

COMMISSION MEMBERS

The Honorable Pete C. Alfaro
Chairman, Baytown

Don Bethel
Vice Chairman, Lamesa

Stephen Fryar
Brownwood

Patsy Reed Guest
Duncanville

Bill Mahomes
Dallas

Gogi Dickson, PH.D.
San Antonio

Juan S. Muñoz, PH.D.
Lubbock



INTERNAL AUDIT DEPARTMENT

Audit Report
on

EXECUTIVE MANAGEMENT

Dwight Harris
Executive Director

Linda S. Reyes, PH.D.
Deputy Executive Director

**Fiscal Year 2006
Texas Administrative Code
Chapter 202 Compliance**

INTERNAL AUDIT DIRECTOR

Karin L. Hill, CIA, CGAP

Internal Audit Department
P.O. Box 4260
Austin, TX 78765

September 2006

Texas Administrative Code,
Chapter 202 Compliance

Audit Team

Karin Hill, CIA, CGAP

For additional copies of this report, please request 06-8



INTERNAL AUDIT DEPARTMENT

TO: Texas Youth Commission Board Members
The Honorable Pete C. Alfaro, TYC Board Chair
Don Bethel, TYC Board Vice Chair
Stephen Fryar, TYC Board Member
Patsy Reed Guest, TYC Board Member
Bill Mahomes, Jr., TYC Board Member
Gogi Dickson, Ph.D., TYC Board Member
Juan S. Muñoz, TYC Board Member

Dwight Harris, TYC Executive Director

FROM: Karin Hill, Internal Audit Director

DATE: September 21, 2006

RE: Results of the Texas Administrative Code, Chapter 202 Compliance Audit

This report presents the results of the Fiscal Year 2006 review of the Texas Youth Commission's (TYC) compliance with the Texas Administrative Code, Chapter 202 (TAC 202), Information Security Standards as amended April 24, 2006.

To determine compliance, we requested Information Resources management to complete a questionnaire which included each requirement of TAC 202; followed up on responses of "No" or "Not Applicable"; and verified selected areas with a "Yes" response.

This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and with *Generally Accepted Government Auditing Standards*.

We appreciate the cooperation and assistance provided to us during our work.

The Texas Youth Commission complies with the Texas Administrative Code, Chapter 202.

TAC 202 is the codification of standards to ensure that the information resource assets of the State of Texas are protected from unauthorized access, disclosure, modification or destruction, as well as assure the availability, integrity, utility, authenticity and confidentiality of information. It assigns management and staff responsibilities for the various aspects of the information security program, such as managing security risks, physical security, business continuity planning, information resources security safeguards and user security practices.

A formal information security program has been approved by the Executive Director. An information security program includes all the people, policies, procedures and equipment deemed necessary to protect the information resources used in the day-to-day operations of the agency. It is designed to protect the individual systems from outside interference and ensure the accessibility, confidentiality and integrity of the information included in them. The information security program is the document which encompasses all the requirements of TAC 202.

The Information Resources Department has completed the information resources risk assessment and presented it to the Executive Director. Risk analyses are used to evaluate a system's risks and determine how those risks have been mitigated. While TYC has a number of information systems, their level of criticality differs and therefore the risks associated with them differ. The Information Resources Department (IRD) completed a comprehensive risk assessment that specifies the risks of each of the agency's electronic systems to include how the agency would need to function to meet its mission in the absence of its electronic systems. The IRD identified three systems as critical to the agency in performing its core mission, but outlined for each that although it would be inconvenient and time-consuming, the agency could still function.

The agency has developed a Business Continuity Plan as well as a Disaster Recovery Plan. Due to recent natural disasters affecting TYC facilities, additional emphasis has been placed on ensuring a comprehensive and effective Business Continuity Plan (BCP) exists. The BCP for the Central Office includes procedures to activate the plan, how to establish the emergency operations center, and checklists outlining each departments responsibilities. While the BCP does not include the Information Resources Disaster Recovery Plan (DRP), it does include the executive summary of that plan. The BCP is maintained by the Director of Risk Management, who keeps a copy at his place of residence and distributes copies to each executive manager. Additionally, the DRP is maintained on the IRD management drive with a copy kept off-site at the Director of Operations residence.

