TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.01, 1.1. I.T. RESOURCE MANAGEMENT AND RESPONSIBILITIES (TAC 202.71, 202.72)

PURPOSE:

REVIEW:

POLICY/PROCEDURE:

Information Security Program

Each state agency head or his or her designated representative(s) shall designate an Information Security Officer (ISO) to administer the state agency Information Security Program. The ISO shall report to executive level management. TTUHSC El Paso's Information Security Program will be reviewed annually for compliance with TAC 202 standards. Other responsibilities of the ISO include the following:

- Document and maintain an up-to-date information security program. The information security program shall be approved by the institution of higher education head or his or her designated representative(s).
- Develop recommended policies and establish procedures and practices, in cooperation with information owners and custodians, necessary to ensure the security of information resources assets against unauthorized or accidental modification, destruction or disclosure.
- Monitor the effectiveness of defined controls for mission critical information.
- Report, at least annually, to the institution of higher education head or his or her designated representative(s) the status and effectiveness of information resources security controls.
- Issue exceptions to information security requirements or controls in this chapter. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.
- Work with the owners of information resources to develop strategies to meet their required responsibilities and to ensure compliance.

Defined Responsibilities

Information Owner Responsibilities – the owner or their designated representative(s) are responsible for and authorized to:

- Approve access and formally assign custody of an information resources asset

- Determine the asset's value
- Specify data control requirements and convey them to users and custodians
- Specify appropriate controls, based on a risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources and services outsourced by the institution of higher education.
- Confirm that controls are in place to ensure confidentiality, integrity, and availability of data and other assigned information resources.
- Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures
- Review access lists based on documented security risk management decisions
- Approve, justify, document and be accountable for exceptions to security controls. The information owner shall coordinate exceptions to security controls with the ISO or other person(s) designated by the state institution of higher education head.
- Classify business functional information

Custodians of information resources shall:

- Implement the controls specified by the owner(s),
- Provide physical, technical, and procedural safeguards for the information resources,
- Assist information owners in evaluating the cost-effectiveness of controls and monitoring, and
- Implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

User Responsibilities - the user of the information resources is responsible for:

- Using the resources only for the designed purpose, and
- Complying with the controls specified by the owner(s).
- Information system owners, in collaboration with the Information Security Officer or designee, shall assess a risk level based on the inherent risk with a ranking of “High”, “Medium”, or “Low”. The criteria for each level are:

High Risk	**Medium Risk**	**Low Risk**
Involve large dollar amounts, or significantly important information that would impact the operations of the HSCEP, or	Involve a moderate or low dollar value, or	Generally available public information, or
Contain confidential or sensitive data, or	Information that could potentially create problems for	Result in a relatively small impact for the

	the parties involved, or	HSCEP
Impact a large number of people or networks	Impact a moderate portion of the Institution's customer base	

- See Policy 1.4.1 for further responsibilities.
- A system change could cause the overall classification to move to another risk level

Managing Security Risks

A security risk analysis of information resources shall be performed and documented on the following schedule:

- Annually on information resources classified as high risk
- Biennially on information resources classified as medium or low risk

Security risk assessment results, vulnerability reports and other security analysis information shall be presented to the President of the HSCEP or their designated representative(s). The President of the HSCEP or designated representative(s) shall make the final security risk management decisions to either accept the risks or to modify the security and controls for the information resources based on its value and sensitivity. The President of the HSCEP or their designated representative(s) must approve the final security risk management plan.