Texas State University
Annual Device Encryption Exception Request Form

Goals and Procedure for Requesting Exceptions

The main goal of device encryption is to protect confidential information entrusted to Texas State University. Because computing devices pose a significant risk for exposure of confidential information, encrypting these devices will make it infeasible for unauthorized retrieval of such information should a device be lost or stolen. The University understands there may be instances in which a device, or group of devices, may need to be exempted from the encryption standard. In these cases, a formal encryption exception request form must be submitted for written approval. Approved exceptions are valid for 365 days.

Instructions

Fill out this form as accurately and complete as possible. Print the document and acquire all appropriate signatures including Department Head/Chair and Dean/VP. When complete, e-mail a scanned copy of the signed form to the IT Assistance Center (ITAC) at itac@txstate.edu. ITAC will contact ISO for final approval and process all approved requests.

1. Requestor Information	
Requestor's First and Last Name	
Title	
Department	
Texas State E-mail Address	
NetID	

2. Device Information: (List individually. Please use final page for additional devices.)						
Tag #	**Computer Name**	**Operating System**	**Wired MAC Address**	**Wireless MAC Address**	**Owning Department**	**Primary Location (Building/Room #)**

3. Describe Current Use of the Device(s)

4. Justification for Exception: (Please provide a business justification for requesting the exception)

5. Describe in Detail Any Compensating Controls That Are in Place or Are Proposed

Example: I will assume responsibility for ensuring these computers are setup to automatically remove all confidential and personally identifiable information upon reboot with the use of a system wipe program or script (e.g., *DeepFreeze, Spiceworks, Reboot Restore, or script*).

Example: This device (these devices) will be physically locked to a permanent structure.

6. Requestor Acknowledgement

Initial these statements to confirm your acknowledgement. Requests will only be approved if all statements are initialed.

_____ **(Initials Required)** I ensure these computers will be encrypted when/if they are ever repurposed from a lab environment or if any of the above stated compensating controls are removed.

_____ **(Initials Required)** I ensure this device/these devices have already been scanned for confidential information using a data discovery program (e.g., *Identify Finder*). In addition, any confidential information identified has been removed.

I hereby acknowledge that I have read and understand the applicable regulations in UPPS No. 04.01.01 – Security of Texas State Information Resources (see section 04.09) and the Data Classification Guidelines by signing below:

_____	_____	_____
Printed Name	*Signature of Requestor*	*Date*

7. Approval/Denial:

Department Chair/Director:

_____	_____	_____	○ Approved ○ Denied
Printed Name	*Signature*	*Date*	

College Dean/Division VP:

_____	_____	_____	○ Approved ○ Denied
Printed Name	*Signature*	*Date*	

Please e-mail scanned form to itac@txstate.edu to complete the following requests.

IT Security Representative:

_____	_____	_____	○ Approved ○ Denied
Printed Name	*Signature*	*Date*	

Notes:

8. Annual Renewal Required

This form must be submitted for review and approval on an annual basis.

Expiration Date: _____

For more information, visit the Texas State Laptop Encryption Program website: https://itac.txst.edu/support/device-encryption.html

2.b. Additional Device Information: (Use only if additional space is needed. List individually.)						
Tag #	**Computer Name**	**Operating System**	**Wired MAC Address**	**Wireless MAC Address**	**Owning Department**	**Primary Location (Building/Room #)**

Additional Device Page # ____ of _____.