Information Security Office

The University of Texas at El Paso
Calendar Year 2014
Information Security Program

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

Approved By:
Richard Adauto III, Executive Vice President

Date: March 14, 2014
# Table of Contents

**Information Security Office**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Summary of Past Calendar Year Program Accomplishments and Events</td>
<td>3</td>
</tr>
<tr>
<td>Major Accomplishments</td>
<td>3</td>
</tr>
<tr>
<td>Mission</td>
<td>4</td>
</tr>
<tr>
<td>Authority</td>
<td>4</td>
</tr>
<tr>
<td>Program Scope</td>
<td>4</td>
</tr>
<tr>
<td>Program Exceptions</td>
<td>4</td>
</tr>
</tbody>
</table>
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 2014 (CY2014) Information Security Program for your review and approval per the referenced statute.

The Information Security Program plans for CY2014 outlined below provide for the continuation of a mature, successful security program for The University of Texas at El Paso (UTEP).

Program Highlights for CY2014
- Desktop Encryption for High Risk Desktops
- Risk Assessments using New Product (RSA Archer)
- Deployment of New Anti-Virus for Campus
- Centralized Computer Configuration Management Services
- Develop Network Inventory of Devices

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:
- Implementation Restrictions on External DNS Recursion
- Implementation of Email Rate-Limiting to Help Reduce Spam/Phishing from Compromised Accounts
- Development of the new Encryption Dashboard Allowing Departments to Monitor Individual/Overall Progress
- Deployment of Absolute Manage to Campus
- SecureDoc Encryption Software Successfully Upgraded to Version 6.2
- Deployment of the New Avast! Endpoint Protection Anti-Virus and Departmental Self-Manage Consoles
- IronPort Virus and Outbreak Filters, and URL Redirect Feature Enabled

---

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:
“(2) All institutions of higher education are required to have an information resources security program consistent with these standards, and the institution of higher education head is responsible for the protection of information resources.”

University Policy: UTS 165 Bulletin #2 - Baseline Standard for Information Security Programs. Bulletin Purpose: Each Entity of The University of Texas System is charged with establishing and maintaining a standards and risk based Information Security Program (Security Program) that:
- secures the information assets under its stewardship against unauthorized use, disclosure, modification, damage or loss to reduce risk to acceptable levels;
- is documented and verifiable; and
- meets regulatory compliance requirements applicable to the Entity.

Program Scope
The program scope includes identifying technologies utilized to minimize risk, establishing training programs to ensure the protection and integrity of confidential information, and establishing procedures for enforcement by the institution.

Please note that this program includes confidential information 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.

Program Exceptions
The Chief Information Security Officer has granted a security exception to student housing to allow students to use networking hardware (switches and hubs) to provide more network access ports in their dorm rooms.