



# Computer Regulations within the CS Department

The following is a set of guidelines intended to bring some focus on security issues within the CS cluster. These steps are absolutely necessary owing to the increased frequency of compromise attempts which, if successful, could potentially cripple the department for days or worse. This document serves as an extension of the Office of Judicial Affairs Policy for Community Rights and Responsibilities. All users are bound by the standards of conduct defined therein. Your cooperation is expected and appreciated.

## What restrictions apply to my account?

- You must change your initial password as soon as possible. Passwords may be checked periodically. Users with passwords deemed insecure by systems staff will be notified and stronger passwords will be required. Failing to change the password will result in the account being disabled.
- Each account is issued for the sole use of its owner. Accounts are not to be shared.
- You are responsible for reading all system bulletins (using msgs), email and course related newsgroups.
- Do not attach any laptop, personal pc or other computer to the department network without prior permission to do so. Any system physically connected to the department LAN must adhere to the security guidelines of the department and of the University and be totally sanctioned before attaching it to the network.
- Unless prior permission is granted by systems NO operating system changes are to be made to any department computer. This includes installation of any software.
- Should you be permitted to install an operating system on any box in the department you must give the administrative password to systems and only in demonstrated need to know will you be permitted to retain root access to the system.
- If permission to install an operating system is granted, you will be required to obtain the approval of the installation by systems. This means that the installation must be checked and tested by systems for security and performance features before it ever is permitted to attach to the network. Without adequate reasons, such installations must be done such that everyone's needs for the machine will be met.
- At **NO** time is an unassigned ip address or the ip address of an existing host to be utilized ("borrowed") for use on any other box.
- Resource usage is monitored. Please be responsible with printing and disk space. Please use previewers and double sided output to minimize the use of paper. Please remove unneeded files and compress files used infrequently.
- No one should leave their office without logging off their system unless they have put a screen lock on the box.
- A formal inventory and inspection of all computers will be conducted regularly. Any box found that doesn't comply fully with these requirements will be removed from the network. If you currently are using any equipment on the LAN that has not been granted approval by systems it must be removed immediately and not be reconnected until approval has been given.
- Programs and data in private directories may also be restricted. File access permissions do not always reflect the owners intention; ask before reading or copying another persons files.
- Generally, actions that violate social norms for responsible behavior (such as but not limited to deliberately crashing or overloading the computers, attempting to gain access to files, account or machines without permission or posting inappropriate messages to mailing lists or bulletin boards) are prohibited.