THE UNIVERSITY of TEXAS
HEALTH SCIENCE CENTER
AT HOUSTON

Submit by Email | Print Form

Information Security Policy Exception Request Form

The purpose of the Information Security Policy Exception Request Form is to allow University of Texas Health Science Center at Houston (UTHSC-H) System Owners or their approved delegates the ability to request specific exceptions from policies for Information Technology systems under their purview.

Full Disk Encryption (FDE) Exceptions
The requestor and/or their delegate agree to the following:

Exceptions can be granted on a temporary basis with a starting and expiration date or on a permanent basis. All exceptions are still subject to a review process and the exception may be revoked if current policies or the information in this request changes.

Hardware Security Requirements
Personal Computers (PCs) and laptops requesting exception are still required to meet UTHSC-H Host Configuration Security Policy and Acceptable Encryption Policy requirements. These requirements include:

PCs and Laptops:

- PCs/Laptops are regularly reviewed and updated for anti-virus, OS patches, and malware/spyware (at a minimum every quarter, monthly if possible).
- Passwords are changed in respect to the UTHSC-H password policy.
- Security Policies are implemented to insure screen savers are set to lock systems after 15 minute of inactivity.
- PCs/Laptops are inventoried and enumerated on each subsequent Exception Request.
- All other applicable University IT Security Policies, Procedures, Standards and Guidelines.

Laptops Only

- Local FDE-based user accounts must be used to access the encryption system installed on the laptop or tablet systems.
- Local FDE-based service accounts will only be used for accessing the laptop(s) named in this form request and cannot be deployed to other systems.
- Insure stewards are advised that labels, temporary or permanent, containing the FDE service account and passwords are not permitted (no exceptions allowed).
- Laptops must be inspected at check in and check out by a central authority (such as local LAN Manager, project manager or similar). This is to insure that stickers or similar notation is not adhered to the laptop containing the user account/password information for unlocking the encryption algorithm.

Note: Should the requestor or delegate be unable to fulfill the above requirements or any UTHSC-H Information Security policy, those items must be explained and included as part of this exception request.

Approval Process
Exception requests are approved or denied by the UTHSC-H Chief Information Security Officer.

Requests for appeal should be sent to the IT Security Core Team.

(Continued)

Other Exceptions
For those requesting exceptions other than Full Disk Encryption, exceptions based solely on the limitation of existing technology will be given serious consideration.

Example: PC or Laptop system cannot participate in the UTHOUSTON Active Directory and therefore receive required Group Policies (GPO).

The technical or logistical reasons supporting each exception must be included in the appropriate section of this form.

Department Contact Information

Department	
Employee Name	
Title	
Email Address	
Phone	
Delegate Name	
Phone Number	
Email Address	

List specific exceptions and supporting rationale to the PC/Laptop Security Standards in this section. Please include compensating controls, if any, required to maintain standards as outlined in the Host Configuration Policy.

Sensitive Information
If the PCs/laptops enumerated on this request are known to contain sensitive, protected or confidential data, the type of data (personal information, HIPAA, FERPA, SSNs, etc.) must be listed below.

Additionally, list the expected length of time the data to exist on the laptop systems before the data can be expected to be exported or otherwise purged.

Data Type	Anticipated Duration (if duration is unknown, mark "unknown")

System Owner (required)

I understand that by signing this form I agree to the terms and conditions set forth in this policy and agree to accept risk associated with this request.

Signature of Responsible Party

Date

Delegate Section (optional)

Signature of Responsible Party

Date

Hardware Requiring Exception (if necessary, append additional pages to the end of this request.)

	Computer Name	Serial Number	UTHSC-H Asset ID Tag#
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			