TEXAS HIGHER EDUCATION
COORDINATING BOARD

P.O. Box 12788 Austin, Texas 78711

(512) 427-6101
Fax (512) 427-6127

Web site:
http://www.thecb.state.tx.us

September 10, 2019

Dr. Raymund A. Paredes
Commissioner of Higher Education
1200 E. Anderson Lane
Austin, TX 78752

Dear Dr. Paredes:

I am attaching the final report of the *Review of Selected Security Awareness Practices at the Texas Higher Education Coordinating Board*, Report No. THECB-IA-WP-19-219.

The issues presented in this report resulted in a Category 1 Report Rating. These reports contain no or minimal reportable observations. While the noted observations require management attention, if addressed timely they do not pose a significant risk for negative reputational or financial consequences.

If you have any questions or comments, please let me know.

Sincerely,

Mark A. Poehl

Mark A. Poehl, CPA, CIA, CISA, CFE
Director, Internal Audit and
Compliance

EXECUTIVE SUMMARY

Selected security awareness practices were generally effective in ensuring that Coordinating Board data is protected from loss or compromise. Our observation of employee work areas and paper recycle bins resulted in no exceptions. Physical documents were protected in compliance with agency policies.

However, issues that warrant attention to better protect the agency's data include:

1. Agency staff are not complying with the agency requirement to lock computer terminals when unattended.
2. Agency mandated annual security awareness training is not updated to properly train staff on how to lock a computer terminal.

Review Objective, Scope and Methodologies

The review objective was to review selected security awareness practices at the Coordinating Board. Our scope was to observe if:

- Confidential data in paper format were protected.
- Passwords were written down and displayed at an employee's work area where they might be seen by unauthorized individuals.
- Computer monitors were left unattended without logging off or locking the device.

We performed unannounced walk throughs both during and after standard working hours.

Background

The Internal Audit plan for FY 2019 included a project to assess corrective action plan implementation to address the NTT Texas Cybersecurity Assessment Report issued in 2017. Since a new vendor, AT&T, was selected by the Texas Department of Information Resources to conduct a cybersecurity assessment in 2019, our Internal Audit project focused on one area, security awareness and training, where the agency scored lower than the statewide average on the 2017 assessment by NTT. Future Internal Audit projects will assess implementation of recommendations from AT&T.

Detailed Observation, Recommendation, and Management Response

1. **Agency staff are not complying with the agency requirement to lock computer terminals when unattended.**

   Agency staff are not complying with the agency requirement to lock computer terminals when unattended.

   We noted unattended workstations with sensitive information displayed in the following areas:

   - Student Financial Aid Programs
   - Academic Quality and Workforce
   - Strategic Planning and Funding
   - College Readiness and Success
   - Academic Planning and Policy
   - Financial Services
   - General Counsel
   - External Relations
   - Commissioner's Office
   - Innovation and Policy Development
   - Information Solutions and Services

   The protection of confidential information in any form is required to comply with the Family Educational Rights and Privacy Act (FERPA) and other applicable laws. Additionally, two Information Solutions and Services policies provide requirements for all agency personnel.

   - Agency security policy HH-10 requires users to ensure that confidential data, regardless of form (electronic media, paper, etc.) are protected from disclosure to or modification by unauthorized individuals.

- Agency user policy HH-13 states that PCs should not be left unattended without logging off/locking the device.

Noncompliance with security law and policy places confidential or sensitive agency data at risk of disclosure to unauthorized individuals.

Recommendations:

Ensure that staff are aware of, and comply with, FERPA and agency policies regarding the security of confidential and sensitive information.

Management Response:

October is the National Cybersecurity Awareness Month. The ISS security team is working on a series of events to help raise awareness among the agency staff on security best practices and the related agency policies. We will include this topic in the training and communication materials.

To ensure continuous awareness and compliance, the Information Security Officer (ISO) will also publish security updates and best practices in the quarterly Employee Newsletters.

Implementation Date:

October 2019

Responsible Party (ies):

Zhenzhen Sun, Assistant Commissioner for Information Solutions and Services

2. Agency mandated annual security awareness training is not updated to properly train staff on how to lock a computer terminal.

Agency mandated annual security awareness training is not updated to properly train staff on how to lock a computer terminal. The content of the training included the process for locking a computer screen as 'Windows + L". However, the related test question listed the correct answer as 'pressing Ctrl + Alt + Del to lock the computer'. Though this answer is an alternate method to take the first step of locking a computer screen, the second step of 'pressing the lock option' was not shown.

Incorrect or incomplete information in the agency training curriculum regarding information security practices places confidential and sensitive agency information at increased risk of compromise.

Recommendations:

Revise the annual security awareness training presentation to ensure that required practices are accurately and completely covered.

Management Response:

Management agrees with the observation. The security team updated the security awareness training content on 8/28/2019 per the audit team's recommendation.

Implementation Date:

August 28, 2019

Responsible Party (ies):

Zhenzhen Sun, Assistant Commissioner for Information Solutions and Services

PERFORMED BY:

Ms. Aporajita Ahmed, CPA, CFE, CGMA, CICA, CITP, Internal Audit Lead

cc:

THECB

Board Members

Commissioner's Office

Dr. David Gardner, Deputy Commissioner for Academic Planning and Policy
Ms. Linda Battles, Deputy Commissioner for Agency Operations and Communications
Mr. William Franz, General Counsel
Zhenzhen Sun, Assistant Commissioner for Information Solutions and Services

STATUTORY DISTRIBUTION REQUIREMENT

Legislative Budget Board
Mr. Christopher Mattson

Governor's Office of Budget & Planning
Mr. John Colyandro

State Auditor's Office
Internal Audit Coordinator

Sunset Advisory Commission
Ms. Jennifer Jones