This document explains the acceptable use of encryption for the UTHSC system. It includes: acceptable encryption software, techniques, algorithms and instructions. Encryption methods and software are arranged by operating systems.

Acceptable Encryption Usage for UTHSC

Avoiding the legal hassles of stolen computers, thumb drives, and portable devices.
# Table of Contents

Purpose ........................................................................................................................................... 2
Introduction ....................................................................................................................................... 2
Microsoft Windows Systems .................................................................................................................. 3
  Turning On BitLocker Drive Encryption on a Fixed or Removable Data Drive (Windows 7) ... 3
  Using BitLocker to encrypt a USB Flash Drive .............................................................................. 5
  Using BitLocker To Go Reader (for Windows Vista and XP Only) .............................................. 8
Macintosh and Linux Systems ............................................................................................................... 10
Xythos ................................................................................................................................................. 12
Appendices for FIPS 140-1 and FIPS 140-2 Validation ................................................................. 14
  Appendix A - Advanced Encryption Standard Algorithm Validation List .............................. 14
  Appendix B - Validated Cryptographic Modules List ................................................................. 15
  Appendix C - Cryptographic Program Modules Validation In Process List .......................... 16
Acceptable Encryption Usage for UTHSC

Purpose
This document explains the acceptable use of encryption for the UTHSC system. It includes: acceptable encryption software, techniques, algorithms and instructions. Encryption methods and software are arranged by operating systems.

Introduction
Enabling UTHSC users to protect sensitive data is the job of IT security. Protecting sensitive UTHSC data is the job of the user. This document empowers users to protect months and years of research, protect privacy of patients, and guard against the costly and damaging effects of compromised data. Be informed, be protected and be secure.

Objectives:

1. Provide access to validated encryption software
2. Provide instruction for use
3. Supply supporting documentation of validation

Compliance with NIST Standards and Guidelines

In accordance with the provisions of FISMA, the Secretary of Commerce shall, on the basis of standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to federal information systems. The Secretary shall make standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of federal information systems. Standards prescribed shall include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.

• Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and binding for federal agencies.2 FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.

• Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management), state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.3

• Other security-related publications, including interagency reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST’s activities. These publications are mandatory only when specified by OMB.

• Compliance schedules for NIST security standards and guidelines are established by OMB.
Microsoft Windows Systems

Turning On BitLocker Drive Encryption on a Fixed or Removable Data Drive (Windows 7)

Updated: August 26, 2009
Applies To: Windows 7

This scenario provides the procedure for turning on BitLocker Drive Encryption protection on a fixed or removable data drive on a computer.

⚠️ Caution

When encrypting a removable drive, do not suddenly remove the drive. If you need to remove a drive before encryption is complete, pause the encryption process and then use either the Safety Remove Hardware icon from the notification area or the Eject command from Windows Explorer to remove the drive. Removing the drive during the encryption process without pausing and intentionally removing the device can cause the data on the drive to be corrupted.

Before you start

To complete the procedure in this scenario:

- You must be able to provide administrative credentials to turn on BitLocker for fixed data drives. Standard user accounts can turn on BitLocker To Go on removable data drives.

- You must be able to configure a printer if you want to print the recovery key.

- Your computer must meet BitLocker requirements. For more information, see "Requirements for BitLocker Drive Encryption" in BitLocker Drive Encryption Step-by-Step Guide for Windows 7.

To turn on BitLocker Drive Encryption on a fixed or removable data drive

1. Click Start, click Control Panel, click System and Security, and then click BitLocker Drive Encryption.

2. Click Turn On BitLocker for the fixed or removable data drive that you want to encrypt.
Acceptable Encryption Usage for UTHSC

[^Note]

If you have configured the Group Policy settings in your organization to back up BitLocker recovery information to Active Directory Domain Services (AD DS), the computer must be able to connect to the domain to complete this process.

3. The BitLocker setup wizard will ask you how you want to unlock this drive. Fixed data drives can be configured to automatically unlock when the operating system drive is encrypted, to unlock after a password is supplied, or to unlock after a smart card is inserted. Removable data drives can be configured to unlock after a password is supplied or to unlock after a smart card is inserted. If you want the removable data drive to automatically unlock, you can specify that option after encryption has occurred by clicking Manage BitLocker from the BitLocker Drive Encryption Control Panel item or by selecting the Automatically unlock on this computer from now on check box when you unlock the drive.
Acceptable Encryption Usage for UTHSC

4. Before BitLocker encrypts the drive, the BitLocker setup wizard prompts you to choose how to store the recovery key. You can choose from the following options:

- **Save the recovery key to a USB flash drive.** Saves the recovery key to a USB flash drive. This option cannot be used with removable drives.

- **Save the recovery key to a file.** Saves the recovery key to a network drive or other location.

- **Print the recovery key.** Prints the recovery key.

