UTEP Standard 23: Security Control Exceptions

23.1 Exception to an otherwise required security control may be granted by the UTEP Chief Information Security Officer (CISO) to address specific circumstances or business needs, relating to an individual program or department, only as authorized by applicable law, and U.T. System and Institutional Policy. Requests for exceptions of this type must be submitted in writing via the Security Exception Request Form and should be initiated by the Data Owner. Both the UTEP CISO and Data Owner are jointly responsible for ensuring that any exception is not contrary to applicable law and/or Policies. For additional information please refer to the UTEP Security Exception Reporting Process.

23.2 The UTEP CISO may issue blanket exceptions to address Institution-wide situations.

23.3 All exceptions must be based on an assessment of business requirements weighed against the likelihood of an unauthorized exposure, and the potential adverse consequences for individuals, other organizations, or the Institution were an exposure to occur.

23.4 As a condition for granting an exception, the UTEP CISO may require compensating controls be implemented to offset the risk.

23.5 All exceptions must be documented, and must include the following elements:

(a) a statement defining the nature and scope of the exception in terms of the Data included and/or the class of devices includes;

(b) the rationale for granting the exception;

(c) an expiration date for the exception, unless otherwise documented exceptions expire on an annual basis;

(d) a description of any compensating security measures that are to be required; and

(e) acknowledgement, via signature (written, electronic, or through automated process), of the UTEP CISO, and, in the case of an exception resulting from a Data Owner request, of the Data Owner.

23.6 Encryption Exceptions

(a) The UTEP CISO may grant an exception to the use of encryption on a device if it is determined that encryption makes the device unsuitable to perform its intended function, there are no alternative hardware or software options available that can be used to allow

encryption, and the Risk posed by the unencrypted device is minimal or moderate based on its use and/or other implemented compensating controls. For more information please refer to the UTEP Security Exception Reporting Process.

(b) The UTEP CISO may recommend to the Chief Administrative Officer an encryption exception be granted for a High Impact Device if encryption makes the device unsuitable to perform its intended function. Exception recommendations have the effect of being approved unless, upon review, the CAO disapproves the recommendation.

23.7 A summary of exceptions and exception recommendations shall be reported to the President in the annual Presidential Information Security Program Report with sufficient detail to provide the President with an understanding of types of Risks and level of Institutional exposure.

23.8 This standard does not apply to or authorize the UTEP CISO to grant exceptions to UTEP Information Resources Use and Security Policy Standard 2: Acceptable Use of Information Resources.

23.9 Revision History

Created: June 1, 2017 (to align with UTS165)
Approved: June 16, 2017
Gerard D. Cochrane, Jr., Chief Information Security Officer