University of Virginia
Computer Science
85 Engineer's Way
Charlottesville, VA 22903
cshelpdesk@virginia.edu

Information and Acceptable Use Policy

JULY 2018

OVERALL GUIDELINES

- **Considerate Use of Resources** – be considerate of others when using department resources.
- **Appropriate Use of Resources** – Accounts are to be used for research, instruction and administrative purposes only.
- **Respect for the Privacy of Others** - you aren't allowed to view someone else's data unless given permission to do so.
- **No expectation of Privacy** – there is no expectation of privacy when using University computing resources.

Serious infractions may involve departmental action, up to and including dismissal from your program of study.

KEY CONTACTS

Users may request help from the system staff by sending email to: **cshelpdesk@virginia.edu**

Information about the CS Department's computing resources can be found here:

https://www.cs.virginia.edu/wiki

SPECIFIC GUIDELINES

Computer Account Usage

- Computer Science (CS) users should only use their personal account.
- Users should never use another user's personal account nor share their account password under any circumstances. If a user needs access to some data in another user's account, they should request permission from the system staff and provide justification.
- In certain circumstances, a user may use a "role" account which has been created for some specific function or purpose while they are acting in that capacity. Role accounts may be for teaching (TA) or research (group account) purposes.
- **Action for violations:** your account may be deactivated or revoked. If an honor violation has occurred it will be reported to the student authorities.

Network Usage

- The network should only be used for research and teaching purposes. Networking devices must be registered by the system staff before being connected to the network.
- Other uses, notably file-sharing and streaming media, which do not typically meet the guidelines for legitimate academic activities, are prohibited. In cases where this capability is needed, the department provides the appropriate infrastructure. Sharing out MP3, MPEG and other media repositories is not permitted.
- The use of personal switching or routing devices is prohibited unless approved by the systems staff.
- **Action for violations:** Users who abuse the network will have their access revoked, regardless of whether the device connected is owned by the university or the user.

Filesystem Usage

- Storage should only be used for legitimate academic purposes.
- A user should not assume they have infinite storage. Users should take into account free space on their file system before writing large files to the system which might eliminate the free space for other users. Requests for more disk space are commonplace; the systems staff should be able to accommodate your request.
- Users should never access or modify another user's data unless that user has made the data public or granted you access to the data.
- **Action on violations:** Accessing or modifying another user's data without permission may be considered an honor violation.

Web Server Usage

- The department provides a web server for general department usage – users may "publish" from the public_html directory in their home directory. The nature of the material posted should be in keeping with the mission of the university. Copyright laws must be observed.
- Commercial and obscene material is prohibited; non-university mission material is prohibited.
- **Action for violations:** Depending on the nature of the abuse, the user may be asked to remove the posting, or it may be removed for them. Users serving up copyrighted material may be reported for copyright violation and subject to prosecution outside the university.

Enterprise Class Services

- The department deploys enterprise class services in a centralized way. These include file, FTP, HTTP, DNS, parallel computing, interactive computing, etc. services. If a user needs some special customization of these services, they should put a request into systems staff.
- Users should not run network services on any individual workstation connected to the department network. P2P file sharing programs like bittorrent are never appropriate.
- Users should not run extended or high CPU load jobs on interactive servers. A wide array of high performance servers is available for use through a job scheduler. See: **https://www.cs.virginia.edu/wiki** for more information.
- **Staff Response:** You will be told to remove unapproved services immediately. If use continues, you will lose your network privileges. Sharing of copyrighted material may be reported for copyright violation.

Printing

- The department provides a wide range of printing services, from simple documents to large format posters. Please "print what you need and need what you print." Retrieve your printouts promptly.
- 72 hour notice is needed for poster printing.
- Do not print jobs which are not work-related. Similarly, you should not continually submit jobs if they do not come out; they will eventually. Do not send PDF files directly to the printer. If a user has problems they should report it immediately to systems staff.
- **Staff Response:** Abuse of the printer resources may result in the user reimbursing the department for the cost of printing.

Workstations

- A user may be granted administrative access to their system to facilitate their work.
- A user should be prepared to share their workstation if necessary, and may ask the same of others.
- A user may install personal hardware (sound card, extra hard disk) in a department system but only with staff knowledge beforehand.
- You may install software and customize your system to suit you.
- Do not rely on the storage on workstations – it is not backed up, and no efforts are made to recover data in the event of a failure. User home directories, which reside on network storage, is backed up.
- If a user assumes responsibility for administering the machine, then they are responsible for software installation and configuration.
- A user should follow sound security practices on their workstation.
- A user should be willing to share with other users who have a legitimate need.
- There is no expectation of privacy when using University systems.
- **Staff Response:** If a machine is compromised, the hard drive will be erased and the default departmental OS and software build will be reinstalled. A user may lose any software or data they have stored.

Personal Systems

- Personal systems are typically only connected to wireless networks.
- The user is responsible for the security of the system.
- Network file systems will not be exported to personal systems.
- Systems cannot be used for commercial purposes involving the commercial use of the University's network.
- Systems cannot be used to attack other systems.
- Systems cannot provide network services.
- Systems staff cannot support personal systems.
- **Staff Response:** If there is a problem with a user's private system, it will be disconnected from the network. Compromised systems will be removed from the network, and will not be reconnected until systems staff has been satisfied that the system has been secured (this generally involves a complete wiping of the system drives).