Chapter 5	Information Management & Services	Effective:	October 2016
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.30	**Information Security Exceptions**	Responsibility:	Chief Information Security Officer

INFORMATION SECURITY EXCEPTIONS

Policy

The Chief Information Security Officer may grant an exception to a required Information Security policy or standard to address a specific circumstance or business need.

1. All Exceptions must be based on an assessment of business requirements weighed against the likelihood of an unauthorized exposure or breach and the potential adverse consequences for individuals, other organizations or the UT Health San Antonio were an exposure to occur.

2. As a condition for granting an Exception, the Chief Information Security Officer may require compensating controls be implemented to offset the risk.

    - When approving an Exception or anytime thereafter, the Chief Information Security Officer may assess the effectiveness of mitigating controls and, if risk or other factors exceed what is described in the request, the Exception may be revoked or additional mitigating controls may be required.

3. The Chief Information Security Officer may issue blanket exceptions to address University-wide situations.

4. The Chief Information Security Officer may grant an Exception to the use of encryption if it is determined that encryption makes the device unsuitable to perform its intended functions and the risk posed by the unencrypted device is minimal or moderate based on its use and/or other implemented compensating controls.

5. A summary of Exceptions shall be reported to the President on an annual basis with sufficient detail to provide the President with an understanding of types of risks and levels of institutional exposure.

6. If an Exception is denied or previous approval revoked, access to Information Resources and/or data may be restricted until such time as the Information Resource can comply with UT Health San Antonio policies and standards or compensating controls approved by the Chief Information Security Officer are

implemented.

7. Both the Chief Information Security Officer and Data Owner are jointly responsible for ensuring that any Exception is not contrary to applicable state and federal law and regulation and UT Health San Antonio and UT System Policy and Standards.

Requests

Requests for an Exception to policy must be in writing and should be initiated by the Information Resource Owner. The request 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 included;

b. the rationale for granting the Exception;

c. an expiration date for the Exception not to exceed one year;

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

e. an acknowledgement, via signature (written, electronic or through automated process), of the Chief Information Security Officer, the Information Resource Owner and the Data Owner.

References

- U.T. System Policy 165 Standard 23