forged email
- To misuse the network or software to allow users to hide their identity, or to interfere with other systems or users
- To send terrorist threats or "hoax messages"
- To intercept or monitor any network communications not intended for you

- To attempt to circumvent security mechanisms
- To use privileged access for other than official duties
- To use former privileges after graduation, transfer or termination, except as stipulated by the university

Respect the privacy and personal rights of others.

For example, it is a violation:

- To use electronic resources for harassment or stalking other individuals
- To tap a phone line or run a network sniffer without authorization
- To access or attempt to access another individual's password or data without explicit authorization
- To access or copy another user's electronic mail, data, programs, or other files without permission
- To disclose information about students in violation of University Guidelines

2. SYSTEM ADMINISTRATOR RESPONSIBILITIES

System Administrators and providers of university computing and information technology resources have the additional responsibility of ensuring the integrity, confidentiality, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately for their intended purpose and only to fulfill their job duties. Any private information seen in carrying out these duties must be treated in the strictest confidence, unless it relates to a violation or the security of the system.

3. SECURITY TIPS

Users are urged to take appropriate security precautions to reduce risk and to help protect institutional computing resources and information such as:

- Safeguarding their account and password
- Taking full advantage of file security mechanisms
- Backing up critical data on a regular basis
- Promptly reporting any misuse or violations of the policy
- Using virus scanning software with current updates

- Using personal firewall protection
- Installing security patches in a timely manner

For additional information, contact your department IT Administrator or IT User Services at **it@umass.edu**. Report all lost or stolen devices, security incidents, and all breaches of institutional information and/or research data to **security@umass.edu**.

4. VIOLATIONS

Every member of the university community has an obligation to report suspected violations of the above guidelines or of the Acceptable Use of Information Technology Resources Policy. Reports should be directed to the unit, department, school, or administrative area responsible for the particular system involved. If ownership is unknown, reports should be sent directly to the **Vice Chancellor for Information Services & Strategy & CIO**.

If a suspected violation involves a student, a judicial referral may be made to the Dean of Students Office of the college of the student's enrollment. Incidents reported to the Dean will be handled through the University Code of Student Conduct.

If a suspected violation involves a staff or faculty member, a referral will be made to the individual's supervisor.

5. EMPLOYEE WORKPLACE ENVIRONMENT

Employees receive computing, networking, and information resources as tools for fulfilling their employment duties. Employees assume responsibility for appropriate usage and must exercise good judgment regarding the reasonableness of personal use.

Employees must be careful, honest, responsible, and civil in the use of computers and networks. They must respect the rights of others, respect the integrity of the systems and related resources, and use these resources in strict compliance with the law, university policies, and contractual obligations.

Using IT resources inappropriately or in ways that diminish employee performance, even if such use does not explicitly violate any university policy, may affect employee performance evaluations.

Any use of IT resources that is inappropriate to the workplace, or

otherwise contributes to creating a harassing or discriminatory workplace, or creates a legal risk, will subject the employee to formal disciplinary action under applicable university personnel policies and/or collective bargaining agreements.

6. SPECIFIC INTERPRETATIONS

This section gives interpretations and procedures that are specific to UMass Amherst IT systems. It is meant to be used with the **Acceptable Use of Information Technology Resources Policy** and the preceding sections of these Acceptable Use Interpretation Guidelines.

In addition to this document, specific computers and labs may have their own rules. These should be posted clearly at the facility, or pointers included in the login message. Violations of those rules are considered violations of Acceptable Use, and may be reported using the procedure in this document.

Interfering with Systems and Networks

Both the policy and guidelines documents indicate that computer resources may not be used to interfere with or inhibit other users.

However, enough cases have come up recently that it seems worthwhile to elaborate on this point.

Bandwidth Use

Problems often occur when someone creates a program that does something lots of times. For example, if you write a program that looks at the same web page thousands of times, this will normally cause a problem. Both the servers that handle web pages, and the network that gets the pages for you, are designed for normal human use. They are not designed to cope with programs that ask for the same thing many times. Similarly, sending the same request via email a large number of times (even in the same email message) will often cause problems. So will repeatedly opening and closing network connections, continuously sending "ping" packets, etc.

Networks can only handle a limited amount of traffic. UMass Amherst is fortunate to have a fairly robust connection to the Internet. However, smaller educational institutions and commercial sites may not have connections that are as robust. It is possible for a single person at UMass to do things that will effectively shut down network access for a smaller

site. If you do this, you are liable not only for university discipline, but also for prosecution. Generally you should be safe if you only use standard system tools in the ways they are intended to be used: viewing web pages yourself, logging in to a computer and using it for legitimate purposes, etc. If you start writing programs or scripts that use these tools repeatedly or in unusual ways, it is your responsibility to make sure that what you are doing will not cause problems for the rest of the network.

Individuals, departments, or students operating computers or networks that consume an excessive amount of bandwidth are subject to having their consumption limited to ensure adequate capacity for the majority of users. For administrative systems, a good-faith attempt will be made to contact a responsible party prior to curtailment or disconnection of a computer or service. In all cases, the legitimate business needs of the university will be considered the highest priority traffic, and the use of resources for entertainment or other personal uses will not be considered essential and may be severely limited.

