aITs Unix cluster systems

The aITs Unix cluster systems (details below) share a common file system, common news and mail systems, and common users. This means users can login to whichever of the systems they want and their same login id and password will work and their files will be available. This also means users can do their own "load balancing" by logging in to whichever system seems to be best for them at the time.

System Details

The cluster machines are as follows:

Alpha Systems
marlowe.umd.edu
marple.umd.edu
tracy.umd.edu
wolfe.umd.edu
holmes.umd.edu

All mail sent to the cluster should be addressed to @umd5.umd.edu (which is the address that is placed on all outgoing cluster mail). Mail sent in this manner can be read from any cluster system. The machine known as umd5.umd.edu is also part of the cluster but acts as a server for the cluster. **DO NOT USE UMD5** for anything other than your EMAIL address. Never login to umd5.

Games, IRC, and MUDs are not allowed on the aITs Unix cluster.

The home directories contain default .login, .cshrc, and .logout files. In addition, the access mode on the home directories has been set to 700. This means that a student will not be able to copy files from an unsuspecting student, unless the owner changes the mode of his home directory to something that allows such access. Of course students can still MAIL things to each other.

User files are NFS mounted on various servers. Symbolic links are used to create the file names found in the system password file. This means the names returned by the pwd command may not match the names found in the system password file. Users should always refer to home directories by the ~loginid c $HOME methods.

The estimated enrollment for your class was used to generate login ids for you, your students and TAs. All login ids have the same attributes; you and your TAs can select any of the ids for your own use. The details of these login ids are listed at the end of this MAIL item.

If you have questions concerning the creation of your Unix course access, you should contact:

```
Ira Gold
Senior Systems Administrator
Academic Environments
Academic Information Technology Services
```

University of Maryland
College Park, Maryland 20742

Electronic mail: igold@umdd.umd.edu

Campus telephone: 405-3040

Ethics

University of Maryland at College Park

Guidelines for the Acceptable Use of Computing Resources

Primary Principles: Freedom of Expression and Personal Responsibility

Freedom of expression and an open environment to pursue scholarly inquiry and for sharing of information are encouraged, supported, and protected at the University of Maryland at College Park ("UMCP"). These values lie at the core of our academic community. Censorship is not compatible with the tradition and goals of the University. While some computer resources may be dedicated to specific research, teaching, or administrative tasks that would limit their use, freedom of expression must, in general, be protected. The University does not limit access to information due to its content when it meets the standard of legality. UMCP's policy of freedom of expression applies to computer resources.

Concomitant with free expression are personal obligations of each member of our community to use computer resources responsibly, ethically, and in a manner which accords both with the law and the rights of others. The campus depends first upon a spirit of mutual respect and cooperation to create and maintain an open community of responsible users.

General

These guidelines set forth standards for responsible and acceptable use of UMCP computer resources. They supplement existing UMCP policies, agreements, and state and federal laws and regulations. Computer resources include host computer systems, UMCP-sponsored computers and workstations, communications networks, software, and files.

Computing resources are provided to support the academic research, instructional, and administrative objectives of the University. These resources are extended for the sole use of University faculty, staff, students, and other authorized users ("users") to accomplish tasks related to the user's status at UMCP, and consistent with UMCP's mission.

Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them for their intended purposes only. Each user is responsible for all transactions made under the authorization of his or her ID, and for all network activity originating from his or her data jack.

Violation of these guidelines constitutes unacceptable use of computer resources, and may violate other University policies and/or state and federal law. Suspected or known violations should be reported to the appropriate UMCP computing unit. Violations will be processed by the appropriate UMCP authorities and/or law enforcement agencies. Violations may result in revocation of computer resource privileges, academic dishonesty or Honor Council proceedings, faculty, staff or student disciplinary action, or legal

action.

User Responsibilities

The following provisions describe conduct prohibited under these guidelines:

- Altering system software or hardware configurations, or disrupting or interfering with the delivery or administration of computer resources.
- Attempting to access or accessing another's account, private files, or e-mail without the owner's permission; or misrepresenting oneself as another individual in electronic communication.
- Installing, copying, distributing or using software in violation of: copyright and/or software agreements; applicable state and federal laws; or the principles described in Using Software, A Guide to the Ethical and Legal Use of Software for Members of the Academic Community, available on inforM.
- Using computing resources to engage in conduct which interferes with others' use of shared computer resources and/or the activities of other users, including studying, teaching, research, and University administration.
- Using computing resources for commercial or profit-making purposes without written authorization from the University.
- Failing to adhere to individual departmental or unit lab and system policies, procedures, and protocols.
- Allowing access to computer resources by unauthorized users.
- Using computer resources for illegal activities. Criminal and illegal use may include obscenity, child pornography, threats, harassment, theft, and unauthorized access.

