

## DATA ENCRYPTION

**Encryption** is the conversion of data into a form that cannot be easily deciphered by unauthorized persons. You are required to use encryption if you absolutely must store sensitive data on a laptop or removable storage. Encryption is necessary if you plan to transfer sensitive data via the internet.

**Without the use of encryption** files may be intercepted and accessed by unauthorized persons resulting in a data compromise, a breach of privacy and disclosure of sensitive information. FERPA, HIPAA, GLBA and other laws may be broken whenever there is an unauthorized disclosure of our students sensitive information.

**Do not forget your password** (key) once you have implemented encryption. If the password is lost there is no reasonable expectation that you will be able to access that information ever again! Be sure to protect your password! Keep it secure!

**If you are faculty or staff** needing help implementing data encryption on your UTA assigned computer or laptop contact the Helpdesk by email [helpdesk@uta.edu](mailto:helpdesk@uta.edu) or by phone 817.272.2208

## ANTIVIRUS SOFTWARE

**Beware:** Software downloads from the internet can potentially infect your computer with Spyware.

**AntiVirus Software**, approved by OIT, is required to be loaded by Desktop Support onto your UT Arlington assigned desktop / laptop and updated regularly for the latest virus protection. Because there is a constant proliferation of new viruses and malicious code that circulates on the internet and removable storage devices daily, it is important that you keep your AntiVirus up to date. It is also highly recommended that you install AntiVirus software on your home computer. Symantec AntiVirus is available to UT Arlington faculty, staff & students at the UT Arlington computer store and by download at [www.uta.edu/antivirus](http://www.uta.edu/antivirus)

**Contact** the helpdesk for more info: 817.272.2208

## SOFTWARE PATCHES

**Software Patches** are regularly created and disseminated by software vendors in order to help protect your operating systems and software keeping them potentially free of security risks. It is especially important to keep your operating system up to date. If you are using a UT Arlington assigned computer visit [www.uta.edu/oit](http://www.uta.edu/oit) (Windows Server Update Services) page. For personal computers (use Internet Explorer) and visit [update.microsoft.com](http://update.microsoft.com) or visit Apple or Linux for their latest O/S updates.

**Contact** the helpdesk for more info: 817.272.2208

## EMAIL / VPN

**Email at UT Arlington** can be accessed by using the Microsoft Outlook client on your office computer or by accessing it over the internet via [www.uta.edu](http://www.uta.edu) "Check Email" box. You can also set up the client at home but must use VPN to connect. For more information on MavMail email visit: [www.uta.edu/email](http://www.uta.edu/email)

**VPN (virtual private network)** must be installed before you can access UT Arlington email using the Microsoft Outlook client from an off network computer. This creates a tunnel through the firewall allowing for secure email traffic to flow to and from your computer to UT Arlington servers. For more information visit: [www.uta.edu/vpn](http://www.uta.edu/vpn)

## MAVSPACE

**MavSpace** is an area on the UT Arlington servers where you can store and backup your digital files. It can be accessed by navigating with your internet browser to [mavspace.uta.edu](http://mavspace.uta.edu) where you can use your NetID and Password to gain access. The server that hosts this service is backed up and maintained regularly and is designated as "https" which means that it is secure. It also is useful because it allows you to access your files from any computer that has an internet connection.

**Be careful**, do not use your NetID and Password on any computers that you do not trust (hotel lobby computers, public kiosks). These computers may be infected with viruses or have key loggers installed.

# PROTECT YOUR COMPUTER AND SENSITIVE INFORMATION



**Information  
Security  
Office**

*Provided for faculty, staff and students by:*

*The University of Texas at Arlington  
Office of Information Technology (OIT)  
Information Security Office*

[www.uta.edu/security](http://www.uta.edu/security)  
[security@uta.edu](mailto:security@uta.edu)

817.272.5487

*Available in accessible format on website*

*(Revised: 12/17/07, Information Security [security@uta.edu](mailto:security@uta.edu))*

## Common Security Problems

- Constant attacks by viruses, worms, keyloggers, bots and spyware that infect computers.
- Email scams (Phishing) targeting sensitive information / attempting to infect networks.
- Social Engineering attempts where unauthorized persons pose as staff to obtain access.
- Criminal / Illegal Acts (Copyright Violations).
- Failure to protect account passwords.
- Installation of unauthorized software.

