THE UNIVERSITY OF TEXAS AT EL PASO

REQUEST FOR DEVICE ENCRYPTION EXEMPTION

This form is to be used for requesting approval from exemption to The University of Texas at El Paso (UTEP) Device Encryption requirement, in accordance with the directive by The University of Texas System Board of Regents (UTS), and UTS 165 Information Resources Use and Security Policy, which states that all University owned/leased laptops and *desktops (containing Confidential Information or purchased after September 1, 2013)* must be fully encrypted using UTEP ISO approved methods.

|  |
| --- |
| **1. Requestor Information** |
| **Person Requesting Exemption:** | Click here to enter text. |
| **Title:** | Click here to enter text. |
| **Department:** | Click here to enter text. |
| **Email:** | Click here to enter text. |
| **Phone Number:** | Click here to enter text. |

|  |
| --- |
| **2. Goals and Procedure for Requesting Exception** |

The main goal of the Device Encryption requirement is to protect confidential information entrusted to the University. Because computing devices poses a significant risk to exposure of confidential information stored on them, encrypting these devices will make it unfeasible for unauthorized retrieval of this information should a device be lost or stolen. The University understands that there may be instances in which a device, or group of devices, may need to be exempted from this standard. In these cases, an approval for exemption request will be routed to your Director/Vice President, the President of The University of Texas at El Paso, and the CISO for final disposition.

**NOTE: Prior to requesting an exemption, this device/these devices may be required to
be scanned for confidential information.**

**Previously Exempted Devices:** Any previous or current exemptions will be reviewed by the CISO periodically.

Devices used for conducting University business **must** not be used without the express written approval as outlined in this document. In unusual cases, where a very unique piece of computing equipment is not otherwise encryptable, approval from the exemption to the Device Encryption requirement must first be sought. Approval will not occur until final approval has been granted by the appropriate parties herein. Additionally, University owned/leased devices that are granted an exception must have a visible label affixed to the device itself indicating that it **must not** be used for storing Confidential Information. Sample labels include: **“WARNING: This device is not encrypted and use with confidential information is strictly prohibited. Please contact the ISO at (915) 747-6324 if the device will be used for University business” or “WARNING: This device is not encrypted. DO NOT place confidential University information on this device. To do so is a serious violation of University policy”.**

**NOTE:** The purpose of the label is to alert individuals that the device **must** be encrypted if repurposed.

|  |
| --- |
| **3. Justification for Exception:** (Please provide a business justification for requesting the exemption from this standard) |
| Click here to enter text. |

|  |
| --- |
| **4. Device Information: (List individually. Please attach a page if needed.)** |
| **UTEP Inventory Tag #, MAC Address, or** **Serial Number** | **Device****Host Name** | **Owning****Department** | **Device Physical Location****Building/Room #** |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

Instructions for retrieving the Host Name and other information may be found here:

* [IP and MAC Address Look-up](https://www.utep.edu/information-resources/iso/_Files/docs/IP%20and%20MAC%20Address%20Lookup.pdf)

|  |
| --- |
| **5. Describe the Current Use For Device** |
| Click here to enter text. |

|  |
| --- |
| **6. Provide Detailed Reason Why Encryption Cannot be Performed** |
| Click here to enter text. |

|  |
| --- |
| **7. Provide Detailed Reason Why Device Cannot be Retired or Replaced (if you are providing information to Section 6. above)** |
| Click here to enter text. |

|  |
| --- |
| **8. Describe in Detail Any Compensating Control That Are in Place or Are Proposed** |
| Click here to enter text. |

|  |
| --- |
| **9. Requestor Acknowledgement** |

I hereby acknowledge that I have read and will abide by the applicable Regents’ *Rules and Regulations*, [UTS 165 Information Resources Use and Security Policy](http://www.utsystem.edu/board-of-regents/policy-library/policies/uts165-information-resources-use-and-security-policy) by signing below.

Additionally The University of Texas at El Paso Policies, Standards, and Guidelines will apply:

* [UTEP Information Resources Use and Security Policy](https://www.utep.edu/information-resources/iso/_Files/docs/utep-policies-and-standards/Security%20Policies.pdf)
* [Standard 2: Acceptable Use of Information Resources](https://www.utep.edu/information-resources/iso/_Files/docs/utep-policies-and-standards/Acceptable%20Use%20of%20Information%20Resources-Jun2014.pdf)
* [Standard 9: Data Classification](https://www.utep.edu/information-resources/iso/_Files/docs/utep-policies-and-standards/DataClassificationStandards.pdf)
* [Standard 11: Safeguarding Data](https://www.utep.edu/information-resources/iso/_Files/docs/utep-policies-and-standards/Standard%2011-SafeguardingData.pdfngData.pdf)

|  |  |
| --- | --- |
| **10. Approval/Denial:** |  |
| **Requestor’s Signature**: | **Date**:Click here to enter a date. |  |
| **Vice President/Director OR****Dean/Chair:** | **Date:**Click here to enter a date. | [ ]  Approved[ ]  Denied |
| **Gerard D. Cochrane Jr,** **Chief Information Security Officer** | **Date:**Click here to enter a date. | [ ]  Approved[ ]  Denied |

For more information, please visit the following web sites:

* [UTEP ISO – Laptop/Desktop Encryption Website](https://www.utep.edu/information-resources/iso/resources/laptop-encryption.html)
* [UTEP International Travel Resources](https://www.utep.edu/travel/international-travel-planning/device-encrypt-decrypt.html)

**Process for Submitting a Device Encryption Exemption Form for Consideration**

Device encryption exemptions may be submitted for consideration by filling out a Device Encryption Exemption Form to the UTEP Chief Information Security Officer (CISO). Please note that exceptions from the encryption directive will be considered only in rare situations.

