THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

| UT Health Science Center:<br>GP-001.02-Security Exceptions and Exemptions to ITS Standards Practices & Controls | |
|---|---|
| Version 4 | Effective Date: 03/17/2016 |

| | |
|---|---|
| Responsible Office: Office of Cybersecurity | Last Review: 01/19/2022<br>Next Review: 01/19/2024 |
| Contact: Chris Madeksho | Phone: 901.448.1579<br>Email: mmadeksh@uthsc.edu |

# Purpose

The Office of Cybersecurity enables business through facilitating a security exception and exemption program that evaluates and documents any deviations to the established UTHSC policies, standards and controls. This document identifies the requirements, procedures, and documentation for granting and controlling exceptions and exemptions to established standards, practices, and controls in order to provide for unusual operational, technical, or administrative circumstances. This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

# Scope

All UTHSC Security Controls and ITS/InfoSec 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 to be a short-term solution to issues related to the security controls and policies. These exceptions should be reviewed or renewed annually if they represent very low to medium risk or every six months if they are high risk or above.

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

**TechConnect** – UTHSC's IT Service Management System

## Responsibilities

**Chief Information Security Officer (CISO)** – 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.

**Office of Cybersecurity Team** – responsible for acknowledging that the requested exception/exemption is justified by a business need and recommends possible other solutions for which the requestor may not be aware. 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** – 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** – responsible for reviewing and acknowledging or rejecting the risk(s) presented for the exception/exemption.

## Practice

1. A Risk Assessment must be conducted per RA-001.01-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, UTHSC IT/InfoSec 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 Office of Cybersecurity conducts a risk assessment on the request.

   a. If needed, the cybersecurity governance committee will conduct a review of the assessment
4. The Office of Cybersecurity documents the results of the risk assessment in the TechConnect ticket and notifies the authorized signer to acknowledge or reject the request.
   a. The approver of the request must be at the level determined in the Risk Response Matrix in RA-001.01-Risk Assessment Process (Figure 8).
   b. The person acknowledging the risk documents the same TechConnect ticket of their decision.
   c. 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 UTHSC's risk register
6. All requests that are granted must be reviewed and/or renewed annually.

## References

1. GP-001-Standard on UTHSC Information Technology Standards and Practices
2. RA-001.01-Risk Assessment Process
3. NIST Glossary of Terms