Section:	Information Security	Effective:	October 2005
Standard:	Electronic Information Security Risk Assessment	Revised:	
Policy Ref:	5.8.26 Electronic Information Security Risk Management Policy	Responsibility:	Chief Information Security Officer

ELECTRONIC INFORMATION SECURITY RISK ASSESSMENT SECURITY STANDARD

Security Standards are <u>mandatory</u> security rules applicable to the defined scope with respect to the subject.

Overview

The goal of the electronic information security risk assessment process is to identify all possible information security risks, and then mitigate significant risks where reasonably possible. Since all risks cannot be totally eliminated, some residual risks are expected. Based on operations, costs, or business needs, some level of risk may be considered acceptable. The electronic information security risk assessment process will provide a level of understanding of what might be considered an information security risk.

Scope

All departments, offices, and schools that are responsible for security management of UTHSCSA's information resources must conduct at a minimum, an annual information security risk assessment. According to 5.8.26 Electronic Information Security Risk Management Policy, Executive Committee members shall designate the entity organization level responsible for security management. This self assessment must at a minimum, include the "Information Security Risk Self-Assessment Survey".

Purpose

The purpose of this document is to define the minimum information security risk assessment requirements for all UTHSCSA departments, offices, and schools. The intention is to establish a partnership between organizations and the Information Security Office in addressing security risk concerns with risk mitigation strategies. These minimum information security risk assessment requirements will also facilitate federal and state regulatory compliance requirements.

Procedure

Each designated organization is required to complete and retain the "Information Security Risk Self-Assessment Survey" along with any other information pertinent to this evaluation. The survey is not intended to be comprehensive; therefore, other tools or processes may be used for assessing information security risks as determined necessary by the organization.

The survey may be jointly completed by personnel within each department that are responsible for computer support and information security (e.g. TSRs, ACEs, webmasters, administration, etc.). Identified security risks should be evaluated

and where possible, mitigation strategies implemented. If needed, the Information Security Office can assist with formulating remediation strategies. The "Score" column of the survey identifies an entity risk and will be used to calculate the total information security risk weight for the entity organization.

The entity organization's risk assessment and overall security risk weight from the survey must be communicated to the respective chair or director for approval and signature. Documentation and mitigation plans should be developed for all risk areas. Example documentation might include such items as:

- New procedures or processes
- New technology
- Configuration or application changes
- Physical changes planned
- Budget items to address risk mitigation strategies
- Management authorization for level of acceptable risks
- User communication
- Elimination of the risk

Monitoring

All departments, offices, and schools are required to electronically send the "Information Security Risk Self-Assessment Survey" to the Information Security Office by March 31 of each year. The surveys will be used by the Information Security Office (ISO) for the security plan development and allocation of resources. Additionally the ISO reserves the right to perform periodic detailed reviews of the self-assessments in order to evaluate completeness of risk identification and mitigation planning, as well as to provide assistance.