# SPH Laptop Policy

Beginning January 2007, new rules go into effect regarding the configuration and use of laptops at the University. These changes apply to all laptops purchased through the University, regardless of the source of funds. This website has been designed to provide you with the most relevant information regarding these changes and how it will impact you and your laptop.

Below are links to the SPH Laptop User Agreement and a short video showing how to use a cable lock.

- **SPH Laptop User Agreement**
- **Video Showing Use of Cable Lock**

## Why are we doing this?

For years there has been no formal policy governing the use and configuration of laptops. As you may have heard, laptop theft has been on the rise for many years and has been linked to a number of identity theft cases. The UTHSC campus has its share or laptop theft as well. As a result, UT System has issued new rules governing the protection of certain data, including Social Security Numbers, Research data, and other forms of sensitive and confidential data. It should be of no additional surprise that many staff, faculty, and even students, keep this kind of data on their laptops and other storage devices. In the future, there will be greater forms of audit and compliance regulation governing the storage and protection of certain data types. In the end, despite the rules and regulations, we are to be good public stewards of the information entrusted to us; therefore, protection of this data is simply the right thing to do.

## Does this apply to my laptop?

The simple answer is "yes". All laptops, regardless of funding source, are governed by the new UTHSC Laptop Policy. Laptops, like other equipment, are considered "controlled" assets and are therefore subject to any and all applicable rules and regulations the State would like to place on them. There can be *exceptions* to this policy. However, any laptop assigned to any specific person or group of persons will not be granted an exception, even if the person(s) using the laptop indicate they do not store any data elements which are considered protected or confidential in nature. If you think you may have an exception case, please consult with **Derek Drawhorn**.

### What does this policy make me do?

The policy basically does three things:

- installation of  whole disk encryption on your laptop hard drive,
- use of a laptop cable lock (optional, in some cases),
- signing of a laptop user agreement

All three of these will be covered later in this document.

### What about my personal laptop?

If you have a personally owned laptop, you should also become compliant with the new policy; however, the University will not supply you with any of the needed software or hardware to become compliant.  To help in this regard, UTHSC IT Security will be creating a website which will assist laptop users with securing their laptops in accordance with this policy.  Becoming compliant may incur some expense for both a software encryption product and a cable lock.  This site, once completed, will be linked from this webpage.

### What is encryption?

By definition, encryption is the process of obscuring information to make it unreadable without special knowledge.  UT System has entered into a contract with **Safeboot Corporation** to provide all laptops with whole disk encryption technology.  Starting in the Fall 2010, certain laptops may also be encrypted with Microsoft encryption technology known as BitLocker.  It should be noted that BitLocker does require an additional chipset manufactured into the laptop and that not all laptops have this chipset installed.  Once your laptop drive has been encrypted, it will remain encrypted no matter what, even if the drive is removed and installed into another computer.  Applying whole disk encryption DOES mean that you will have a password to enter when the laptop boots.  This password must be a strong password in accordance with the University's password policy.  The password must be at least 8 characters in length and have a mix of characters with upper, lower, and numerals represented.  The password will also expire every 90 days.  Unfortunately, this password is NOT directly associated with our password servers, so it will not be synchronized with your domain account.  However, you will be able to manually change your laptop password whenever you like.  This will give you an ability to keep them synchronized yourself.

## What is a cable lock?

In May, 2011, UTHSC Information Technology Security modified its position on the use of laptop cable locks. If you can otherwise secure your laptop when you are not using it, such as a locked office door, cabinet, drawer, or other means, then you will not need to purchase or carry a cable lock with your laptop. However, if you are unable to physically secure your laptop, a laptop cable lock will be provided to you with your laptop purchase.

A cable lock is designed to physically secure your laptop to an immovable object. Typically, a cable lock includes a cable, a locking mechanism, and a device to secure your laptop to the lock. SPH will be providing a laptop cable lock, free of charge, to all employees with a University laptop. These locks are manufactured by Belkin and are shown in the picture below.

You may also watch **this short video clip** demonstrating how to use the cable lock. The one thing we cannot specifically indicate to a laptop user is *when* to use the cable lock. Below are some recommendations regarding how best to use your cable lock.

