Securing Your Computer:

There are four ways you can secure your computer and your accounts:

- Create strong passwords
- Protect your UT EID
- Install and run security software on your computer
- Log off or lock your computer when you are away from it

Strong Passwords:

Your first step in securing your computer and online accounts is to create and use strong passwords. Hackers have become increasingly skilled at cracking passwords. A weak password can give a hacker access to your computer and the personal information found on it, such as your address or credit card numbers.

To create a strong password:

- Use a combination of upper and lower case letters, numbers and symbols.
- Use between 8 to 20 characters.
- Consider using a phrase, such as “my dog has fleas.”
- Use different passwords for your different accounts—especially your EID account. This way, if one of your accounts is compromised, the hacker can’t use the same password to access other accounts.

Some examples of unsafe passwords include:

- Your name, birth date, social security number, address or anything that can personally identify you.
- Any word found in a dictionary—even those spelled backwards.
- Words using numbers in place of letters.
- Keys next to one another on the keyboard.
- Repeating patterns.

Other password guidelines you should follow include:

- Don’t give them out or share them with anyone. This is against university policy.
- Don’t write them down and keep them posted near your computer for anyone to see or steal.
- Change your passwords regularly—every 6 months or so.
- Don’t enable the “save password” option if you are prompted to do so. These passwords can be stolen if the application is compromised.

Protect your UT EID

- Every student, faculty and staff member is provided with their own UT electronic identification, or EID. Your EID is used to perform secure online transactions at UT, such as paying bills or entering restricted Web sites.
- When you receive your EID, you agree to the UT Electronic ID Agreement, which states you accept full responsibility for any actions taken using your EID.
- Your EID acts as your legal signature on university materials.
- Don’t share it; don’t trade it; don’t abuse it.
- If you share or trade your EID password, you are giving someone else the ability to become you online, and YOU will be held responsible for any actions initiated with your EID.

Log Off or Lock Up Your Computer

- You can also secure your computer by logging off or locking it when away for any length of time. This prevents anyone but you or your system administrator from accessing your computer and its contents.
- It’s also important to protect your computer from being stolen by keeping it physically secured with a security cable or by locking it in a drawer or cabinet overnight.
- Also, lock access to your office, lab, or work area to prevent theft.
- Remember, it only takes a moment for a thief to steal your computer—and years of your work!

Complying with Federal Copyright Law

- The guidelines for complying with federal copyright law are an important component of the AUP.
- It is against federal law to illegally download copyrighted materials, including music, movies or software.
- And, it is a violation of university policy to use campus resources to illegally download or otherwise infringe upon copyrighted materials.

Category-I Data

- Category-I Data is considered restricted and confidential.
- This is primarily personal information that the University possesses that is protected by state and federal law.
- You must NEVER disclose or use Category-I data without proper authorization.
- Category-I data includes:

  > Social security numbers.
  > Personal information for university students, donors, or employees.
  > University business data, such as contract terms or status.

Category II & III

- Category-II refers to data that is subject to an “open records” request, per the
  Texas Public Information Act. This data may include specific e-mail messages or correspondence found on your computer
- The Texas Public Information Act provides the public with access to the business and official acts of our state government, public officials and employees. This act extends to business at The University of Texas at Austin.
- Category-III: refers to data not requiring special protection.

Safe Electronic Communications

- Another responsibility shared by all university employees is the responsible and safe use of electronic communications, namely e-mail and instant messaging.
- Please be aware that e-mail and instant messaging are **not** private or confidential. Anyone monitoring a network can read your messages.
- A good rule to follow is to never put anything in an e-mail you wouldn’t want to see on the front of the local newspaper.
- You should NEVER send account numbers, credit card numbers, passwords, or social security numbers through e-mail or IM.
- Contact your technical support contact for more secure messaging options.