Information Security Office

The University of Texas at El Paso
Calendar Year 2017
Information Security Program

Submitted by
Gerard D. Cochrane, Jr.
Chief Information Security Officer

Approved By: _____
Richard Adauto III, Executive Vice President

Date: March 20, 2017

Table of Contents

Executive Summary

Texas state law requires that each state agency, including Institutions of Higher Education, have in place an Information Security Program (ISP) that is approved by the head of the institution.[1] Governance for all information security is the responsibility of the Information Security Office (ISO). This document provides a broad overview of the Calendar Year 2017 (CY2017) Information Security Program for your review and approval per the referenced statute.

The Information Security Program plans for CY2016 outlined below provide for the continuation of a mature, successful security program for The University of Texas at El Paso (UTEP).

Program Highlights for CY2017

- Deployment New Anti-Virus for Campus
- System Center Configuration Manager (SCCM) Replacing Windows Server Update Services (WSUS)
- Deployment of Firewalls for all Payment Card Industry Point of Sale Devices (PCI POS)
- Development of an Information Security Dashboard
- New Information Security Policies and Standards based on new UTS165 and TAC§202

Summary of Past Calendar Year Program Accomplishments and Events

Major Accomplishments

The ISO focused its efforts on a security layered approach, also known as layered defense, to improve its overall security posture. Some of these efforts included:

- Deployment of 2-Factor Authentication (DUO)
- Deployment of New VPN Solution (PaltoAlto)
- Deployment of Campus Firewall Appliance
- Upgrade and Deployment of New Payment Card Industry Point of Sale Devices (PCI POS)

[1] Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter B, Rule §202.71 (d)(2): The Information Security Officer shall document and maintain an up-to-date information security program. The information security program must be approved by the state agency or his or her designated representative(s).

Mission

The mission of the Information Security Office (ISO) is to protect information acquired and found throughout the University by conducting risk assessments on all sensitive information, promoting security related training and awareness programs, monitoring university systems, and auditing and compliance in support of the University's missions and goals.

Authority

State Law: TAC §202.70 requires that each institution of higher education have an information security program:
"(5) ensure that senior institution of higher education officials support the institution of higher education Information Security Officer in developing, at least annually, a report on institution of higher education information security program, as specified in §202.71(b)(11) and §202.73(a) of this chapter;" . . . and TAC §202.70 "(7) review and approve at least annually institution of higher education information security program required under §202.74 of this chapter;"

University Policy: UTS 165 Standard 3: Information Security Programs. Each Institution and any governing body with oversight for Common Use Infrastructures must establish and maintain a Security Program that includes appropriate protections, based on risk, for all Information Resources including outsourced resources, owned, leased, or under the custodianship of any governing body or department, operating unit, or employee of the Institution. Each Security Program must include and document the following:

- annual risk assessment;
- current inventory of institution-owned or managed computing devices deployed throughout the institution, and Mission-Critical applications and applications containing Confidential Data;
- strategies to address identified risks to Mission Critical Information Resources and Confidential Data;
- annual action plan, training plan, and monitoring plan; and
- metrics, reports, and timelines established by the U. T. System Office of Information Security.

Program Scope

The program scope includes identifying technologies utilized to minimize risk, establishing training programs to ensure the protection and integrity of Confidential Data, and establishing procedures for enforcement by the Institution.

Please note that this program includes Confidential Data that is entrusted, transmitted, processed, acquired, stored, transferred, and/or maintained by The University of Texas at El Paso. This program also applies to all individuals granted access privileges to any University Information Resources regardless of form, format, and/or affiliation.