LIBERAL ARTS
TEXAS A&M UNIVERSITY
PHILOSOPHY

Computer Access Policy

Updated January 2013

The Department of Philosophy provides computing resources to faculty, staff, and graduate students for their use in research, teaching, and other activities in support of the Department's mission. These resources include desktop workstations and the services provided by the department's main server, philosophy.tamu.edu (which include email, file access, web services, and shell accounts). In order to have access to these services, users must first acknowledge in writing that they will use these resources in accordance with applicable policies. Here is the procedure for obtaining access to our computer resources:

1. Study the contents of this web page
2. Read carefully the University Rule on Responsible Computing.
3. After you have completed these steps, print and sign the Department of Philosophy's Computer Access Agreement
4. Submit the agreement to the Department for approval
5. Once your agreement is approved by a departmental IT administrator and the department head, you will be given an account on the department's server and access to departmental computing resources according to your status (faculty, staff, graduate student, student worker, etc.).
6. University rules require that you sign a new agreement form every year

Responsible Computing

In order to be granted access to **any** computing system at Texas A&M University, all users must first acknowledge in writing that they are familiar with, and will abide by the provisions of, University Rule 29.01.99.M2, Responsible Computing.

Further information:

- University SAP on Security Awareness and Training
- Texas Administrative Code concerning Information Security Standards
- University SAP on Acceptable Computer Use

Incidental Computer Use

All Texas A&M University computing resources, including those owned by departments, are subject to state and system policies concerning the use of university resources. Your use of any departmental computing equipment or resources is governed by policies on Acceptable Use. In general, acceptable use means use to accomplish tasks in support of the University's mission, which for our department includes teaching, research, and whatever is necessary to support those activities. Use for personal purposes is also allowed provided that it is consistent with the policy on Incidental Computer Use. However, no university resources may be used for any illegal purpose or in connection with any political campaign. They also may not be used for any commercial activity, unless this is in connection with approved outside employment or consulting (see Use of System Resources for External Employment, below).

Further information:

- University SAP on Incidental Computer Use
- System Regulation on Use of System Resources for External Employment

Privacy and the Texas Public Information Act

Under University, System, and State policies, the files you create and maintain on departmental computer systems are not considered generally accessible. This means that, in general, other users (including system administrators) may not read or modify these files without your prior explicit consent. However, there are exceptions. First, law enforcement agencies and university or system auditors may obtain access to your files using appropriate procedures. Second, system administrators may need to examine your files to perform necessary system maintenance, or they may inadvertently see the contents of a file while engaged in maintenance. While university policies require system administrators to make every effort to respect the privacy of users' files, administrators also are obligated to report evidence they encounter of illegal activity.

In addition, any information on any computing system owned by the department is subject to the provisions of the Texas Public Information Act. Under that act, any citizen may request, and obtain, any such information unless it is considered confidential or otherwise excluded from disclosure by specific provisions. Confidential information includes, among other categories, most student records and some information in employee records. It does not, however, include general email correspondence. Bear in mind that any email message that you send, including copies of messages stored in mailboxes on your computer, may be subject to a request under the Public Information Act.

Further information:

- Texas Public Information Act
- University SAP on Privacy and Information Resources
- Where to direct complaints concerning the use of University information resources

Portable Computing and Encryption Issues

If you use any form of portable computing device or storage device for transporting confidential information, including student grade information, then you must protect that information by encrypting it. This applies not only to laptop computers but also to PDAs, smart phones, and removable storage media such as flash/thumb drives, iPods, CDs, DVDs, and any removable disk drives. It also applies to devices that you own yourself, if you store confidential information on them (that includes your personal laptop or flash drive, for example, if you keep your grade information on it).

The Department has adopted TrueCrypt (follow this link and choose your operating system in order to install) as its standard for file encryption. Department IT staff will assist you with setting up TrueCrypt on your office computer. You can install TrueCrypt on your personal computer by following the link below:

If you need to keep confidential information like this on your office desktop, then department policies require that you keep it in a TrueCrypt volume *on your network share on the department server*. Departmental IT staff can assist you if you need help in creating such a share. Information kept in this way is securely protected because the unencrypted information is never on your office computer's disks at all.

CAUTION! When encrypting any information on a computer, be *extremely* careful not to lose the encryption key that you use. Modern encryption is very powerful, if done properly, and if you lose your key then **you have lost access to your information, forever**. Despite what you may see in movies and television shows, it is for all practical purposes impossible to recover encrypted information without the key, unless you have an extraordinary amount of computing power and a very long time, or unless the key was badly chosen in the first place. To be safe, encrypt only what you need to encrypt. If you are encrypting essential files, you may wish to consider storing a copy of the key securely with the department.

Further information:

- University SAP on Information Security for Portable Computing Devices
- Encryption page from the University's Department of Information Technology

Email and Privacy

Email on any university system, including the department's system, is subject to the same provisions concerning appropriate use as other university resources. You should not use a university email account in support of a political campaign, for instance. In addition, please remember that unless it is encrypted, email is not a very private medium. In particular, any email message that leaves the campus network ought to be considered completely insecure, since it may pass through many different servers on its way to its destination. Moreover, it is usually difficult or impossible to be certain that the message is actually going to the person to whom it is directed. For these reasons, you should never send any confidential information through an email message unless you are able to encrypt it in way that can be decrypted only by the person it is intended for. This includes correspondence with students concerning their grades.

Further information:

- University SAP on Email Use

Passwords

As a user of a computer system, you have an obligation to keep your account protected with a good password. Your password must be at least eight characters long and should include a mix of upper and lower case letters, numerals, and punctuation symbols (you may be surprised to know that you can include spaces in your password). It should not be a word in English (or any other major language, for that matter), or a word with a few numbers at the beginning or the end, or a word backwards. For more information on what constitutes a good password, see the links below.

When you are initially assigned a computer account, you will be given a password (on paper) by a computer system administrator. The first time you log in, you will be required to change this to another password. It is a very good idea to decide what your new password will be before you log in for the first time.

Our departmental policies require that you change your password at least every 90 days. Beginning two weeks prior to expiration, you will receive daily reminders by email that you need to change it. These will include an explanation of how to change it.

Plan ahead for password changes. New passwords thought up on the spur of the moment, when confronted by a demand from the system, are liable to be both poor choices and easy to forget. To avoid this, start thinking about a new password when you receive the first warning message, and do the change when you want to rather than when the system forces you to.

If you forget your password, a system administrator can assign you a new one (which you will have to change the first time you use it, as above). System administrators can't tell you what your old password is because there is no practical way they can find out what it is.

University policies also require that you never give your password to anyone else (this includes system administrators) and that you not write it down and leave it near your computer.

Further information:

- University SAP on Passwords and Authentication
- Some advice about good passwords:
  - Advice from the University of Maryland (a little out of date: we require at least eight characters in our passwords)
  - Advice from the U.S. Computer Emergency Response Team
  - Advice from the Australian Computer Emergency Response Team
- Password strength checker: there is no indication that this site is anything other than it appears to be, but because it is not using SSL encryption, it would be prudent only to test passwords that are similar to any passwords that you actually use.

ACKNOWLEDGEMENT

Once you have read this page and the University rule concerning Responsible Computing, please print and sign the Department of Philosophy's Computer Access Agreement and submit it to the department for approval.