CLASS Laboratory Computer Resource and Internet Access Policy

30 May 2006 (Revision 0.0)
20 Sep 2006 (Revision 1.0)
26 Sep 2006 (Revision 1.1)

QUICK OVERVIEW

1) Use all CLASS Labs computer resources for CLASS Labs work only.

2) Do not install or modify software or hardware on any CLASS Labs computer.

3) Do not share you password or permit others to access your accounts.

4) Do not use CLASS Labs computer resources for any fraudulent, unacceptable, prohibited, unethical, or illegal activity.

5) Report all violations of this policy to your supervisor or CLASS IT personnel.

POLICY

The CLASS Lab promotes Internet use that enables employees to perform Departmental missions and encourages its employees, students, volunteers, and contractor personnel to develop Internet skills and knowledge.

If an employee's supervisor determines that Internet access is in the best interest of the Lab, the employee will be permitted, within the limits set forth below, to use the Internet on personal time to build his/her network search and retrieval skills.

Employees who do not require access to the Internet as part of their official duties, may not access the Internet using CLASS Lab facilities under any circumstances.

It is expected that employees will use the Internet to improve their job knowledge; to access scientific, technical, and other information on topics which have relevance to the Lab. Users are advised not to use the Internet for any purpose which would reflect negatively on the CLASS Lab or its employees.
CLASS Lab systems are for Lab use and not for personal use; however, when certain criteria are met, CLASS Lab users are permitted to engage in the following activities:

1) During working hours, access job-related information, as needed, to meet the requirements of their jobs.

2) During working hours, participate in news groups, chat sessions, and E-mail discussion groups (list servers), provided these sessions have a direct relationship to the user’s job with the Lab. If personal opinions are expressed, a disclaimer should be included stating that this is not an official position of the Lab.

3) During personal time, retrieve non-job-related text and graphics information to develop or enhance Internet-related skills. It is expected that these skills will be used to improve the accomplishment of job-related work assignments and that all such activities must not violate any of our “Unacceptable Use” policies. In this context, “personal time” is defined as being: before, or after, regular office hours; during your lunch break; or, during supervisor approved breaks.

4) Employees are prohibited from initiating non-work related Internet sessions using CLASS Lab information resources from remote locations.

The following CLASS Lab Internet users are covered by this policy:

1) Full or part-time employees of the CLASS Lab.

2) Students and volunteers who are authorized to use CLASS Lab resources to access the Internet.

3) CLASS Lab contractors who are authorized to use Lab equipment or facilities.

This policy applies to Internet access when using CLASS Lab equipment and facilities, and performed using Internet Protocol addresses and domain names registered to the CLASS Lab.

SECURITY

To protect the information contained on the CLASS Lab networks, there have been a number or security measures implemented. Each user is issued an account and password. This password will grant the user access to information based on their job requirements and security level.
Your password may not be given to anyone. If a person has requested the use of your network account, you may direct them to your supervisor or the Information Technology group. In addition, using another’s account or representing another user is prohibited. You may be held responsible for any abuse if you knowingly let someone use your account. If you believe your password is known by another user, please contact your supervisor or the Information Technology group to request a new password.

FRAUDULENT USE OR BEHAVIOR

Users must respect the integrity of computing and network systems; for example, users shall not intentionally develop or use programs that harass other users or infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

Under no circumstances is an employee of the CLASS Lab authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CLASS Lab owned resources. An employee that suspects or is aware of such activity is required to notify their supervisor immediately.

Network security is a very serious issue. Tampering with data or attempting to circumvent the flow of data is strictly prohibited.

UNACCEPTABLE USE

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. An employee aware of any activity or activity by another employee that violates this policy is required to notify their supervisor and the Information Technology group immediately.

The following activities are strictly prohibited, with no exceptions:

System and Network Activities

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the CLASS Lab.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
• Revealing your account password to others or allowing use of your account by others

• Using a CLASS Lab computing asset to actively engage in procuring or transmitting material that is in violation of University of Michigan sexual harassment and/or hostile workplace policies.

• Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinging floods, packet spoofing, denial of service, and forged routing information.

• Port scanning or security scanning is expressly prohibited unless authorized by the Information Technology group.

• Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

• Circumventing user authentication or security of any host, network or account.

• Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

• Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communications Activities

• Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

• Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
Unauthorized use, or forging, of email header information.

Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

**Intranet /Internet Activities**

The posting, uploading, or downloading of pornographic or vulgar messages, photos, images, sound files, text files, video files, newsletters, or related materials is strictly prohibited.

Engage in any unlawful activities or any other activities which would in any way bring discredit on the CLASS Lab.

Use of CLASS Lab computer resources for private business or commercial activities, fund-raising or advertising on behalf of non-CLASS Lab organizations is prohibited.

**General Uses and Actions that are Expressly Prohibited**

Any commercial use or any use for personal gain.

Adding, removing, or modifying identifying network header information (aka "spoofing").

Attempting to impersonate any person by using forged headers or other identifying information.

Facilitating use or access by non-authorized users, including sharing your password or other login information with anyone.

Obtain and/or use another user’s passwords without their knowledge and consent.
• Attempt to gain access to files and resources to which you have not been granted permission.

• Try to "crash", or unnecessarily retard, the network or computing systems.

• Make copies of another user's files without their knowledge and consent.

• Steal, vandalize or obstruct the use of computing equipment, facilities, or documentation.

• Using any CLASS Lab services to harm, or attempt to harm, endanger, harass, or otherwise threaten minors in any way. This includes but is not limited to the collection of information from children in violation of the 1998 Children's Online Privacy Protection Act.

• Using any CLASS Lab services to transmit any material (by e-mail, uploading, posting, or otherwise) that threatens or encourages bodily harm or destruction of property.

Software and Hardware

• The illegal use of software is prohibited.

• All segments of the computer systems remain CLASS Lab property and are furnished to employees for business use only. Entertainment through the use of computer games is not permitted except such games or entertainment programs as may be provided as part of the official CLASS Labs IT installation suite and that such use takes place only during personal time.

• You may not install software onto the computer or onto the network without the permission of the Information Technology group. You may not download any software without the permission of the Information Technology group. Permission must be obtained prior to beginning the process of downloading software.

• You may not install hardware without permission of the Information Technology group. Devices such as wireless access points, storage devices and network hardware may present a security risk or impede operations.
MONITORING AND PRIVACY

The CLASS Lab reserves the right to monitor all Internet and e-mail activity on its networks.

Individuals using CLASS Lab equipment to access the Internet are subject to having activities monitored by system or security personnel. Use of this system constitutes consent to security monitoring, and employees should remember that most sessions are not private.

VIRUSES

The threat of a virus infection can arise from downloading files from the Internet, loading data into your computer from a diskette, or running an e-mail attachment. If you question the authenticity of data, you may have the Information Technology group scan it for viruses.

CLASS Lab users must follow existing security policies and procedures in their use of Internet services and will refrain from any practices which might jeopardize the Lab's computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.

REPORTING AN INFORMATION SECURITY INCIDENT

University policy requires all users of University information technology resources to promptly report security incidents to their unit IT department. IT units in turn escalate serious IT security incidents to the Information Technology Security Services (ITSS) office (pursuant to University Policy SPG 601.25).

An information security incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy (as defined in SPG 601.7).

Examples of information security incidents include (but are not limited to):

1. Computer security intrusion
2. Unauthorized use of systems or data
3. Unauthorized change to computer or software
4. Loss or theft of equipment used to store private or potentially sensitive information
5. Denial of service attack
6. Interference with the intended use of information technology resource
7. Compromised user account

Additionally, you are expected to report information you may have concerning instances in which any guidelines in this Policy have been or are being violated.

VIOLATIONS OF THIS POLICY

In accordance with established University practices, policies, and procedures, confirmation of violations of this policy may result in termination of computer access, disciplinary review, expulsion, termination of employment, legal action, or other disciplinary action.