Dalhousie University
Faculty of Computer Science

Local Policies For Responsible Computing

Policy Governing Use of an Account

Usage of your account on any system owned or operated by the Faculty of Computer Science is governed by the policies set out in the Dalhousie Acceptable Use Policy (AUP) and this document. Make sure you are familiar with these policies. Failure to adhere to these policies may be grounds for suspending access to your account, or for academic discipline. Some of these policies are repeated below.

Accounts are issued for doing work that pertains to the University, be that course work or research. Guest accounts, such as for alumni, may also be issued. No account, on any computer system within the Faculty of Computer Science, can be used for any endeavour which is for-profit. This includes developing software products, putting up for-profit web sites, or web sites related to or redirecting a user to for-profit web sites, doing commercial contract work, etc. Failure to adhere to this policy will result in the suspension of the user's accounts.

Exclusive Use of Account

The accounts issued to a particular user is for use by that person only. It must not be loaned out to others (anyone with a legitimate need may obtain their own account). In any case, the person issued the account will be held responsible for all uses of the account. Violation of this policy is considered cause for immediate suspension of the account.

No Food or Drink

There is to be no food or drink near any of the public use computers in the faculty of Computer Science.

Privacy and Security

We (the systems managers) arrange for programs to run on a regular basis to scan for security risks on the systems (situations or practices that cause an increased risk of damage to or loss of data). The user(s) involved are notified of any such situation. These programs scan through users' directories checking permissions and actually examine the contents of a few system-related files. This might be construed as an invasion of privacy, but no personal files are examined in any way, so the invasion is minimal.

If a situation is detected where we suspect that one or more user's files are at considerable risk, we will take steps to remove such a risk. This may involve further examination of a user's files, with the user's permission when possible, and/or temporary suspension of a user's account pending further investigation or action. This clearly risks inconvenience for one or a few users to protect a larger number of users.

If a student is suspected of violating a university policy, performing an illegal activity, or of having their account otherwise being used for illegal or unethical behaviour, the system manager has the authority to view any files relating to the complaint. Every effort shall be taken to avoid viewing the files of any student without significant cause.

Further, if a student has inadvertently caused undue stress to the computer systems, the system manager may take action to correct this. Examples of this include bad crontab entries, runaway processes/jobs, malformed .forward files, etc.

Communications Etiquette

Student accounts are allowed access (send/receive) to mail and news. This is a privilege that may be revoked for all students if it is abused. Avoid sending or receiving large volumes of mail (such as software distributions) without explicit prior permission. Questions should always be directed to a local person or news group first, before consuming the resources and time of the network at large with a question that could have been answered locally. To do otherwise will cause embarrassment to both you, the individual, and the university.

Forgery of mail or news is considered a serious offence and may result in suspension of the account.

Offensive Material

Never send news or mail, or post to your web pages, anything that could be construed as racist, sexist or libellous. Likewise, public display terminals must not be used to display pictures that might cause offense.

Protection of Licensed Software

The computer systems provide access to a number of licensed software packages. In most cases, the packages are licensed for a single machine or small number of machines. No user should examine or copy any software without explicit authorization; to do so may violate license agreements and make the University liable to legal action.

Similarly, the systems must *never* be used to store illegally copied software.

Conservation of Scarce Resources

At times, some of the resources on equipment in the faculty are in high demand. At these times, it is important to make all the available resources available for course-related work. To this end, we will define scarce resources and suggest guidelines to maximize their availability at times of high demand. At present, the following is presented as a set of guidelines to govern considerate and ethical use of the resources -- failure to follow them will be dealt with on a case-by-case basis, first by a friendly reminder, then by referral to the Computing Resources Committee for further action.

At the present time, the following are potentially scarce resources: workstations (PC, Mac and Unix), system memory, disk space and CPU time. At times when any of these resources is scarce, then the resource in question should not be used in any significant way for any non-course-related activity. Non-course-related activities include, but are not limited to: game playing, viewing of "recreational" graphics, reading of "recreational" news, use of dynamic graphics programs such as 'xeyes', 'xload' and 'xclock' and storage of personal non-course-related files.

In practical terms, this means (at present):

1. if more than 2/3 of the workstations in the building are in use, anyone using the system for anything other than course work should sign off and leave (*not* just stop doing non-coursework)
2. when the load average climbs above 5.0 on the undergraduate server (as shown by 'uptime'), all jobs that are not related to course work should be terminated
3. when a warning has been issued that the disk space is getting full on a particular system, users are to delete any files possible on the system in question

Tools to Help Manage Resource Usage

It is important when using the computer not to 'hog' resources. The main cause of this is running several intensive jobs simultaneously. Two general guidelines can be followed to avoid this situation: run a maximum of two "background" jobs at a time and always use the `nice' command to run long-running or intensive jobs (this reduces the priority and thus the impact of your job). To use the `nice' command, simply add the word `nice' as a prefix to the command that you would normally type, e.g. `nice command ARGUMENTS'. Type `man nice' for more information. Additionally, long running or CPU-intensive processes should be run on a workstation, not on torch.cs.dal.ca.

If in doubt, run the 'top' command, which will display, in order, the most resource consuming jobs currently running on the system.

Another important resource is disk space. It is easy to accumulate unnecessary files. Being watchful of your disk usage is an important way to reduce disk clutter.

Passwords

A password is a series of letters, numbers and/or control characters that is like a key to your account. When you first get an account, a password will be given to you. This is just a temporary password so that you can log on for the first time.

Once you do log on, you *must* change it to a more permanent password. This new password is the one you will have to use to log on to your account from then on (or until you change it again), so remember it! Nobody but yourself, not even the system administrator, should know your password. A legitimate system administrator will never have need of your password, nor will he/she ask for it. Treat any such request with the highest level of suspicion. Should someone else use your account through knowledge of your password, *you* will be held responsible for that person's actions. Remember, an intruder could not only damage or destroy your files, but could also use your account to harass others, or to embarrass you.

Your password must *not* be an obvious one. Having an obvious password puts your own account and files at risk and, to some extent, those of others on the system. It should *never* be anything so obvious as your first name (even in reverse), your spouse's name, or a word that could be found in a dictionary. You should consider using a mixture of upper and lower case, as well as numbers and control characters.

You can change your password at any time. If you do not know how, see the Help Desk for instructions. The system will ask you to type in your current password, and then it will ask you to type in your new one twice, to be sure you did not make an error while typing it in. Your password will not appear on the screen as you type it. Once this is done, your password has been changed and you will have to use the new one to log in from then on. It is recommended that you change your password at least once every other month.

Backups and Restoring Lost Files

The file systems will be regularly backed up. Full backups are done approximately every month. Other backups are done every working day.

It may be possible to restore files which you have inadvertently destroyed. Send mail to *cshelp* if you need a file restored.

Automatic File Deletion

Certain Unix utilities and some programs create temporary or backup files which they do not automatically remove. The system is designed to periodically check for certain types of files and delete them. Therefore you should avoid using such files unless it is your intention that the files be removed automatically.

Files whose name begins with the character `#' and which are more than a couple of days old will disappear. These files are generated by `emacs' as backup files in case of accidental failure during an editing session. There are similar files ending with `~'; these are removed when they become about 2 weeks old. The system is also set up to remove files beginning with `.#' every couple of days. Since these are rather unusual file names, it is unlikely that deleting them will cause you any problems, but you should be aware that this procedure exists.

Files placed in the `/tmp' or `/var/tmp' directories may be deleted after a day or two. Those in `/tmp' will be deleted when the system is restarted after a shutdown or power failure.