In addition to the BCP for the Central Office, the agency has developed a plan for the evacuation of its facilities. On two different occasions, institutions and/or halfway houses required evacuation last year. This is an enormous undertaking that requires coordination of a multitude of other agencies and TYC locations. This plan is updated and improved as lessons are learned from implementing it.

Physical access to the agency's information resource systems is adequately controlled. Physical access to TYC information resources is controlled by security badges with permissions set by employee responsibility at the Central Office and entry gates and reception areas in the field. The Texas Building and Procurement Commission (TBPC) is responsible for the building the Central Office resides in and provides the necessary environmental protection for the equipment. TBPC last tested the emergency processes and equipment in July 2006 during a power source upgrade. The IRD management has requested updated procedures in writing from TBPC staff.

Staff are made aware and routinely reminded of their responsibilities concerning the agency's information resources. Newly hired staff are briefed on their responsibilities to properly use information and maintain the required confidentiality during new employee orientation (NEO) at which time they sign the HR-016, Information Security and Non-Disclosure Agreement. In addition to NEO, all staff are required to complete Ethics and Confidentiality annually which includes information regarding information security. With the exception of the correctional care and finance systems, persons identified as "owners" (based on their position) of information resources are responsible for granting access to other staff. Access to the finance system and CCS is usually given upon request from the hiring supervisor based on each individual's job responsibilities.

The Information Resource Logon section receives daily reports that summarize personnel changes and use these to ensure access to the network, CCS and the finance system is appropriately discontinued when staff terminate employment from the agency. However, verification work on another audit identified that staff that leave the agency are not always removed from systems which IRD does not control. With IRD disabling access for terminated employees, those terminated would no longer have access to the network and therefore could not access these other systems either; however, not disabling their access leaves the potential for current staff, to use UserIDs that should no longer be valid. A process to ensure staff's UserIDs are removed from all agency applications when employment is terminated.

Data storage devices are removed from obsolete computers and destroyed according to State requirements. With much of the information agency staff handle being confidential, ensuring that that information is not accidentally released through inappropriate disposal of storage devices is paramount. To address this, the IRD has implemented a process that require hard drives to be removed from computers that are being disposed of to be destroyed. As computers are taken out of service and replaced, the hard drives are removed and brought to the Central Office where they are put in a locked bin. As required, TYC contracts with Austin Task, Inc. for the pick up and destroying of storage devices – the amount due for the service is based on the weight of the devices being destroyed. Although once in the bin, ensuring the items are destroyed is controlled by the lock; there is no control to ensure the hard drives are always removed and put in the bin. This weakness in controls allows for the chance that a hard drive, containing sensitive or confidential information, is inadvertently left in a machine which is disposed of.

RECOMMENDATION	MANAGEMENT RESPONSE CURRENT STATUS PROJ. COMPLETION DATE
<p>1. To strengthen the controls over system access, the Assistant Executive Deputy Director of Information Resources should develop a process to ensure that individual UserIDs to all agency applications are removed upon termination of employment with the agency.</p>	<p>CONCUR Planned November 1, 2006</p> <p>IRD Security staff will prepare a report of users for owners of systems that do not use integrated network security. The report will be provided on a routine basis and owners will be asked to confirm access for all authorized system users.</p>
<p>2. To strengthen the controls over the disposal of electronic storage devices, the Assistant Executive Deputy Director, Information Resources should develop a process to ensure their proper removal and disposal.</p>	<p>CONCUR Planned November 1, 2006</p> <p>Upon removal from a computer, support staff will write the property tag number on each electronic storage device (hard drive). As storage devices are packaged for destruction the tag numbers will be logged and retained to confirm proper disposal.</p>

PLANNED: Management concurs with the recommendation but actual implementation of the recommendation has not begun.

UNDERWAY: The implementation process of the recommendation has been started.

IMPLEMENTED: All new procedures, policies, systems, processes, related documents, and other elements relevant to the audit recommendation have been prepared, approved, and put into operation.

UNABLE TO IMPLEMENT: Management concurs with the recommendation; however, due to resource constraints and competing priorities is not able to implement or can only partially implement the recommendation.