5.8.30 Information Security Exemptions

Chapter 5 - Information Technology	Original Effective Date: October 2016
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: October 2016

I. Purpose

To establish a framework for exemption to existing Information Security policies.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third-party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. General Policy

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

1. All exemptions 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 (UTHSA) were an exposure to occur.
2. As a condition for granting an exemption, the Chief Information Security Officer may require compensating controls be implemented to offset the risk.

   When approving an exemption 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 exemption may be revoked or additional mitigating controls may be required.

3. The Chief Information Security Officer may issue blanket exemptions to address UTHSA wide situations.
4. The Chief Information Security Officer may grant an exemption 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 exemptions 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 exemption 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 UTHSA 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 exemption is not contrary to applicable state and federal law and regulation and UTHSA and UT System Policy and Standards.

B. Requests

Requests for an exemption to policy must be in writing and should be initiated by the Information Resource Owner. The request must include the following elements:

1. a statement defining the nature and scope of the exemption in terms of the data included and/or the class of devices included;
2. the rationale for granting the exemption;
3. an expiration date for the exemption not to exceed one year;
4. a description of any compensating security measures that are to be required; and
5. an acknowledgement, via signature (written, electronic or through automated process), of the Chief Information Security Officer, the Information Resource Owner and the Data Owner.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

U.T. System (UTS) Policy
UTS 165 Information Resources Use and Security, Standard 23: Security Control Exceptions

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
10/2016	Policy Origination		
02/2023	Policy Review/Discretionary Edits		