THE UNIVERSITY OF TEXAS AT TYLER

SECURITY ASSESSMENT AND AUTHORIZATION POLICY

Table of Contents

1 Information Security Mission Statement

The University of Texas at Tyler's Information Security Office reduces risk to and secures university data and assets, verifies compliance requirements, and promotes information security awareness across campus.

2 Purpose

The purpose of the Security Assessment and Authorization Policy is to empower the Information Security Department to perform periodic risk assessments to determine the inherent impact Information Resource vulnerabilities could cause and to initiate appropriate remediation.

3 Definitions/Acronyms

Acceptable Risk – level of risk considered to be tolerable
Data Custodian – the person who has technical control over an information asset
Data Owner – the person responsible for day to day accuracy and integrity of the data
Remediation – process of selecting countermeasures to reduce risks
Risk Assessment – the process of identifying and documenting hazards and potential vulnerabilities of an information resource and determining appropriate ways to eliminate or control the risk
Vulnerability – a weakness or flaw in a system which can leave it open to attack

4 Scope

The Security Assessment and Authorization Policy applies to all systems and data on the University network, owned by the University or operated on behalf of the University. Risk assessments will be conducted on mission critical information resources containing confidential data annually and at periodic intervals for non-mission critical resources not containing confidential data. Risk assessments of third-party service providers are required when services result in exchange of University data whether on premises or at a vendor facility. Risk assessments for sponsored projects will be performed annually, based on risk.

5 Policy

The execution, development and implementation of the security risk assessment is the combined responsibility of the department responsible for the system/data being assessed and the Information Security Department. Decisions relating to remediation and risk acceptance must be documented and approved by the Information resource owner, in consultation with the Information Security Officer. Any high risks which cannot be mitigated to a tolerable level must be reviewed and approved by the Chief Administrative Officer, or designee, based on recommendations of the data owner and Information Security Officer

6 Roles and Responsibilities

Information Security Officer:

- Ensures risk assessments are performed and documented on all identified resources, per frequency and in compliance with policies and regulations

Information Security Staff:

- Identifies resources which require annual risk assessments (mission critical containing confidential data)
- Identifies resources which require periodic risk assessments (non-mission critical, not containing confidential data)
- Coordinates the initial generation of risk assessments and delivery of questionnaires to the responsible data owners
- Provides guidance/instruction to data owners as needed
- Reviews assessments completed by the data owners and makes recommendations where necessary

- Reviews risk assessments requiring mediation with appropriate staff
- Informs Data Custodians of risks that require remediation
- Reviews residual risk of Low or moderate items with Data owners for final approval
- Provides Chief Administrative Officer with reports regarding High Risk items with residual risk for final risk acceptance approval
- Assessments that may be required system wide, will be submitted to the UT System Executive Compliance committee and the UT system board of regents upon final approval
- Monitor the effectiveness of risk mitigation actions and document results
- Evaluate the risk assessment process
- Schedule the next risk assessment engagement

Data Owners:

- Conduct and document risk assessments, within requested timelines, in consultation with the Information Security Staff

Data Custodians:

- Implement approved risk mitigation strategies, adhering to Information Security policies and procedures, for the resources under their care.
- Report status of remediation to Data Owners and Information Security Staff

7 Contacts and Notification

Below is contact information for members of the Information Security Department:

Team	Department	Name	Contact Information
CIRT	Information Security	Chris Green Information Security Officer	cgreen@uttyler.edu (W): 903.566.7190
CIRT	Information Security	Kaytee Hassell Security Analyst	mhassell@uttyler.edu (W): 903.565.7292
CIRT	Information Security	Mona Claiborne Security Analyst	rclaiborne@uttyler.edu (W): 903.565.5667