Information Security Office

The University of Texas at El Paso
Calendar Year 2019
Information Security Program

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

Approved By: _____

Richard Adauto III, Executive Vice President

Date: 03/09/19

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 2019 (CY2019) Information Security Program for your review and approval per the referenced statute.

The Information Security Program plans for CY2019 outlined below provide for the continuation of a mature, successful security program for The University of Texas at El Paso (UTEP).

Program Highlights for CY2019

- Development of New Security Requirements for Controlled Unclassified Information (CUI) Program for the protection of Federal grants
- Development of New Security Requirements for the protection of Intellectual Property (IP)
- Enhancements to the Cybersecurity Program to be More in Line with the Federal Cybersecurity Framework (CSF)
- Automated Metrics Collection and Analyses

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:

- Deployed of 2-Factor Authentication to Microsoft's Outlook Web Application (OWA)
- Campus-Wide Application Inventory
- Performed Web Application Security Reviews - Texas House Bill 8 (TXHB8)
- Deployed Physical Firewalls and Completed Merchant Annual Self-Assessment Questionnaires (SAQs) for UTEP-wide Compliance with Payment Card Industry Data Security Standard (PCI DSS)

[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.

Event:	Deployment of 2-Factor Authentication (2FA) to Microsoft's Outlook Web Application (OWA)
Dates:	February 15, 2019
Description:	The University of Texas at El Paso Information Security Office (ISO) deployed DUO 2-Factor Authentication (2FA) to Microsoft's Outlook Web Application (OWA) access. This new requirement was mandated by U.T. System and is intended to help mitigate phishing attacks, and enhance security measures for Faculty and Staff when accessing Webmail remotely. Additionally, this enhancement affords users full control of access to their OWA account. For instance, if a user's credentials are compromised, or a hacker attempts to access their account via OWA, the user will be alerted to the real-time login event and can take action to either "Approve" or "Deny" access based on whether they initiated the access to their account or not thus mitigating account fraud. This will be an invaluable tool in helping to stop hackers from taking over accounts for the purpose of launching phishing campaigns against unsuspecting individuals or potentially gleaning Confidential information.

Event:	Campus-Web Application Inventory
Dates:	October 31, 2018
Description:	The University of Texas at El Paso ISO concluded an initiative to gather and consolidate a more comprehensive campus-wide inventory of all web applications. This initiative was required in order to gather inventory data for completion of House Bill 8 security reviews.

Event:	Perform Web Application Security Reviews – Texas House Bill 8 (TXHB8)
Dates:	Ongoing
Description:	Reviews were conducted of all web applications collecting Confidential Information to help prevent data leakage. Texas House Bill 8 (TXHB8) requires cybersecurity for state agency information resources be reviewed and assessed on a recurring basis to reduce risks and incidents involving cyber-attacks. New standards were instituted for all web applications thus elevating the security controls for any collected information. Additionally, a process was developed for collecting this data through a consistent, repeatable reporting mechanism on an ongoing basis.

Event:	Deployment of Physical Firewalls and Completed Annual Merchant Self-Assessment Questionnaires (SAQs) for UTEP-wide Compliance with Payment Card Industry Data Security Standard (PCI DSS)
Dates:	October 2018 – February 2019
Description:	New Payment Card Industry Data Security Standard (PCI DSS) requirements call for additional measures for the segmentation of the PCI Cardholder Data Environment (CDE) from the rest of the UTEP private/public network as well as within the CDE. In order to achieve compliance will PCI requirements, physical firewalls were deployed campus-wide to specific, targeted point of sales (PoS) devices as well as systems processing credit card payments. UTEP Merchants completed their annual self-assessment with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS) thus insuring that UTEP is PCI compliant.

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.