## COMPUTING POLICY / LAWS

All UT Arlington students, staff and faculty are expected to abide by:

- UT Arlington OIT Policy, Practice Standards and Guidelines  
[www.uta.edu/oit/policy](http://www.uta.edu/oit/policy)
- UT System Policies  
[www.utsystem.edu/policy/lib\\_number.html](http://www.utsystem.edu/policy/lib_number.html)
- UT System Policy 165  
[www.utsystem.edu/policy/ov/uts165.html](http://www.utsystem.edu/policy/ov/uts165.html)
- Texas Administrative Code 202  
[www.sos.state.tx.us/tac](http://www.sos.state.tx.us/tac)
- Family Educational Rights and Privacy Act (FERPA)  
[www.ed.gov/policy/gen/guid/fpco/ferpa](http://www.ed.gov/policy/gen/guid/fpco/ferpa)
- Health Insurance Portability and Accountability Act (HIPAA)  
[www.dol.gov/ebsa/newsroom/fshipaa.html](http://www.dol.gov/ebsa/newsroom/fshipaa.html)
- Digital Millennium Copyright Act (DMCA)  
[www.copyright.gov/legislation/dmca.pdf](http://www.copyright.gov/legislation/dmca.pdf)
- Federal Copyright Laws (Title 17)  
[www.copyright.gov/title17](http://www.copyright.gov/title17)
- UT System Policy 107  
[www.utsystem.edu/policy/ov/uts107.html](http://www.utsystem.edu/policy/ov/uts107.html)
- UT Arlington Compliance  
[www.uta.edu/compliance](http://www.uta.edu/compliance)

## NETWORK MONITORING

The University of Texas at Arlington (UTA), Information Security Office has network monitoring software and hardware devices in place that allow our Security Services Team to monitor inbound and outbound network communications.

**Users** of the UT Arlington computing network may be subject to computing audits in accordance with the Texas Public Information Act. University administration will provide any evidence of illegal computing activities to law enforcement officials such as UT Arlington Police, Local and State Police, FBI, CIA, Interpol.

## SENSITIVE AND CONFIDENTIAL DATA

**UTS165:** [www.utsystem.edu/policy/ov/uts165.html](http://www.utsystem.edu/policy/ov/uts165.html)

**Sensitive Data:** Information maintained by state agencies or institutions of higher education that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. The controlling factor for sensitive data is that of integrity.

**A designation of "Sensitive"** shall be based on compliance with applicable Federal or State law or on the demonstrated need to (a) document the integrity of that Digital Data (i.e., that the Data had not been altered by either intent or accident), (b) restrict and document individuals with access to that Digital Data, and (c) ensure appropriate backup and retention of that Digital Data. These would most frequently be required by:

- Federal or State agencies (e.g., Food & Drug Administration)
- Employee Benefit Providers
- Office of General Counsel or Institutional Office of Legal Affairs (i.e. data subject to or involved in litigation or confidentiality agreements)
- Intellectual Property and /or Technology Transfer requirements; or Federal regulations (e.g., FERPA, HIPAA, Gramm-Leach-Bliley, Biodefense, Homeland Security, DOD etc.)

**Confidential Data:** Data maintained by state agencies and universities that is exempt from disclosure under the provisions of the Public Records Act or other applicable state and federal laws. The controlling factor for confidential Data is that of disclosure.

**If you must store sensitive data** on your computer, for business related reasons, be sure to follow portable computing and encryption practice standards. For more information visit: [www.uta.edu/security](http://www.uta.edu/security)

**Note:** Never send sensitive information by email or FTP (especially unencrypted!) it can be intercepted!

**Forward all open records requests** to UT Arlington Business Services Office x2194 for processing.

## INCIDENT HANDLING

**UT Arlington** computers and networks may have sensitive information on them so it is sometimes necessary to collect information regarding any potential breach of access. If your computer has access to sensitive information and you suspect that someone has gained unauthorized access or your computer has been compromised by malicious code (such as a virus) contact the UTA Helpdesk immediately! [helpdesk@uta.edu](mailto:helpdesk@uta.edu) / 817.272.2208

**If your computer or laptop is stolen**, contact the UT Arlington Police and file a report: 817.272.3381

## PASSWORD SECURITY

**Your password** is your first line of defense! You should always use a strong password which is one that uses a combination of lower case and upper-case letters, with a combination of numbers and symbols at least eight to ten characters in length. Never use a common word that is found in the dictionary of any language.

**An example** of a poor password would be a common word like your pets name (Fluffy) even combining it with numbers such as (Fluffy1945) is not secure! An example of a strong password would be (F!4fe19for+y5). A pass phrase is even stronger, for example (I like th4 song y3!!0w\*Tz) However, some systems may limit how many characters can be used for a pass phrase.

**Note:** Do not use any of the above example passwords since they are now known. Create your own!

**Do not share** your password with anyone and try to avoid writing it down. If you do have to write it down, to remember it, then be sure to keep it secured, not stuck to monitor or under keyboard!

**Implementing** a strong password helps avoid the password from being compromised by password cracking software. For more information on password security visit: [www.uta.edu/security](http://www.uta.edu/security)

**Never use blank or null passwords!**