Use one or more of these options to preserve the recovery key. For each option that you select, follow the wizard steps to set the location for saving or printing the recovery key. When you have finished saving the recovery key, click **Next**.

---

**Important**

The recovery key is required when a BitLocker-protected fixed data drive configured for automatic unlocking is moved to another computer, or the password or smart card associated with unlocking the fixed or removable drive is not available, such as when a password is forgotten or a smart card is lost. You will need your recovery key to unlock the encrypted data on the drive if BitLocker enters a locked state. This recovery key is unique to this particular drive. You cannot use it to recover encrypted data from any other BitLocker-protected drive.

5. The BitLocker setup wizard asks if you are ready to encrypt the drive. Click **Start Encrypting**.

6. The **Encrypting** status bar is displayed. You can monitor the ongoing completion status of the drive encryption by moving the mouse pointer over the **BitLocker Drive Encryption** icon in the notification area, at the far right of the taskbar.

By completing this procedure, you have encrypted a fixed or removable data drive, associated a key protector with an unlock method for the drive, and created a recovery key that is unique to this drive.

### Using BitLocker to encrypt a USB Flash Drive

To enable BitLocker encryption on a USB flash drive, do the following:

1. Insert the USB flash drive, click **Start**, and then click **Computer**.

2. Right-click the USB flash drive, and then click **Turn On BitLocker**. BitLocker initializes the drive.
Acceptable Encryption Usage for UTHSC

3. On the Choose How You Want To Unlock This Drive page, choose one or more for the following options, and then click Next:
   - **Use A Password To Unlock This Drive** - Select this option if you want the user to be prompted for a password to unlock the drive. Passwords allow a drive to be unlocked in any location and to be shared with other people.
   - **Use My Smart Card To Unlock The Drive** - Select this option if you want the user to use a smart card and enter the smart card PIN to unlock the drive. Because this feature requires a smart card reader, it is normally used to unlock a drive in the workplace and not for drives that might be used outside the workplace.
Acceptable Encryption Usage for UTHSC

4. On the How Do You Want To Store Your Recovery Key page, click Save The Recovery Key To A File.

5. In the Save BitLocker Recovery Key As dialog box, choose a save location, and then click Save.

You can now print the recovery key if you want to. When you have finished, click Next.

6. On the Are You Ready To Encrypt This Drive page, click Start Encrypting. Do not remove the USB flash drive until the encryption process is complete. How long the encryption process takes depends on the size of the drive and other factors.

The encryption process does the following:
1. Adds an Autorun.inf file, the BitLocker To Go reader, and a Read Me.txt file to the USB flash drive.

2. Creates a virtual volume with the full contents of the drive in the remaining drive space.

3. Encrypts the virtual volume to protect it. USB flash drive encryption takes approximately 6 to 10 minutes per gigabyte to complete. The encryption process can be paused and resumed provided that you don’t remove the drive.

As a result, when AutoPlay is enabled and you insert the encrypted drive into a USB slot on a computer running Windows 7, Windows 7 runs the BitLocker To Go reader, which in turn displays a dialog box. When you are prompted, enter the password, smart card PIN, or both to unlock the drive. Optionally, select Automatically Unlock On This Computer From Now On to save the password in an encrypted file on the computer’s system volume. Finally, click Unlock to unlock the volume so that you can use it.

Acceptable Encryption Usage for UTHSC
Using BitLocker To Go Reader (for Windows Vista and XP Only)

BitLocker is more than just a USB protector. It protects any type of removable drive and it works independently of the OS's BitLocker, so "regular" BitLocker isn't required. However, BitLocker Reader must be installed on systems running Windows Vista or earlier.

(Go to Page 9)
Acceptable Encryption Usage for UTHSC

BitLocker To Go overlays a "discovery volume" on the physical drive, which contains the BitLocker To Go Reader and installation instructions. The reader is also available for download from the link below:


Install BitLocker To Go Reader following the wizard instructions.
Insert USB drive into USB slot.
Users can read from, but not write to, protected devices on Windows Vista and Windows XP. Only password-protected volumes (not smart card or domain) are usable with the reader.

Enter the password and click unlock.

NOTE: You will not be able to open the document from the drive, copy it to your desktop and open normally. If changes are made to the document, you will NOT be able to save it back on the USB drive.
Macintosh and Linux Systems

Encryption for the Macintosh (OS X Leopard, Snow Leopard, & Lion)

You can turn on disk encryption to encrypt the information in your home folder. Encryption scrambles the data in your home folder so that unauthorized users, applications, or utilities can’t access your data.

To set up disk encryption for your home folder, you must be an administrator on your computer, or you must get an administrator’s help.

When you turn on disk encryption for the first time, your home folder is encrypted. While your home folder is being encrypted, you won’t be able to log in to your account or use your computer to do other tasks. The process could take a while, depending on how much information you have in your home folder.

