Section:	Information Security	Effective:	March 2007
Standard:	Third-Party Risk Assessment Security Standard	Revised:	
Policy Ref:	5.8.18 Third-Party Management of Information Resources	Responsibility:	Chief Information Security Officer

THIRD-PARTY RISK ASSESSMENT SECURITY STANDARD

Security Standards are mandatory security rules applicable to the defined scope with respect to the subject.

Overview

The goal of the Third-Party Risk Assessment Security Standard is to educate and provide departments with a tool to assist in risk management related to procurement of information technology (IT) services. The “Information Security Third-Party Assessment Survey” tool communicates information security best practices for third-party/vendor management and serves as a benchmark tool for managing associated risks. Data classification, business operations, and cost are critical factors in determining acceptable risk.

Scope

The Standard provides direction to all UTHSCSA organizations (schools, departments, offices, and centers) responsible for information security management. In particular, this Standard provides guidance for engaging vendors, contractors, consultants, or other third-party entities to develop, maintain, manage, transmit, or store information assets. The Standard and related survey tool focuses on mitigating third-party risk from remote access, data transmission and offsite storage.

Departments should use the Information Security Third-Party tool to assess all third-party IT service arrangements. Examples include:

- Web hosting
- Application Development
- Database Management
- Network Monitoring
- Web content development
- Data Backup
- System Maintenance
- Offsite Storage

Again, the process is recommended for all third-party IT service relationships; however, the process is mandatory where Confidential/High Risk data is accessed remotely, transmitted, or stored offsite. In these instances, the Information Security Third-Party Assessment Survey must be reviewed by the Information Security Office.

Section:	Information Security	Effective:	March 2007
Standard:	Third-Party Risk Assessment Security Standard	Revised:	
Policy Ref:	5.8.18 Third-Party Management of Information Resources	Responsibility:	Chief Information Security Officer

Purpose

The purpose of this Standard is to define the incremental risk to an organization when engaging third-party IT service providers to assist in the development, management, access management, transmission and/or storage of UTHSCSA's information assets; as well as define a due diligence process for mitigating those risks. The Information Security Office has developed the Third-Party Risk Assessment Survey tool to assist departments with assessing and mitigating risk related to third-party IT service relationships. The intention is to reinforce the existing risk management partnership between UTHSCSA organizations and the Information Security Office.

With the development of policy, employee and student training, technology solutions, and monitoring processes, UTHSCSA has made significant progress in reducing the organization's Information Security risk. However, information assets can be subject to additional threats when data leaves our controlled environment and/or external users access our assets. A primary example of this potential for external risk is third-party IT service relationships.

Procedure

Departments should use the "Information Security Third-Party Risk Assessment Survey" to evaluate potential third-party IT service relationships. It is recommended that departments have all prospective service providers complete the survey. Management should evaluate a prospective service provider based on the survey results. Additionally, the survey can be used an effective negotiation tool when developing contractual obligations.

The survey is a recommended tool for evaluating and managing all third-party IT service providers; however, the process is mandatory for third-party relationships that involve remote access, transmission, hosting, and/or offsite storage of Confidential/High Risk data. Prior to finalizing any business agreements involving Confidential/High Risk data, the completed "Information Security Third-Party Risk Assessment Survey" must be forwarded to the Information Security Office for review. This survey may be found at the Information Security web site (http://infosec.uthscsa.edu).