

**YOUR RESPONSIBILITY**

You represent Texas A&M AgriLife when you use or access any information resource. You are part of a shared network and are individually responsible for the way you use AgriLife resources.

**Acceptable Use**

Web browsing for educational information and resources

Business-related email

Web browsing to access agency and Texas A&M University resources

Websites for official business

**Unacceptable Use**

Sending or forwarding chain mail

Personal use or profit

Promoting personal or family websites or services

Transmitting offensive, fraudulent, harassing, or nonbusiness promotions

Using peer-to-peer networking to exchange movies, music, or nonbusiness documentation

As a user of Texas A&M AgriLife information resources, you should be familiar with and adhere to established procedures regarding

**Internet and email use**

**Software installation and licensing**

**Passwords**

**Virus protection and workstation security**

**Portable computing**

**Physical security**

**Backups**

**Internet and Email Use**

Ensure that your communications are for professional reasons.

You are responsible for all content you store and send.

Official communications must have an appropriate signature block.

Do not transmit copyrighted material without permission.

Virus scan all files received through the Internet.

DO NOT click on email attachments that are from unknown sources or that seem unusual in any way.

Avoid transmitting private customer or employee information. When transmission is necessary, take steps to ensure the information is protected.

Your email is not private and is not secure; it can be accessed and viewed by authorized staff in certain situations and for specific purposes.

DO NOT copy, transfer, rename, add, or delete programs or information owned by another person without express permission from the owner.

**Software Installation and Licensing**

Install and use software only if it has a business or computer-maintenance purpose, is owned by AgriLife, and is specifically licensed for your computer.

DO NOT copy software, except as allowed specifically by the license.

Maintain proof of purchase, media, license certificate, box, or other documentation showing that software is properly licensed.

Keep licensing documentation near the computer or in an easily accessible central file.

Information technology (IT) support staff members can remove nonbusiness or unlicensed software from your computer and are restricted from installing software that does not have proof of purchase.

**Passwords**

You must use a password.

Your password must be reset every 90 days for resources with mission-critical data and every 180 days for all other resources.

## WHAT ARE THE AGENCY PROCEDURES?

As a “user” of Texas A&M AgriLife information resources, you have certain responsibilities. They are defined in the user responsibility sections of the agency procedures, titled *Information Security, Computer Use and Software Installation/Use*, which can be found online at

[agbr.tamu.edu/policies.btm](http://agbr.tamu.edu/policies.btm)

Specifically, they are section 21.99.10.X1.01 for the Texas AgriLife Extension Service and section 21.99.10.A1.01 for Texas AgriLife Research.



## Passwords

- must be at least 8 characters in length and include upper- and lowercase letters and numbers;
- should not be something easily tied to you, such as your name or nickname or your child’s or pet’s name;
- should not be simple dictionary words or acronyms;
- should be different from personal passwords.

DO NOT give your ID and password to anyone. If it is necessary to do so for a repair, you should change your ID and password when the repair is complete.

Activate a screen saver on your computer that requires your password to be re-entered (see “Tip Sheet 1: Locking Your Screen”).

Neither you nor your IT support should ever disable passwords.

You are responsible for all transactions made using your ID and password.

Change your password if you suspect it has been disclosed.

## Virus Protection and Workstation Security

Computer viruses, Trojans, worms, spyware, and other such malicious applications are designed to make unauthorized changes to programs and data and therefore can destroy agency resources.

Viruses are easier to prevent than cure; you **MUST** use an anti-virus program and you **MUST** ensure it is up-to-date. AgriLife provides Sophos End Point anti-virus software at no cost to your department. We recommend you take advantage of Sophos to meet this requirement. Please contact your IT manager or call AgriLife Information Technology (AIT) for a copy.

Use only trusted sources for data and programs, and scan downloaded files before using or installing.

For day-to-day login and operation, use a non-administrator account. This strategy will restrict an accidental infection from damaging critical files on your computer (see “Tip Sheet 2: Creating a Standard User Account”).

Ensure that your operating system and installed software are set to receive updates and are applied at monthly intervals.

DO NOT load diskettes, USB drives, CDs, or DVDs that are of unknown origin; they could contain viruses.

If you get a virus alert or believe you have an infection, unplug your network cable or turn off your wireless network, and contact your IT support for help.

Before connecting a new computer (workstation or server) to the network, ensure that anti-virus software is installed and functional and that you have followed these security guidelines.

If you use email other than the AgriLife standard, ensure that the email system has virus protection enabled.

DO NOT use Internet chat software to transfer files; these are known sources of infections.

