April 30, 2015

Dr. W. David Watts, President
University of Texas of the Permian Basin
4901 E. University Boulevard
Odessa, Texas 79762

Dear Dr. Watts:

We have completed our audit of the University of Texas of the Permian Basin (UTPB) compliance with the information security rules as required by the Texas Administrative Code, Title 1, Part 10, Chapter 202, on information security standards (TAC 202).

Our audit was conducted in accordance with the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing and criteria set forth under TAC 202.

Overall, we found that UTPB is in general compliance with TAC 202. We did find that improvement in certain areas would enhance protection of information resources and compliance with TAC 202, as detailed in the attached report.

We wish to express our appreciation to management and staff of UTPB for the courtesy and cooperation extended to us during this audit.

Sincerely,

Glenn Spencer
Director of Internal Audit – UT Permian Basin
UT System Audit Office

cc: Mark McGurk, Vice President for Business Affairs, University of Texas of the Permian Basin
Ken Bridges, Interim Director, Information Resources Dept., University of Texas of the Permian Basin
Steven Larizza, Chief Information Security Officer, University of Texas of the Permian Basin
J. Michael Peppers, Chief Audit Executive, UT System Audit Office
Eric Polonski, Assistant Director, UT System Audit Office
Randy Wallace, Associate Vice Chancellor–Controller, UT System
Dr. Pedro Reyes, Executive Vice Chancellor for Academic Affairs, UT System
Alan Marks, Assist. Vice Chancellor for Academic Affairs, UT System
Ed Osner, Legislative Budget Board
Candice Woodruff, Governor’s Office
State Auditor’s Office
Sunset Commission
Texas Administrative Code (TAC) 202
System Security
Audit Report – FY 2014

April 2015

Office of Internal Audit
4901 E. University
Odessa, Texas 79762
Table of Contents

Executive Summary ................................................................................................................. 3
Background ............................................................................................................................. 3
Audit Objectives ...................................................................................................................... 3
Scope and Methodology ......................................................................................................... 3
Audit Results ........................................................................................................................... 4
Conclusion .............................................................................................................................. 5
Executive Summary

Based on our audit, The University of Texas of the Permian (UTPB) information resources security program is in general compliance with the information security standards found in Chapter 202, Subchapter C, of the Texas Administrative Code (TAC 202). However, improvement in certain areas would enhance protection of information resources and compliance with TAC 202 provisions.

TAC 202 requires that each State agency conduct a biennial review of its information security program. This audit is intended to meet that requirement.

Background

TAC 202 is a compilation of information security rules for Texas state agencies. Chapter 202, Subchapter C, sets forth information security standards specifically for institutions of higher education. According to these standards, all institutions must conduct a biennial compliance review of its information security program, based on business risk management decisions. UTPB’s prior audit of TAC 202 compliance was completed in March 2012 by the UT System Audit Office.

UTPB’s Chief Information Security Officer (CISO), along with the Information Resources Division (IRD) Interim Director, are charged with ensuring the University’s compliance with TAC 202 requirements.

Audit Objectives

The objectives of this audit were to determine whether the UTPB information resources security program complies with the information security standards prescribed by TAC 202 and to satisfy the requirement for biennial compliance review of the information security program pursuant to §202.71(e).

Scope and Methodology

The scope of this audit encompassed management of all UTPB information resources including, but not limited to, centralized information systems. Our audit was conducted in accordance with the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing.

We performed a risk assessment to identify high-risk areas within the TAC 202 provisions that were in effect at the time of our audit. Along with this, we considered the results from the prior audit along with the implementation status of recommendations. Audit procedures included interviews with management and staff; review of current policies, procedures, guidelines, and other supporting documentation; and limited testing.
Audit Results

As a whole, UTPB’s information security program generally complies with TAC 202. Improvements could be made in certain areas as described below, but audit findings are not of such significance to indicate non-compliance. A discussion of those specific areas that can be improved upon are shown below.

Finding #1: Management and Staff Responsibilities-§202.71
TAC §202.71 (b) requires that institutions of higher education are responsible for defining all information classification categories. University of Texas System Policy UTS165 also requires data classification at the institution level. However, UTPB has not adopted and included data classification standards in its information technology (IT) operating procedures.

Recommendation: UTPB should review, update as necessary, and include data classification standards in its IT operating procedures.

Management’s Response: We concur. The University will develop the University’s Information Security web pages to include the standards in its information technology procedures. This change will be communicated to the campus via email notification.

Implementation Date: August 31, 2015 – Posted to the UTPB website.

Finding #2: Managing Security Risks-§202.72
TAC §202.72 (a) requires that a risk assessment of information resources be performed and documented. It also requires that the risk assessment be updated based on inherent risk. IRD participates annually in providing information for the internal audit risk assessment process. However, this risk assessment process is of a different scope and uses different criteria in determining risk than the IT risk assessment process required by TAC 202.

Recommendation: IRD should complete IT security risk assessments as required under TAC 202 and include the Chief Information Security Officer (CISO) in the process.

Management’s Response: We concur. UT System has procured the necessary tools for Information Security to do risk assessments, called RSA Archer.

Implementation Date: A risk assessment of the Information Security Program will be completed by July 31, 2015.

Finding #3: Business Continuity Planning-§202.74
This section of the TAC requires that UTPB have a disaster recovery plan, obtain approval of the plan from the University head (or designee), and that the plan be tested annually. The University has a plan; however, approval of the plan by the University head (or designee) could not be documented. In
addition, the plan should be updated to include current systems such as PeopleSoft. Finally, testing of the plan was not formally documented in detail.

**Recommendation:** The disaster recovery plan should be updated, approved by the University head (or designee), and annual testing documentation should be formally documented in detail with information to include items such as: exact steps taken; who performed the testing; the results of such testing, and management review and approval.

**Management’s Response:** We concur. UTPB IRD will review and update the existing disaster recovery plan and obtain appropriate management review and approvals. Once approved, the plan will be tested, documented in detail and reviewed by management. Due to the number of resources currently referenced that are in the process of migration and the current vacant CIO position, we plan to begin review immediately but will not be able to fully complete and test until those projects are completed. Barring any unforeseen circumstances, it is expected that this can be completed before the end of 2015; however there are a number of variables that could affect that date, so the implementation date takes that into account.

**Implementation Date:** March 31, 2016

**Finding #4: Information Resources Security Safeguards- §202.75**
This section of the TAC requires that each institution of higher education head or designee and information security officer shall create, distribute, and implement information security policies. UTPB has information security policies and the CISO (Chief Information Security Officer) has developed a draft Information Security Manual which has not been adopted and included in its IT procedures.

**Recommendation:** UTPB should review, update as necessary, and include the Information Security Manual in its IT operating procedures.

**Management’s Response:** We concur. The Information Security Manual is under review by the CISO and will be ready to send to the VPBA in July 2015.

**Implementation Date:** August 31, 2015 – Posted to the UTPB website.

**Conclusion**
Overall, UTPB has an information security program in place that provides for the necessary knowledge, awareness, and authority to address compliance with TAC 202. The University is in general compliance with TAC 202. We noted some opportunities for improvement, and we believe action on the recommendations in this report will help enhance protection over information resources and compliance with TAC 202.