- **When Using Your Laptop**. You do not need to secure your laptop with the cable lock when you are actively using your laptop, or when the laptop is in your physical possession. It is assumed that if someone attempted to steal your laptop while you are using it, or while in your possession, that you would engage in some course of action to stop the theft.
- **Leaving Your Laptop in your Office Overnight**. The number one place laptops are stolen is from the workplace. Your locked office is not a safe place to leave your laptop in the open. At SPH, many people have access to your office. If you have a lockable cabinet or drawer, you should secure your laptop overnight in one of these compartments, providing a double layer of locked protection between a thief and your laptop. While the device is locked in the drawer/cabinet, there is no reason to use the cable lock. *(Never attempt to charge your laptop battery while the laptop is in a confined space, such as a drawer or cabinet. This is a serious fire hazard.)*
- **Leaving Your Laptop in a Car**. This is the second most frequent place where laptops are stolen. SUVs, or similar vehicles without a trunk, are especially vulnerable to laptop theft. If you have a car with a trunk and must leave your laptop in your vehicle, consider leaving it in the trunk and not using the cable lock. If your laptop can be seen through a window, consider keeping a small blanket in your vehicle to cover the laptop. You may also want to

use the cable lock and secure the laptop bag to the under-carriage of a seat where there is strong metal support to the frame of the vehicle.

- **Leaving Your Laptop in a Hotel Room**. It would be the recommendation of IT Services to use the cable lock if you must leave your laptop in a hotel room. However, you may have trouble finding a good object to secure the cable lock.

- **Using Your Laptop at Home**. You should attempt to secure your laptop when it is at your residence, especially if nobody will be at the residence. You can be guaranteed, if a thief enters your home, the laptop is the first item out the door. If they have to spend any time working to free the laptop from the cable lock, they may move on to other items.
- **Laptop Bag**. Another innovative way to throw thieves off your trail is by not traveling with a laptop bag which is so obviously a laptop bag. There are a number of companies who manufacturer laptop carry bags which look more like brief cases, shoulder bags, or even back packs which help to deter a thief from knowing what you are carrying. **This link is a company with several examples**.

***Note:*** SPH IT Services fully understands that these cable locks will not prevent a seasoned thief from stealing your laptop. They are quite easy to defeat. However, a thief is notorious for (1) looking for the easy steal, and (2) not getting caught in the act. A cable lock is merely a deterrent which will give the thief pause to consider whether they want to spend the extra time required to defeat the security mechanism.

### SPH Laptop User Agreement

All laptop users must acknowledge and sign a "laptop user agreement". You will be presented a copy and asked to sign the agreement when you pick up your laptop after encryption has been installed. The signed agreements will be kept on file with IT Services. Feel free to read over the agreement, linked at the top of this page, and forward any questions you may have to **Derek Drawhorn**.

### Frequently Asked Questions (FAQ)

**Does Safeboot support the Linux operating system?** It does support some flavors of Linux. Please contact IT Services for additional help in this regard.

**Does Safeboot work on Macintosh computers?** Not at this time. The OS X operating system supports an internal feature known as FileVault, which is a folder based encryption tool for Macintosh computers. While it is not whole disk encryption, it is the best alternative for Macintosh computers at this time. If you need additional information on how to properly configure FileVault, please contact IT Services.

**Can you give me a license of Safeboot for my personal home computer?** No. At this time, all license are for UT owned laptops. IT Security will be providing a new website with information on how best to secure your home computers, including drive encryption.

**How will Safeboot affect my laptop's performance?** Safeboot will have a very small impact on your laptop performance when writing files. One of the key features in why Safeboot was selected was based on its low impact to performance ratio. Laptops greater than 3 years old and not running either Windows 2000 or Windows XP will likely see the greatest impact on performance.

**I share a laptop with several other people, how will this new laptop username and password work?** Safeboot handles this issue fairly well. All users who use a laptop will be put into a special group within the Safeboot server environment. As a result, any user in that group can access any laptop also in the group. In this way, multiple people all can have access to the same laptop using their own Safeboot username and password. There will be no need to share a password with another person. When you bring in your laptop for encryption, let us know if other people will also be using the laptop.

**What if my laptop is too old for the Safeboot software?** If your computer is very, very old, IT Services recommends you secure the funds necessary to replace the laptop. Safeboot will work on many platforms, but we cannot guarantee how well it will perform on extremely old hardware, especially if it is not a name brand, such as Dell, IBM, HP, or Gateway.

**What if I just don't want to do this?** This question has been posed to me several times and it is a respectable question. If you have some serious doubts about doing this, please contact Derek Drawhorn with your reasoning; however, in the long run, all laptops are to conform to the policy. Audits are routinely expected in the coming years.