cfs policies - facilities

Home

Policies for Use of Departmental Computing Facilities

- Standard Policy
- Trusted User Policy

Standard Policy for Use of Departmental Computing Facilities

1. Permitted Uses of the Facility

1.1 Computer accounts are given only for the purpose of computer science research and education as directed by the faculty and research staff of the Computer Science Department. Computing activities that interfere with this purpose are not permitted. Prior written approval from the Director of Computing Facilities is required for: 1) Any commercial activities or work for hire not explicitly permitted by university policy; 2) Any significant use of computing resources that is not clearly related to the department's goals and functions.

1.2 Only people who have been issued accounts by a member of the Computing Facilities staff are authorized to use the computing facility. Only the individual who is given an account may use that account. He or she is not authorized to allow anyone else to use his or her account without prior permission from the Director of Computing Facilities.

1.3 The creation of network services (e.g. WWW servers, IRC servers) on machines in the computing facility potentially allows non-users access to the resources of the facility. Creating such services requires the prior approval of the Director of Computing Facilities.

2. Using Resources in the Facility

2.1 Certain computer systems were either purchased by or are designated for use by specific research groups. Other systems are located on specific faculty and staff desktops and are used as those individual's primary systems. User's should obtain permission from the research group or individual prior to using these machines.

2.2 The departmental computing facilities form a shared depart-mental resource. Users should plan their use of systems resources so as not to adversely affect other users. Work that will involve the use of large quantities of resources, i.e. programs running for several days, consuming large quantities of disk storage, or running on more than a few machines, must be scheduled with the Computing Facilities Staff.

3. Security, Privacy, and Confidentiality

3.1 Both physical and information security are essential to the operation of the computing facility. Users are responsible for safeguarding any keys they are issued during their asso-ciation with the department and returning them when they leave. Users are also responsible for safeguarding any passwords they use to gain access to our systems. In par-ticular, any password that is used to generate one-time passwords or challenge/response passwords (e.g. the Skey secret password) must NEVER be sent (or typed) over the net-work.

3.2 Confidential material is maintained on the systems. Attempts by unauthorized individuals to access protected private computer files, break the encryption on encrypted materials, or obtain privileges to which they are not entitled will be regarded as a serious offense. Being in possession of programs to perform any of the above actions without prior written permission of the Director of Computing Facilities is also prohibited. Any of these actions may result in loss of all computer privileges, and may, for student users, result in expulsion from the university.

3.3 Due to the nature of academic computing, no guarantee of privacy of data can be provided. Further, in return for receiving accounts, users grant permission to Computing Facilities staff to access any of the user's files or transmissions in the normal course of their duties. This does not mean that the staff would normally browse through users' files; it just means that any file might have to be examined. The computing facilities staff will hold in strict confidence anything that they may discover in the user's files except: 1) for discussions with other C.S. department computing facilities staff; 2) when they have reason to suspect a violation of law or of university or department policy; or 3) when they have good reason to pro-vide the files to another member of the community, and in this case notification of the access will be given to the user.

4. Legal Obligations

4.1 Much of the software on our computer systems was purchased under license or is protected by copyright. These licenses or copyrights restrict the rights of users to make copies of the software, and in some cases restrict the ways in which the software can be used. No one may make copies of any licensed or copyrighted software from any of our systems without prior written approval (which will be based on the terms of the individual license or copyright). Violation may result in university, civil, and criminal penalties.

4.2 The illegal use of copyrighted or licensed software is a major problem. No user may install software on the computing facility in violation of applicable copyright laws or licensing agreements.

4.3 The department provides various methods to disseminate information locally and over the networks to other individuals and organizations (e.g. Usenet, FTP service, WWW service). Users must not use the facility to disseminate information that: 1) violates copyright or other intellectual property law; 2) harasses individuals in violation of law or university policy; 3) violates community obscenity standards as defined by the U.S. Supreme Court; 4) endangers the security of the computing facility; or 5) violates other laws or departmental or university policy.

4.4 The departmental computers are connected to networks over which access may be gained to a wide variety of educational, industrial, and government computers. Attempts to use these networks to gain unauthorized access to other machines, either directly or by means of a virus or worm program, is forbidden. Be advised that such actions are also likely to be a violation of state and federal law. In some cases, these violations will be felonies, with sentences of up to five years imprisonment for the first offense.

Trusted User Policy for Use of Departmental Computing Facilities

Trusted Users are individuals who have been given passwords that would allow them to examine or change private information that has been placed on the computer systems in the Computer Science Department by other individuals. This information may include private files that are protected against examination by normal users and private electronic mail.

The performance of the normal duties of a Trusted User might involve reading private information maintained on the department’s computer systems. The following policies govern such access

- Trusted Users will only examine or change private information when such examination is necessary to the normal performance of their duties.
- Any information discovered by the examination of private data on the computer systems will normally be held in strict confidence. The Trusted User will neither reveal this information to anyone else nor act on it him or herself, subject to the following exceptions:

    1. The information uncovered reveals a violation of law or university policy, which will be reported to supervisors and the appropriate authorities.
    2. The information revealed a problem with the computer system that requires discussion with Systems Administrators, supervisors, and technical support personnel. In this case, only as much information as is necessary to deal with the problem should be revealed.
    3. The Trusted User is unsure whether or not the information involves one of the above exceptions, in which case it may be discussed with Systems Administrators or supervisors.

Updated: undefi

Top