Information Security Office

The University of Texas at El Paso
Calendar Year 2020
Information Security Program

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

Table of Contents

Information Security Office

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 2020 (CY2020) Information Security Program for your review and approval per the referenced statute.

The Information Security Program plans for CY2020 outlined below provide for the continuation of a mature, successful security program for The University of Texas at El Paso (UTEP).

Program Highlights for CY2020

- Development of New Cybersecurity training for Texas HB8 (85R) and Texas HB3834 (86R)
- Enhancements to Network Security Monitoring
- Enhancements to Vulnerability Management
- Increased use of Cybersecurity table-top exercises
- Automated Metrics Collection and Analyses (Key Performance Indicators)

Summary of Past Calendar Year Program Accomplishments and Events

Major Accomplishments

The ISO focused its efforts on updated and new security controls and requirements to improve its overall security posture. Some of these efforts included:

- Installation of Intrusion Detection Systems from UT Austin at campus network's perimeter
- Additional logging of internal and external campus traffic (Netflows)
- Participated in multiple cybersecurity incident response exercises
- Determined Key Performance Indicators (KPI) for ISO and developed systems to collect and maintain metrics for KPIs.

[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).

Major Events

These are the major events occurring since the last reporting document.

Events:	Installation of Intrusion Detection Systems from UT Austin at campus network's perimeter
Dates:	November, 2019
Description:	The University of Texas (at Austin) has previously provided external scanning of all UTEP IR to identify any vulnerabilities or compromised systems communicating externally to malicious endpoints and notify UTEP ISO. In addition to these capabilities, Intrusion Detection Systems (IDS) have been installed on the campus network to provide additional scanning from an internal campus network perspective. This addition augments the already existing external scanning process and provides invaluable details about internal network activity not previously captured.

Events:	Additional logging of internal and external campus traffic (Netflows)
Dates:	January 6th, 2020
Description:	In addition to providing alerts on malicious network traffic, UT Austin began collecting netflow data from UTEP's network perimeter. Netflow data provides detailed information about communication patterns within the UTEP network as well as with external networks. This information can be leveraged for various ISO investigations, network traffic debugging, and verification of network traffic.

Events:	Participated in multiple cybersecurity incident response exercises
Dates:	November 7th, 2019 & January 13th-24th, 2020
Description:	The ISO participated in table-top and penetration tests that were conducted against UTEP's mission critical Information Resources. On November 7th, 2019, UT System's ISO and Sylint, a third-party security services provider and consultancy company, visited the UTEP campus and met with representatives from all IR teams to conduct a table-top exercise. During the exercise, all mission critical systems were supposed to have failed due to ransomware. Through the discussion, it was determined that all mission critical systems could be recovered within a week's time, with secondary systems (i.e. non-mission critical) returning soon after. The ISO also participated in a Red-Team exercise against mission critical systems that was performed by UT Austin's ISO. Starting on January 13th, and given only a low level user's access, UT Austin conducted a Red-Team exercise over a week and a half. Critical vulnerabilities were identified as part of the exercise and resulting recommendations are actively being incorporated into UTEP's architecture and policies.

Events:	Determined Key Performance Indicators (KPI) for ISO and developed systems to collect and maintain metrics for KPIs.
Dates:	December 2019 through February 2020
Description:	With the assistance of Dr. Roy Mathew, the ISO developed KPI for reporting to the UTEP cabinet on a monthly basis. These metrics are to assist UTEP leadership with status changes across departments that could help identify trends as well as unmet needs that could be addressed to help achieve the University's mission. The metrics required several discussions with Dr. Mathew to understand the mathematical and managerial expectations created by various measurements as well as to understand how changes in these measures over time would be represented and understood. Once metrics were decided, the systems capturing those metrics were reviewed and augmented to ensure data was captured as accurately as possible and that information reported was complete.

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.