Before you begin, make sure you have enough free space on the hard disk that contains your home folder. You need as least as much free space as your home folder currently occupies. For example, if your home folder uses 20 MB, make sure you have at least 20 MB of available space. This space is needed temporarily during the encryption process.

You must create a master password in case you forget your regular login password.

WARNING:
Don’t forget your master password. If you turn on disk encryption and then forget both your login password and your master password, you won’t be able to log in to your account, and your files and settings will be lost forever.

To set up disk encryption on your computer:

1. Choose Apple menu > System Preferences, click Security, and then click Disk Encryption.

2. Open the FileVault pane of Security preferences.

3. If the Security preferences pane is locked, click the lock icon, and then type an administrator name and password.

4. If the Security preferences pane shows that a master password hasn’t been set, click Set Master Password, and then type a password in the Master Password box.
Acceptable Encryption Usage for UTHSC

5. Type the password again in the Verify box.

6. Type a hint in the Hint box to help you remember the password.

7. Click OK.

8. Click “Turn On Encryption”.

You are logged out of your account during the encryption process. When the encryption process is finished, log back in to your account. Your home folder icon changes to show that it’s encrypted.
Acceptable Encryption Usage for UTHSC

Xythos and ePHI

Xythos provides a collaborative work area for your data. By default, our installation of Xythos provides both secure data transmission and backup for disaster recovery. Xythos is suitable for use with ePHI (or other confidential data) if you follow the procedures below.

To use Xythos with ePHI, you must (1) enable ‘File Versioning’, (2) enable ‘File Logging’ on a per document basis and (3) change the defaults in “Issue Tickets” so that you identify your collaborators and provide them with a password. You will also need to have (4) an Access Report run that shows disclosure to others of your data before all your data is deleted. These four actions are required to comply with HIPAA and are not optional.

File Versioning

The Versioning function is an effective way to keep track of the changes made to any file. (See the online HELP file within Xythos for other information about Versioning.)

Turn Versioning on for a file:

1. Click the box next to your document.
2. Click on the Manage icon at the top of the screen and then choose Versioning.
3. Use the Enable Versioning button to turn versioning on.
4. Click the Exit button to exit the Versioning screen.

File Logging

The Logging option allows you to keep a record of who accesses your files and when they do so. The current Logging status of a file, on or off, can be seen in the file's Summary/Manage screen. When an action is performed against a file, an entry is added to the log history including:

- The user who performed the action
- The type of action performed
- The date and time the action occurred
- The IP Address of the machine from where the action occurred

Actions include but are not limited to users viewing or editing the file, permission changes, and file comments that are added, edited, or deleted. (See the online HELP file within Xythos for other information about File logging.)

Turn logging on or to view a history of file access:

1. Click the box next to your document.
2. Click on the Manage icon at the top of the screen and then choose Logging.
3. Within the Logging screen, click the Enable Logging button.
4. Click the Exit button to exit the Logging screen.

The Logging screen displays the history of who has accessed the file for the time period in which Logging is on. *Note that a logging history can only be applied to files, not to folders.*
Acceptable Encryption Usage for UTHSC

Issuing Tickets

To issue a ticket for a document containing ePHI, name your ticket to identify to whom you are sending the ticket, define the permissions you are granting your collaborator, set a lifetime for the ticket, and enable a password (the dialog box may say ‘optional’, but for ePHI, it’s NOT optional. See the online HELP file within Xythos for other information about Tickets.)

During the creation of a new ticket, the file or folder’s Permissions screen is updated with the new permissions.

To issue a ticket:

1. Select the file or folder you want to which you want to grant access.
2. Click the Manage button and select the Ticket option from the drop down menu.
3. Click on New Ticket.
4. Enter a name for the ticket if you wish. Select the appropriate permissions. Set the length the ticket will be valid (after this time the ticket will no longer allow access to this file). You may password protect this file. Click OK.
5. *Note: DO NOT include the password in the same email as the link to the file*
6. Edit the email if you wish. You can only change the text that is NOT inside the table. Click the Finish button.

Access Report

You should always have a report run that details the disclosure of that ePHI, for your records, before you delete the document. You will need to keep that report at least three years.

To run a report:

1. Choose the document in your Xythos area by checking the box name.
2. Choose Manage. Choose Logging.
3. The access log for that document will be shown on the screen. You should either screen-print or copy and paste the information into a document on your computer.

For more detailed help documentation and frequently asked questions, please visit the UTHSC Xythos webpage at:

https://academic.uthsc.edu/edtech/xythos/
Acceptable Encryption Usage for UTHSC
Appendices for FIPS 140-1 and FIPS 140-2 Validation

Appendix A - Advanced Encryption Standard Algorithm Validation List
Acceptable Encryption Usage for UTHSC

Appendix B - Validated Cryptographic Modules List
Acceptable Encryption Usage for UTHSC

Appendix C - Cryptographic Program Modules Validation In Process List