THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: IT0003-HSC-A.02 Security Exceptions and Exemptions to ITS Standards Practices & Controls	
Version 5	Effective Date: 03/17/2016

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To identify the requirements, procedures, and documentation for approving or denying exceptions and exemptions to established cybersecurity standards, practices, and controls to provide for unusual operational, technical, or administrative circumstances.

Scope

All UT Health Science Center Security Controls and ITS/Cybersecurity Standards, Practices, and Controls. These Standards may be written authoritative documents or other ITS standards, such as baseline configurations and firewall rules.

Definitions

Control - The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature.

Exception – a request considered as a short-term solution to issues related to security controls and standards. These exceptions should be reviewed or renewed annually if they represent low to medium risk or every six months if they are high risk or above.

Exemption – a request considered as a longer-term solution to issues related to security controls and standards. These exemptions should be reviewed for accuracy and need on an annual basis if they represent low to medium risk or every six months if they are high risk or above.

TechConnect – UT Health Science Center's IT Service Management System

Responsibilities

Chief Information Security Officer (CISO) is responsible for providing guidance and direction in assessment, planning, and implementation of all security standards and practices. This individual is responsible for the adherence to this document.

Governance, Risk, and Compliance (GRC) Team under the Office of Cybersecurity is responsible for acknowledging that the requested exception/exemption is justified

UT Health Science Center:
IT0003-HSC-A.02 Security Exceptions and Exemptions to ITS Standards Practices & Controls

Version 5	Effective Date: 03/17/2016

by a business need and recommends possible other solutions for which the requestor may not be aware to either reduce or eliminate the risk. This role also ensures that the solution proposed contains detailed information, so that the approver is aware of the risks, and can make an informed acknowledge/reject decision.

Requestor is responsible for providing the business justification; explanation of risk involved/being acknowledged, mitigation plan/controls in place to reduce risk, etc. for the exception/exemption request. This contact will be ultimately responsible for following the request through the approval process. This role will also have the responsibility to review and resubmit an exception/exemption annually as deemed necessary. This role is usually the Business/Data/System Owner or Custodian.

Authorized Signer is responsible for reviewing and acknowledging or rejecting the risk(s) presented for the exception/exemption.

Practice

1. A Risk Assessment must be conducted per IT0004-HSC-A.01-Risk Assessment Process to identify, analyze, evaluate, and develop a response for acknowledging the risk associated with the exception/exemption.

2. Requests for exception from security controls, UT Health Science Center IT/Cybersecurity Standards or Practices must be submitted in writing to the Office of Cybersecurity using TechConnect and the subsequent Security Exceptions and Exemptions to ITS Security Controls Request Form found therein. At a minimum, each request shall have the following information completed by the requestor, or the request will not proceed:
   a. Contact information on the requestor and authorized signer
   b. The standard, practice, or controls from which an exception is desired
   c. Request type (i.e. Exception, Exemption)
   d. Explanation of the Request
   e. Business Justification/Reason

3. The GRC Team conducts a risk assessment regarding the request.
   a. If needed, the cybersecurity governance committee will conduct a review of the assessment.

4. The GRC Team documents the results of the risk assessment in the TechConnect ticket and notifies the authorized signer to acknowledge or reject the request.
   a. If the risk level is higher than the acceptable level, the approver of the request must be at the level determined in the Risk Response Matrix in

UT Health Science Center:
IT0003-HSC-A.02 Security Exceptions and Exemptions to ITS Standards Practices & Controls

Version 5	Effective Date: 03/17/2016

IT0004-HSC-A.02--Risk Assessment Process.
- The person acknowledging the risk documents the same TechConnect ticket of their decision.
- If the authorized signer rejects the exception, they document the reason for the rejection and notify the requestor.
5. The Office of Cybersecurity documents the acknowledged risk in UT Health Science Center's risk register.
6. All granted requests must be reviewed and/or renewed annually.

Policy History

Version #	Effective Date
1	03/17/2016
2	07/29/2021
3	01/21/2022
4	06/11/2024
5	03/01/2025 – new naming convention

References

1. IT0003-Information Technology Security Program Strategy
2. IT0003-HSC-A-UTHSC Information Security Program
3. IT0002-HSC-A.01-Risk Assessment Process
4. NIST Glossary of Terms