Report any infections or security issues to [securityhelp@ag.tamu.edu](mailto:securityhelp@ag.tamu.edu).

## TECHNICAL SUPPORT

### Need help?

Call your regional IT specialist, unit IT staff, or the FirstCall Help Desk.

### FirstCall

Toll Free: (866) 996-2056  
College Station: (979) 985-5737  
first-call.tamu.edu  
Fax: (979) 845-0829

### Regional Specialists

Steve Paz, Lubbock  
Weldon Floyd, Stephenville  
Aimee Sandifeer, Overton  
Greg Thomas, Bryan  
Pete Flores, Corpus Christi  
Jeffrey SoRelle, San Angelo

### Looking for more?

[ait.tamu.edu](http://ait.tamu.edu)  
[ittoolbox.tamu.edu](http://ittoolbox.tamu.edu)

Report security issues to  
[securityhelp@ag.tamu.edu](mailto:securityhelp@ag.tamu.edu)

AgriLife Information Technology  
2468 TAMU  
College Station, TX 77843-2468

## Portable Computing

The small size and convenience of notebook computers, smart phones, and USB drives make them useful for our business. These same features increase the likelihood for loss and increase our responsibilities.

You **MUST** use a password or other means of entry.

All sensitive data must be stored in encrypted format (see “Tip Sheet 3: Encrypting Portable Drives”).

Wireless transmission must **NOT** be used unless proper security protocols are enabled.

Use AgriLife networks when possible to access AgriLife IT resources. Use VPN when accessing agency resources from other Internet connections.

If you use a personally owned device on AgriLife networks, it must meet all standards and procedures.

## Physical Security

Protect information resources based on their value to the agency.

Access to resources with mission-critical or sensitive data should be restricted and managed.

Access should be reviewed periodically and removed for those no longer needing it.

DO NOT share keys, access cards, or passwords to resources with anyone.

Keep portable devices and storage media out of sight, locked up, and protected.

Use a UPS (battery backup system), and protect your computer from environmental hazards.

You are accountable for agency-owned electronic equipment assigned to you.

## Backups

All electronic information of institutional value **MUST** be copied onto backup storage media on a regular basis (i.e., backed up) for disaster-recovery and business-continuity purposes.

You should establish and write down your method for regular backup and how to restore.

How often to back up depends on the importance of your data, but you should keep at least two copies.

For mission-critical data you **MUST** store one backup copy off-site in a secure location. Contact your IT resource to find out what backup services are offered in your area.

You can copy mission-critical data to a managed file server to help protect the data.

## Tip Sheet 1: Locking Your Screen

### TECHNICAL SUPPORT

#### Need help?

Call your regional IT specialist, unit IT staff, or the FirstCall Help Desk.

#### FirstCall

Toll Free: (866) 996-2056  
College Station: (979) 985-5737  
first-call.tamu.edu  
Fax: (979) 845-0829

#### Regional Specialists

Steve Paz, Lubbock  
Weldon Floyd, Stephenville  
Aimee Sandifeer, Overton  
Greg Thomas, Bryan  
Pete Flores, Corpus Christi  
Jeffrey SoRelle, San Angelo

#### Looking for more security tips?

[ait-security.tamu.edu](mailto:ait-security.tamu.edu)  
[first-call.tamu.edu](mailto:first-call.tamu.edu)  
[ittoolbox.tamu.edu](mailto:ittoolbox.tamu.edu)

Report security issues to  
[securityhelp@ag.tamu.edu](mailto:securityhelp@ag.tamu.edu)


AgriLife Information Technology  
2468 TAMU  
College Station, TX 77843-2468

Each time you get up from your desk during the workday, your computer is vulnerable to unauthorized access of your files, email, or programs, since you are still logged in.

To prevent such access, set your computer screen and keyboard to lock when you leave the office. (It doesn't hurt to lock the door too, if you have one.)

When activated, the screen lock setting will require you to type in your password to unlock the screen and resume computer use.

### Microsoft Windows Users

If you are a Windows user, you can lock your screen quickly by pressing Windows logo key  +L

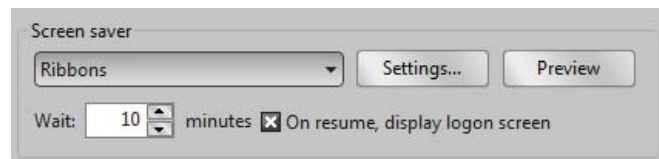
(If you have wondered what that key was for, this is only one shortcut; look up the logo key in Windows Help for a full list.)

