The University of Texas at El Paso
Calendar Year 2018
Information Security Program

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

Approved By:

Richard Adauto III, Executive Vice President

Date: Jan 29, 2018
Table of Contents

Executive Summary .................................................................................................................. 3
Summary of Past Calendar Year Program Accomplishments and Events .................................................. 3
  Major Accomplishments ......................................................................................................... 3
  Major Events ......................................................................................................................... 4
Mission .................................................................................................................................... 5
Authority ............................................................................................................................ 5
Program Scope ..................................................................................................................... 6
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 2018 (CY2018) Information Security Program for your review and approval per the referenced statute.

The Information Security Program plans for CY2018 outlined below provide for the continuation of a mature, successful security program for The University of Texas at El Paso (UTEP).

Program Highlights for CY2018
- Deployment of 2-Factor Authentication to Microsoft’s Outlook Web Application (OWA)
- Development of an Information Security Dashboard (ongoing)
- Campus-Wide Application Inventory
- Web Application Security Reviews - Texas House Bill 8 (TXHB8)
- Transition Campus Away from Older VPN Service

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 Password Reset Initiative
- Deployment New Anti-Virus for Campus
- Upgrade Windows Server Update Services (WSUS)
- New Information Security Policies and Standards based on new U.T. System 165-Information Resources Use and Security Policy (UTS165) and TAC§202

\(^1\) 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.

<table>
<thead>
<tr>
<th>Event:</th>
<th>Deployment of Password Reset Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dates:</td>
<td>January 2, 2017</td>
</tr>
<tr>
<td>Description:</td>
<td>The University of Texas at El Paso began enforcing stronger password requirements beginning on January 2, 2017. All users were asked to reset their password prior to the deadline and launched a campaign to inform the community that they would be required to reset their password once a year. Additional password complexity and requirements were conveyed starting on October 31, 2016 in preparation for the enforcement of the new expiration mandate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event:</th>
<th>Deployment of New Anti-Virus for Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dates:</td>
<td>October 20, 2017</td>
</tr>
<tr>
<td>Description:</td>
<td>The UTEP Information Security Office (ISO) deployed Bitdefender as the new anti-virus solution to the campus. Bitdefender ranked amongst the best anti-virus programs and received the “Gold Award Winner”, earning a perfect score in malware detection and removal, by TopTenReviews™. It was also ranked number one by Consumer Reports and Windows Central in 2017. Increased ransomware and malware attacks on the University community prompted the decision to transition to a superior product that could keep pace with the University’s diverse and unique cyber landscape. The University benefits from Bitdefender’s use of advanced artificial intelligence, as well as other revolutionary technologies to anticipate, detect and instantly block even the newest threats from around the globe and provides improved reporting functions and statistics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event:</th>
<th>Upgrade Windows Server Update Service (WSUS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dates:</td>
<td>March 2017</td>
</tr>
<tr>
<td>Description:</td>
<td>Patch management is a critical function and the University was moving towards phasing out the WSUS system by replacing it with Microsoft’s System Center Configuration Manager (SCCM) solution. The patch management system was upgraded in March 2017 to the latest version. The upgrade allows the ISO to utilize improved reporting features, which in turn improves patch deployment and management of devices.</td>
</tr>
</tbody>
</table>
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.