

## SECURE DATA TRANSFER

**FTP is not secure** - information is transferred in plain text, allowing sensitive information to be intercepted and read by anyone. SFTP is an interactive file transfer program, similar to FTP, which performs operations over an encrypted connection. See [www.uta.edu/security](http://www.uta.edu/security) (Secure Data Transfer) for more information.

## IDENTITY FINDER

**Identity Finder is a tool** approved for use by UT Arlington staff and faculty. Identity Finder can be used to search your system for sensitive information such as ssn's, credit card info & account info. More information will be posted to our website as it is available: [www.uta.edu/security/idtheft.htm](http://www.uta.edu/security/idtheft.htm)

**In a continued effort** to reduce the number of computers that have sensitive information (such as social security numbers), you must regularly audit your network, computer & removable media.

**Identify Finder is an easy tool** that has a built in wizard that guides you through the process leading up to the scan of your system. ID Finder also has an advanced mode that provides flexibility for more specialized searching by network admin's.

**Identity Finder should be used** by Information Security Administrators (ISA's) to regularly scan departmental computer drives to identify files that may have sensitive information. If found the files should be reported to their owners and either stored on a private network drive (K: Drive) or deleted. Refer to the UT Arlington Records Retention Policy before destroying any documents. For info visit: [www3.uta.edu/policy/retention/home.htm](http://www3.uta.edu/policy/retention/home.htm)

## SAFEBOOT

**SafeBoot is a program** that provides full disk encryption and is approved for use on UT Arlington desktop and laptop computers for added security. Using full disk encryption aids in the protection of information should a computer be stolen. More information will be posted to our website as it is available: [www.uta.edu/security/idtheft.htm](http://www.uta.edu/security/idtheft.htm)

## CLASSROOM LEARNING LAB NETWORKS

**Classroom learning lab networks** and network capable devices that do not require internet connectivity must be placed on an isolated network. Learning lab computers are often rebuilt to varying levels of security and patch application, providing easy targets for viruses and attacks. If on the network, these computers can become a serious threat very quickly!

## DEEP FREEZE

**Along with antivirus software** you must install Deep Freeze on public lab machines and kiosks. This will provide additional security for machines that are accessed by multiple users and forms of media. Contact: [helpdesk@uta.edu](mailto:helpdesk@uta.edu) / 817.272.2208

## BEWARE OF SOCIAL ENGINEERING

**Persons conducting** a "social engineering attempt" are trying to gain access to information or resources by pretending to be someone that they are not, tricking you into giving them access.

**They may do this** by calling you on the phone, by visiting you in person, or even by staging events that make it appear that they are legitimate personnel responding to a crisis.

**Examples may be persons** pretending to be law enforcement agents, emergency services personnel, technical support, cleaning staff, or even a vendor sending you patch software for your server. Anything to win your trust, giving them access to their target.

**Sometimes they may simply** do a "walk through" in which they walk through an area and see what files or passwords they can find that are left out on office desks. Areas that are especially targeted are reception desks, open offices, kiosks and server / switch closets that are unlocked or easily accessible.

**Be sure that you know** who has access to areas that are off limits to the general public. Lock doors to your office, server rooms, switch closets, etc. when you leave (if even for just a moment). This will help prevent unauthorized access / intrusion.

# BASIC NETWORK SECURITY GUIDELINES AND STANDARDS



**Information  
Security  
Office**

*Document maintained 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: 11/14/07, Information Security [security@uta.edu](mailto:security@uta.edu))*

## Purpose of this Brochure

This brochure helps provide a security standard for network managers and system administrators to follow when setting up servers and networks, helping prevent unauthorized compromises and disclosure of sensitive information.

In addition to this brochure you should have also read the brochure "Protect Your Computer and Sensitive Information" [www.uta.edu/security](http://www.uta.edu/security)

## SERVER REGISTRATION

All UT Arlington servers must be registered with Information Security: [security@uta.edu](mailto:security@uta.edu) / x25487.

## NETWORK VULNERABILITY SCANS

UT Arlington Information Security Office, upon request, will provide a scan of your UT Arlington server / network for vulnerabilities. This scan checks for missing O/S patches, outdated or missing anti-virus software, open ports, remote file access, p2p, spyware, viruses and bot networks. For scan requests: [security@uta.edu](mailto:security@uta.edu) / x25487.

