Texas Administrative Code 202: Phase I

Audit Report # 13-08
June 20, 2014

Office of Auditing and Consulting Services

"Committed to Service, Independence and Quality"
June 20, 2014
Dr. Diana Natalicio
President, University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited-scope audit of the Texas Administrative Code 202 Security Standards for Institutions of Higher Education. The main audit objective was to determine whether an information security policy exists and is enforced, and information resource roles and responsibilities are defined and adhered to.

We appreciate the cooperation and assistance provided by the management and staff of the Information Security Office.

Sincerely,

[Signature]
William A. Peters, CPA, CIA
Director
Report Distribution:

University of Texas at El Paso
   Mr. Richard Adauto III, Executive Vice President
   Dr. Stephen Riter, Vice President for Information Resources and Planning
   Mr. Gerard Cochrane, Jr, Chief Information Security Officer
   Ms. Sandy Vasquez, Assistant Vice President for Compliance Services

University of Texas System
   Dr. Pedro Reyes, Executive Vice Chancellor for Academic Affairs
   Mr. Alan Marks, Assistant Vice Chancellor of Academic Affairs & Athletics Counsel
   Mr. J. Michael Peppers, Chief Audit Executive

External
   Governor’s Office of Budget
   Mr. Ed Osner, Legislative Budget Board
   Internal Audit Coordinator, State Auditor’s Office
   Sunset Advisory Commission

Auditors Assigned to the Audit:
   Lori Wertz (Audit Manager)
   Jerry Montes (IT Auditor)
# Table of Contents

EXECUTIVE SUMMARY ...................................................... 1  
BACKGROUND ........................................................................ 2  
AUDIT OBJECTIVES.............................................................. 2  
SCOPE AND METHODOLOGY .................................................... 2  
Password Policy Enforcement (Priority) ................................. 3  
Separation of Duties Policy .................................................... 3  
User Roles & Responsibilities ................................................ 4  
Security Policy Review ........................................................ 4  
CONCLUSION ......................................................................... 5
EXECUTIVE SUMMARY

The Office of Auditing and Consulting has completed a limited-scope audit of the Information Security Office to determine compliance with established guidelines and requirements specified in Texas Administrative Code Chapter 202 (TAC 202) Subchapter C: Security Standards for Institutions of Higher Education. The objectives of the audit were to determine whether an information security policy exists and is enforced, and to determine whether information resource roles and responsibilities are defined and adhered to. During the audit we noted that:

- the University is not in compliance with password policies,
- the University does not have a separation of duties policy,
- the information security policy does not define user roles and responsibilities, and
- the information security policy has not been reviewed and updated annually.
BACKGROUND

A limited review of University adherence to the Texas Administrative Code 202 (TAC 202) was completed on the Information Security Office (ISO) to evaluate the information security program and determine compliance with established guidelines and requirements as specified in Subchapter C: Security Standards for Institutions of Higher Education. We have divided the TAC 202 audit into four phases that cover the following information security modules:

- Phase 1: Security Standards Policy / Management and Staff Responsibilities
- Phase 4: Managing Physical Security / Removal of Data Processing Equipment

This report outlines the Phase 1 audit results.

AUDIT OBJECTIVES

The objective of this audit was to determine University compliance with TAC 202. Our focal points were to review:

- security standards and polices, and
- management and staff responsibilities.

SCOPE AND METHODOLOGY

The audit scope was limited to information security policies and procedures in effect as of December 1, 2013. Audit procedures included interviewing key personnel, reviewing applicable regulations and verifying the existence of appropriate institutional policies and procedures. The scope for this audit is for sections 202.70 and 202.71 of the TAC 202.

The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors.

AUDIT RESULTS

According to The University of Texas (UT) System Audit Office, “Priority” audit findings/recommendations are reportable audit findings/recommendations that are deemed significant at the institutional level by the institution’s internal audit committee or their designee. Priority audit findings/recommendations are submitted to and tracked by the UT System Audit Office. UTEP’s Office of Auditing and Consulting Services (OACS) tracks all other findings/recommendations. We identified four findings, one of which is considered a priority.
Password Policy Enforcement (Priority)

The University of Texas System (UTS) Identity Management Federation Membership Operating Practices, (MOP), cited as the authority for account management by UTS 165 Information Resources Use and Security Policy, requires that passwords be changed every 90 days. In reviewing section 4.0 of The University of Texas at El Paso (UTEP) Password Policy, however, we determined that this policy has not been followed. The policy states that “all user-level passwords must be changed at least every six months.” Changing passwords more frequently decreases the ability of unauthorized users to gain access to UTEP information resources.

The MOP also requires all user accounts with access to UTEP information resources meet the password complexity requirements. “Passwords must have a minimum length of 8 characters, contain a mix of upper and lower case alpha characters, have at least 2 non-alpha characters (i.e. numerals and/or special characters), and have a password life of 90 days. Additionally, a password history must be maintained to prevent reuse of the current password as the new password.”

Recommendation: User accounts with access to UTEP information resources need to comply with UT System password policies, which include password expiration dates of 90 days and password complexity requirements.

Management Response: Policy will be reviewed and modified to increase the entropy of stored passwords to allow for longer expiration dates. Additional changes will be made to adhere to common practices of password complexity guidelines.

Responsible Party: Gerard Cochrane Jr.

Implementation Date: September 30, 2014

Separation of Duties Policy

During a review of all security policies, we determined that the University does not have a separation of duties policy. Separation of duties ensures that duties are assigned to individuals so that no one individual is assigned incompatible responsibilities. This practice of separation of duties promotes integrity in a process and also limits the ability for one user to have over-reaching access based on his or her assigned duties.

Recommendation: A separation of duties policy should be created by the Chief Information Security Officer (CISO), approved by University management and adhered to by all University employees.
Management Response: A new policy will be created to address the separation of duties issues. This will also include user roles and responsibilities as requested in the next audit result since these areas are related.

Responsible Party: Gerard Cochrane

Implementation Date: September 30, 2014

User Roles & Responsibilities

The Information Security Policy defines the responsibilities of the information owner and custodian; however, user roles are not defined. The absence of user role definitions may allow for the improper use of information resources.

Recommendation: The CISO should define user roles and responsibilities in the Information Security Policy.

Management Response: This policy will be included in the separation of duties policy.

Responsible Party: Gerard Cochrane

Implementation Date: September 30, 2014

Security Policy Review

The information security policy for the University has not been updated since 2002, nor is there a record of the policy being reviewed annually. Out-dated security policies do not contain current changes in laws, regulations and legislation, which could cause improper use of UTEP information resources.

Recommendation: Procedures should be developed to review and update security policies on an annual basis. Any changes should be documented on a revision page which annotates both the change and date of change.

Management Response: Working to develop a new process for reviewing and approving updates to the policy on a regular basis.

Responsible Party: Gerard Cochrane

Implementation Date: December 31, 2014
CONCLUSION

Based on the results of audit procedures performed for the security modules covered in Phase 1, we believe that the University is not in compliance with sections 202.70 and 202.71 of TAC 202; however, we believe that the University will be in compliance by implementing our recommendations.

As stated in the Password Policy Enforcement recommendation, UTS 165 requires passwords have expiration dates of 90 days and meet complexity requirements. We are of the opinion that the action plan provided in the management response is not sufficient to meet those requirements, and therefore is considered a Priority Finding with management accepting the associated risk of noncompliance.

We thank the Information Security Office and staff for their assistance and cooperation during the audit.