### Windows Screen Saver

If you have a screen saver set on your Windows computer, it is simple to add the lock option. In your display preferences for the screen saver:

1. Check the option "On resume, display logon screen."
2. Set timer (we recommend 10 minutes, but less time is better).

When you walk away, your computer will lock after 10 minutes. When you return, just type in your password to get back to work!



### Macintosh Users

1. Open System Preferences, and then click Security.
2. Select "Require password to wake this computer from sleep or screen saver."

When you return, use your account user name and password to unlock the screen.

## Tip Sheet 2: Creating a Standard User Account

Texas A&M AgriLife computers support two types of user accounts: administrator and standard.

An administrator account gives permission to install software, change settings, and even reconfigure your operating system and disable such features as anti-virus software. Using an administrator account for everyday computing can make your computer vulnerable to infection with viruses and other malicious software and can allow hackers to gain full administrative access to your computer.

A standard account has limited permissions; while logged in to your standard account, you cannot install software or make configuration changes unless you confirm them by giving an administrator password.

For the best security you should use a standard user account as your daily login.

### Microsoft Windows User Account Setup

In Windows, user account setup is found in the Control Panel.

From the Start menu, open Control Panel.

Click User Accounts to open the dialog.

For Windows Vista and Windows 7, click “Manage another account.” (If you are prompted for an administrator password or confirmation, you are already using a standard account. You will need to type the password or provide confirmation.)

Click “Create a new account.”

Type the name you want to give the standard user account.

Click “Standard User Account type” (called Limited in Windows XP).

Click “Create Account.”

Click on the account to open it.

Click “Create a password.”

Type in your password and confirm it; then click “Create.”

Exit the Control Panel—account setup is complete.

The next time you log in you will see the new account on the Welcome Screen.

### Macintosh User Account Setup

On the Mac, account setup is found in System Preferences.

From the Dock or the Apple menu, open System Preferences.

Click Accounts to open the dialog.

You may need to click the lock to make changes. If so, you will be prompted for the master account password.

Click on the + symbol to add a new account.

Select “Standard” for the “New Account type.”

Enter a name for the account.

Enter a password and confirm it.

Click “Create Account.”

Be sure to click the lock to prevent unwanted changes.

Exit Accounts—setup is complete.

*Note about Mac logins:* If your Mac starts up and doesn't prompt for a password, Automatic Login is enabled. To disable Automatic Login, go back to Accounts, click “Login Options” and select “Disabled for Automatic Login.”



## Tip Sheet 3: Encrypting Portable Drives

External, portable data-storage drives, such as USB external drives, flash drives, and solid-state pocket-size drives — as well as DVDs and CDs — are popular for making backups and for transporting and sharing digital information.

When you use these with any sensitive data, they must be fully encrypted. This is a State of Texas requirement.

There are three strategies for protecting portable drives:

1. Set an access password.
2. Use the device's built-in security system.
3. Install and use full disk encryption software.

The first method offers some protection but is fairly easy to circumvent and access the data.

The second method depends on the device. Some are very good, like the IronKey flash drive. Others are far less secure. Look for drives that use 256-bit AES encryption.

The third method offers a way to be consistent and to use the USB and flash drives you already have. Our favorite full disk encryption software is TrueCrypt.

### Need to buy a new portable drive?

Here are some with built-in security you might consider:

- IronKey flash drive
- Maxtor (now Seagate) BlackArmor

Look for 256-bit AES encryption.



### Using TrueCrypt Software

TrueCrypt is available for both Microsoft Windows and Macintosh at [truecrypt.org/](http://truecrypt.org/). Review the beginner's tutorial at [truecrypt.org/docs/?s=tutorial](http://truecrypt.org/docs/?s=tutorial).

You can use one of two methods to create a storage volume to encrypt sensitive data:

1. Create a file, called a container.
2. Encrypt an entire drive, such as a USB backup drive.

Since you are protecting sensitive information that is on a portable device (either for backup or for transportation), you can either use the container method or encrypt all of the removable drive (if you create a container the size you will need and encrypt a whole drive, the container will use it all). The best protection for sensitive data is to purchase a specific removable drive for that data and then encrypt the entire drive.

You can also make the TrueCrypt storage volume hidden, if you choose, as an added layer of protection. Even if your password is compromised, the volume is not readily visible. Use the 256-bit AES option when creating the volume, and use the default "hash algorithm."

Enter a password; longer is better. You can also create optional key files for another layer of protection.

Finally, format the volume, using either the FAT or the NTFS file system. NTFS is the Windows XP, Vista, or Windows 7 file system, but all can use the simpler FAT system.

Once the volume is created, you must run TrueCrypt and "mount" the volume to gain access to the files, so if you use more than one computer, remember to install TrueCrypt on all of them.