Disruption of Core Network Services

UMass Amherst IT will be the primary provider of network "services" such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) on UMass Amherst IT networks. Any computer or equipment that replicates or disrupts these services or other network services will be immediately disconnected. Computers or devices that require a static Internet Protocol (IP) address must have one properly assigned by UMass Amherst IT. All residential computers must use an IP address assigned by DHCP (there are no exceptions). Static addresses may be requested for administrative computers from **hostmaster@it.umass.edu**. Such requests must be made by an employee of the university that is responsible for managing the computer or device.

Enforcement

The university's communications network accommodates many thousands of users on and off campus. The network is constantly monitored to track volume and performance. In the event that the campus network experiences significant degradation due to excessive utilization of resources or a network based attack from internal

or external computers or networks, the university reserves the right to take any measure necessary to insure stability and performance. These measures may include rate-limiting, filtering, or disconnection of any computer, network, or building that is involved. Whenever possible, prior notice will be given; however in emergency, after-hours, or widespread network disruptions this may not always be possible.

Copyright Violations

When the university receives a notice of infringement from a copyright holder or designated agent in compliance with the DMCA (Digital Millennium Copyright Act), the university will take the measures necessary to remove the ability to access the infringing material via the network without prior notice. This activity is illegal, and a violation of the UMass Amherst IT Acceptable Use Policy and will not be tolerated from either the residential or the academic computer networks.

Commercial or Political Use of UMass Amherst IT Resources

Commercial or political use is covered in both the policy and guidelines documents. This is being mentioned here simply because

commercial use is one of the most common violations of acceptable use. Here are some of the most common examples of things we consider commercial use:

- Using a UMass system to host a web page for any business, including your private consulting practice, your political campaign, or to campaign for another person
- Referring people to a UMass email address for commercial or political use (e.g., in print ads or commercial web pages)

There are often ambiguities about what is permitted. Do not plan to "ask forgiveness" after the fact! You are best advised to "ask permission" before starting to develop any information that may be interpreted as "commercial" in nature. In such cases, please feel free to call the UMass Amherst IT Help Center at 413-545-9400 or fill out our **Help Request form**.

Note: Some commercial uses could be violations of federal tax law and some political uses may be a violation of state law of public funds.

Harassment

- It is a violation to send email that a reasonable person would consider

harassment. Examples: Emailing people who have asked that you not email them and with whom you have no legitimate business need to email. Repeatedly emailing people with whom you have no pre-existing personal or professional relationship

- All email must contain a valid *From:* field, identifying an email address to which questions and complaints may be directed.

Chain letters are letters that come to you asking that you participate in a pyramid scheme to make money, receive goods, or in some cases simply send well wishes on to "5 of your friends" for good luck. If you know math you will recognize that chain letters attempt to create exponential growth. If not stopped, they will quickly overwhelm any network or mail system. Thus it doesn't matter whether items of value are involved or not. Chain letters have been illegal if sent through the United States Postal Service (USPS) for many years.

Many Internet chain letters often start out by saying "this is absolutely legal", or "I used to think this was illegal, but I checked with a lawyer and it's not." The USPS and FBI say that this is false. These schemes (and various related ones, including some multilevel marketing scams) are

considered to violate Federal laws against both gambling and wire fraud. We (and most Internet Service Providers) will take action against any chain letter, or any other form a communication that asks each individual to send something to lots of others.

The best action for you to take is to simply delete any message that appears to be a "chain letter." In this way you protect both yourself and the sender.

Issues with Netnews

We expect our users to follow community standards in use of Netnews. This includes (but is not limited to):

- Abiding by any rules specified in the charters of the newsgroup
- Abiding by rulings of the moderator in moderated groups (and not attempting to bypass moderation for moderated groups)
- Posting only to relevant groups
- Not sending substantially the same posting to more than 10 groups

In some other areas it is hard to codify acceptable behavior in a policy such as this, because certain standards differ from group to

group. These standards often include the level of personal attack and strong language that are allowed. In certain groups there are other standards. We expect our users to follow prevailing standards. If you consistently violate those standards, readers may complain to the system administrator. If a system administrator or other UMass Amherst IT staff person instructs you that your postings are inappropriate, we expect cooperation (see the next section). For the good of the campus community, this policy is intended to deal with violations of group charters or similar standards for a group. University policy does not permit content-based censorship. Thus this rule may not be used by staff to control what views may be expressed by users.

Cooperation with System Administrators

From time to time activities may interfere with operation of the system, even though they may not clearly be prohibited by the Acceptable Use Policy. In such cases, the system administrator or other UMass Amherst IT staff person may contact you and require you to discontinue a practice. You are expected to comply with such instructions. Once you have received

such a warning, any further activity of the same kind will be treated as a violation of Acceptable Use.

This is intended to allow staff to intervene when immediate action is required to stop a concrete problem, such as overloading a system or network, interfering with other users' normal use of the system, or a security breach. It is not intended to give system administrators arbitrary authority. If you think a staff member has acted inappropriately in asking you to discontinue a practice, you may ask for the decision to be reviewed by the Vice Chancellor for Information Services & Strategy & CIO, in accordance with university policies and procedures. However, you will be expected to comply with the ruling of the staff while this review is happening.

Original material courtesy of Cornell University Rights and Responsibilities.

Printer-friendly version

Security

Software

Employment

OTHER

Learning Commons

UMass home

Report a Security Incident

IT Project Request Form