

Sponsor: Director, Desktop Support Group
Effective Date: October 22, 2008
Last Review Date: October 22, 2008
Report Errors: it_riskmanagement@uth.tmc.edu

TABLE OF CONTENTS

1.0 POLICY STATEMENT	2
2.0 RESPONSIBILITY	2
3.0 SCOPE	2
4.0 DEFINITIONS.....	2
5.0 STANDARDS.....	3
6.0 EXCEPTIONS.....	3
7.0 ENFORCEMENT (<i>optional</i>).....	4
8.0 CONTACTS.....	4
9.0 REVISION HISTORY.....	5

Portable Storage Device Policy

1.0 POLICY STATEMENT

All University of Texas Health Science Center at Houston (UTHSC-H) confidential or sensitive information that is stored or transported on portable media must be encrypted. Portable storage media are to include any device that allows for the removal and transport of computer files.

2.0 RESPONSIBILITY

The Desktop Support Committee is responsible for ensuring this policy is appropriate and current.

IT desktop support groups are responsible for maintaining and communicating a current list of acceptable portable storage devices, and/or for providing acceptable portable storage.

Users are responsible for storing confidential or sensitive data on encrypted portable devices, or by encrypting such files if stored on unencrypted portable devices. Users are responsible for reporting incidences of non-compliance.

3.0 SCOPE

This policy applies to all UTHSC-H faculty, staff, students and recognized university associates who have access to university-owned data and/or computer resources.

This policy specifically addresses encryption solutions for external drives and flash drives. It does not address portable devices other than the ones listed below. Other portable devices should either not be used for storage of sensitive or confidential data or the user should find some other way to secure the data.

4.0 DEFINITIONS

Portable Storage Device Policy

Term	Definition
Confidential Information	Refer to HOOP 17.01
Sensitive Information	Refer to HOOP 17.01
Portable Storage Device	External hard drives and flash drives
Encryption	The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

5.0 STANDARDS

All purchased portable storage devices must include encryption technology compatible with university encryption standards established in policy by the UTHSC-H Information Security department.

IT desktop support groups will maintain a list of acceptable portable storage devices for purchase. This list should be made available and communicated to their users and to the purchasing community within their respective user community. IT desktop support groups should keep this list current with advances in technology corresponding to the needs of their user community.

Users may purchase portable storage devices found on the list of acceptable portable storage devices after obtaining approval from their IT desktop support group.

As an option, schools and departments may wish to fund a program to provide acceptable portable storage devices to their users. For instance, for users affiliated with university administration, the School of Nursing or the Dental Branch, one encrypted storage device will be provided by their IT desktop support group.

6.0 EXCEPTIONS

Portable storage devices previously purchased and implemented prior to the activation of this policy are grandfathered and allowed for use. However, any confidential or sensitive data stored on these portable devices must be encrypted. Local desktop support groups should encourage the use of alternative encryption technologies to provide acceptable encryption to these devices. When the device is replaced, the policy will apply.

Desktop support groups can deploy alternative encryption technologies under the following conditions: (a) the local IT desktop support group supports the users with the technology, and (b) the encryption technology complies with university [encryption guidelines](#).

Portable Storage Device Policy

Other exceptions to this policy must be approved by the IT Security Core Committee under the direction of the UTHSC-H [Chief Information Security Officer](#). Users requesting an exception to this policy must complete the IT Security Exception Request form, which will require the following information:

1. The specific exception being requesting (e.g. to purchase a portable device that is not on the approved list);
2. The justification for the exception (e.g. why a non-approved portable device must be used in lieu of an approved one);
3. The additional steps that will be taken or controls that will be put in place to mitigate the risk of inappropriate disclosure of confidential and/or sensitive data;
4. The type of data that will be stored on the portable storage device (e.g. personal information, HIPAA, FERPA, SSNs, etc.);
5. The time period for which the exception is being requested.

7.0 ENFORCEMENT

This policy is enforced through the procurement policy. It is also enforced when non-compliance is discovered through a report or observation.

8.0 CONTACTS

Name of Technical Contact	Title or Office/Department	Telephone	E-mail
Derek Drawhorn	School of Public Health	713-500-9533	derek.d.drawhorn@uth.tmc.edu
Bassel Choucair	Medical School/IMM	713-500-5034	bassel.choucair@uth.tmc.edu
Bob Andriola	Administration, School of Nursing, Dental Branch	713-500-3694	robert.b.andriola@uth.tmc.edu
Alfred Valladolid	Graduate School of Biomedical Sciences	713-500-9858	alfred.m.valladolid@uth.tmc.edu
Dat Phan	School of Health Information Sciences	713-500-3928	dat.q.phan@uth.tmc.edu
Vernon Chandler	UT Physicians	713-500-6945	vernon.e.chandler@uth.tmc.edu
Shamus Sadai	Harris County Psychiatric Center	713-741-8644	shamus.sadai@uth.tmc.edu

Portable Storage Device Policy

9.0 REVISION HISTORY

Preparer's Name	Revision Date	Reason For Change	Version	Approver's Name	Approval Date
Derek Drawhorn	Jul 29, 2008	Initial document	1	NA	NA
Kim Beckett	Oct 9, 2008	Added Standard for users who will be provided encrypted storage device. Reviewed at 10/21 DSG meeting.	1.1	NA	NA
Kim Beckett	Oct 22, 2008	Updated for minor changes requested at 10/21/08 DSG meeting.	1.2	NA	NA
Kim Beckett	Oct 29, 2008	Updated to address review comments agreed upon at 10/29/08 IT Direct Reports meeting.	1.3	NA	NA
Kim Beckett	Oct 31, 2008	Updated section 3.0 to further define the scope.	1.4	NA	NA
Kim Beckett	Nov 5, 2008	Approved version.	1.5	Rick Miller, CIO	Nov 3, 2008