Administration

The maintenance, operation, and security of computing resources require responsible UMCP personnel to monitor and access the system. To the extent possible in the electronic environment and in a public setting, a user's privacy will be preserved. Nevertheless, that privacy is subject to the Maryland Access to Public Records Act, other applicable state and federal laws, and the needs of the University to meet its administrative, business, and legal obligations.

System Access

The only access to the aITs Unix systems is via the campus network.

WAM (Workstations At Maryland) workstations, such as those located in CSS room 3330, are directly connected to the campus network. Directions for using WAM workstations can be found in each workstation laboratory and in the aITs Information Technology Library (CSS West Wing room 1400).

Consulting

Academic Information Technology Services provides First-Aid and general consulting services to those who use Unix computing systems on campus. aITs Unix machines run the Ultrix version of Unix. With the realization that there are other versions of Unix being used on campus, First-Aid and Consulting Services will address questions based on their experience with the aITs Unix systems.

Your students should use the First-Aid service (located in all WAM workstation laboratories). They may also use the First-Aid Hotline for phone-in questions (405-6941), which is answered by First-Aiders in the PGII WAM lab.

Exact hours of service are posted at each First-Aid station.

University faculty, staff, graduate researchers, and teaching assistants can use the following consulting services.

Consulting on a walk-in or phone-in basis in the Consulting Lab (CSS West Wing room 1400, phone (301) 405-1500), 8:00 a.m. - 6:00 p.m., Monday - Friday during the Fall and Spring semesters (9 a.m. - 4:30 p.m. during semester breaks and the Summer semester).

Electronic mail at any time; use the Internet address consult@umail.umd.edu. Questions are answered by a member of the Consulting staff at the earliest possible opportunity. The consult command has been added to the aITs Unix systems to make sending mail easier, just type consult and follow the directions.

The aITs Information Technology Library (CSS West Wing room 1400) has reference copies of Unix manuals and documentation for your use. The Library also sells "Introduction to the aITs UNIX Systems" (aITs Unix handout number 1).

News

Academic Information Technology Services uses the Usenet news system on its Unix systems to inform users about system outages, new software, etc. The news group csc.news is used for all news items. Items that are considered of interest to the general University community are also placed in the um.general news group.

The default .login file contains a call to the readnews program. On some systems, users prefer to use the rn program to read news. If rn is used, the call to readnews should be removed from the users' .login file.

Printing

aITs has replaced the stock lpr program with a shell script that calls MDQS to print a file on prl, which is the 3800 laser printer attached to the campus UMDD IBM system.

The call is lpr to initiate printing of file .

Output may be retrieved at the aITs dispatch counter on the first floor of the CSS building.

File Recovery

A dump of all files is taken every week. These file backups are for recovery from catastrophic loss. Individual user file recovery is not available at this time.

Passwords

Unix systems do not have the concept of an account manager; this means that if a user forgets his password, aITs must change it for the user.

Requests for change of password should be made to Ira Gold at the address above. Requests to change student passwords will only be honored when they are made by the instructor. Instructors can make such requests via electronic mail. Requests must include login id and system name.

Disk Quota

All user login ids on the aITs Unix systems have a disk quota associated with them. When the disk quota is exceeded, the user will not be able to create new files until the amount of disk space in use has been reduced, or the disk quota has been increased.

Requests for change of disk quota should be made to Ira Gold at the address above. Requests to change student disk quotas will only be honored when they are made by the instructor. Instructors can make such requests via electronic mail. Requests must include login id, desired new disk quota (expressed in kilobytes), and system name. In all cases, requests for higher disk quotas will be evaluated against system resources and system load.

/tmp and /var/tmp

/tmp is a small directory used by system utilities for short term scratch files. Users should not place their files in /tmp. User files should be placed in user directories (every user has one) or /var/tmp (again, short term storage).

Files residing in /tmp and /var/tmp can be deleted without notice if disk space becomes critical. See "Disk Quota" above for information about requesting disk quota changes.

/tmp and /var/tmp are local to each system in the cluster.

Software

The cluster file /usr/local/doc/cluster contains cluster details, including a table showing software availability. Please read this file for full cluster details.

This document last updated January 15th, 1997.