UTSA Institutional Compliance
Office of Information Security

OIS 15 – Standard for Information Security Risk Assessment

I. STANDARD STATEMENT

Departments and data owners who manage information resources must sponsor formal risk assessments to identify potential problems that would affect the operation and security of their information assets. Risk assessments are the first step in the process of protecting information resources, and they shape mitigation strategies and plans.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. DEFINITIONS

1. **appropriate unit level** - For administrative areas, appropriate unit levels would be departments or business units reporting to associate vice presidents (AVP). AVPs and vice presidents will summarize the assessments to provide summary assessments to the Office of Information Security. For academic areas, appropriate unit levels would be academic departments and Principal Investigators (PIs) of grants. These may be combined or separate. College deans and the Provost office will summarize the assessments to provide an Executive Summary to the Office of Information Security.
2. **regular basis** - annually.
3. **risk assessment strategy report** – This is the report that that results from the assessment. It should cover the planning and controls for the most critical risks,

identification information for each asset, contacts and contact information, vulnerabilities and threats, and actions and resources needed to mitigate or accept risk.

4. **assessor** – likely to include Information Security Administrators, Information Technology Associates and other functional managers

B. PROCEDURES

1. Risk assessments will be performed on a regular basis at an appropriate unit level, summarized and provided to upper organization levels.
2. The Risk Assessment must include, at minimum:
   a. An inventory of software, hardware and secured facilities under their responsibility
   b. Classification of digital data based on sensitivity and risk
   c. Methods being used to protect data from loss (i.e. backup schedule)
   d. Implementation status of approved mitigation strategies that adhere to information security policies and procedures for managing risk levels for information resources. Implementation status of approved mitigation strategies that adhere to information security policies and procedures for managing risk levels for information resources.
   f. Identification of controls in place to ensure the confidentiality, integrity and availability of data and other assigned information resources.. Identification of controls in place to ensure the confidentiality, integrity and availability of data and other assigned information resources.
   g. Copies of (or reference to) related scores on InSight metrics
   h. Action plans to address control weaknesses, non-compliance with InSight metrics and to mitigate unacceptable risks.
3. Data Owner will review and update the Risk Assessment on a regular basis; ISAs will provide assistance as needed.
4. Copies of risk assessment reports and executive summaries will be provided to the Office of Information Security.
5. The strategy report that results from the assessment will be submitted to the Information Security Officer (ISO) on an annual basis.

Title: OIS 15 – Standard for Information Security Risk Assessment
Effective Date: January 1, 2014
Last Revised: July 30, 2020