## RESTRICT USER ACCESS

Unless technically prohibitive all server applications will utilize the Cedar (Kerberos / LDAP) for NetID user authentication and directory information. See [www.uta.edu/cedar](http://www.uta.edu/cedar) for details.

Each user having access to UT Arlington servers must have a uniquely identifiable account. Generic, common or shared accounts are strictly prohibited and in violation of state law. If a user requires root access, **sudo** or similar technologies must be implemented to ensure accountability.

User access will be periodically reviewed. All accounts and access privileges should be adjusted and limited accordingly. In the event that a user is terminated, Human Resources x25554 and OIT Information Security Office x22271 should be notified immediately. For information on "clearance form" contact [helpdesk@uta.edu](mailto:helpdesk@uta.edu) / 817.272.2208

## BUILDING YOUR SERVER

- It is highly recommended that servers be located and managed by the OIT Server Team. Contact: [helpdesk@uta.edu](mailto:helpdesk@uta.edu) / 817.272.2208 Consult checklists: [security.utexas.edu/admin](http://security.utexas.edu/admin)
- Backup your server and regularly test your backups for accuracy and dependability. Rotate and store them offsite if possible.
- Systems must be built offline. Download patches and virus definitions onto a secure, virus free machine and then install them onto your build.
- Install antivirus software. UT Arlington has an enterprise license, contact OIT Information Security Office for a server client. [security@uta.edu](mailto:security@uta.edu)
- A system vulnerability assessment should be performed prior to placing the device online. OIT Information Security Office can perform assessments upon request: [security@uta.edu](mailto:security@uta.edu) x25487
- Turn on the firewall. Check to see what ports are required by your applications and remove unnecessary services.
- There should never be any FTP or Telnet services running on any UT Arlington Servers.
- Server system and application logging is required so that if your server is compromised it will be easier to determine what may have been accessed and the method of compromise.
- Place server on an Uninterruptible Power Supply (UPS) with power surge protection.
- Again, connect your server to the network only after you have patched the operating system and applications (offline), you have installed and updated the antivirus software (offline), and it's been placed behind the OIT approved firewall.
- All servers / applications will be patched / updated on a scheduled and reoccurring basis.
- All servers will have documented disaster recovery and continuity plans, regularly updated.
- Conduct a "Business Impact Analysis (BIA)" of your servers. Use the BIA as a tool to create a "Disaster Recovery Plan". Test this regularly!

## WINDOWS SERVERS

You must install and run MBSA (Microsoft Baseline Security Analyzer) to check for security risks and outdated patches. [www.microsoft.com](http://www.microsoft.com)

Implement VPN for users to access UT Arlington servers. This creates a tunnel through the firewall allowing for secure traffic to flow to and from the users computer to UT Arlington servers. For information on VPN: [www.uta.edu/vpn](http://www.uta.edu/vpn)

Wireless encryption is available for all wireless access points on campus. Encryption is required in Davis, Wetsel, UTACC and recommended for improved security in all areas. For information on wireless encryption and wireless access points (WAP) visit: [www.uta.edu/wireless](http://www.uta.edu/wireless) You can also request a wireless account from this page for campus visitors. WAP requests should be sent to [helpdesk@uta.edu](mailto:helpdesk@uta.edu) / 817.272.2208

## UNIX AND LINUX SERVERS

UT Arlington has purchased a site-subscription for Red Hat Enterprise Linux. This subscription allows us to offer an enterprise-class Linux operating system and accompanying services to current students, faculty, and staff members for both personal and institutional use.

Departments wishing to deploy Linux are strongly encouraged to deploy Red Hat Enterprise Linux. No other distribution is supported by OIT. For information visit: [linux.uta.edu/rhel](http://linux.uta.edu/rhel)

Departments wishing to deploy a server, but without expertise to do so, must contact the OIT Enterprise Operations and Systems Group for details on services to assist in your deployment. For more information visit: [www.uta.edu/oit/eos](http://www.uta.edu/oit/eos)

## WINDOWS / UNIX / LINUX SERVERS

UT Arlington has encrypted services (such as SFTP and SSH) that will be used in place of clear text services (such as FTP or Telnet). FTP and Telnet must be disabled since they pose a potential security risk. BitVice is now the recommended utility. Contact [helpdesk@uta.edu](mailto:helpdesk@uta.edu) / 817.272.2208