

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

**Information Technology:
Security – Youth Access**

INTERNAL AUDIT DIRECTOR

Karin L. Hill, CIA, CGAP

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

November 2006

**Information Technology:
Security – Youth Access**

Audit Team

Charlene Severance, CIA, CPA, CISA, CMA
Barbara Simpson, CGAP

For additional copies of this report, please request 06-7



INTERNAL AUDIT DEPARTMENT

TO: Texas Youth Commission Board Members
Pete Alfaro, TYC Board Chair
Don Bethel, TYC Board Vice Chair
Stephen K. Fryer, 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, Ph.D., TYC Board Member

Dwight Harris, Executive Director, Texas Youth Commission

FROM: Karin Hill, Internal Audit Director

DATE: November 16, 2006

RE: Results of the Information Technology: Security – Youth Access Audit

Attached for your approval is our report on the audit of the Texas Youth Commission's (TYC's) Information Technology: Security – Youth Access. The objective of this audit was to determine the adequacy and effectiveness of the agency's controls over youth access to/on information resources.

To achieve this objective we interviewed and surveyed staff in Central Office and the field; surveyed superintendents and principals; reviewed education policies; analyzed data on incidents involving youth misuse of computers; and attempted to circumvent security on classroom and staff computers on the TYC network.

The agency has effective controls in place to ensure that youth do not use computers to gain access to inappropriate or confidential information. Policies and practices have been put in place to ensure the physical security of both staff and youth computers. In addition, the Central Office Information Resources Division (IRD) has implemented security features on staff and youth computers that make it very difficult for youth to access inappropriate or confidential information.

There were no recommendations from this audit, however several best practices were noted. We appreciate the cooperation and assistance provided to us by the institutional staff we visited or contacted and Central Office management.

cc: Linda Reyes, Ph.D., Deputy Executive Director

This report presents the results of our audit of Information Technology (IT): Security – Youth Access. The objective of this audit was to determine the adequacy and effectiveness of the agency’s controls over youth access to/on information resources.

To accomplish this objective we: interviewed and surveyed staff in Central Office and the field; surveyed superintendents and principals; reviewed education policies; analyzed data on incidents involving youth misuse of computers; and attempted to circumvent security on classroom and staff computers on the Texas Youth Commission (TYC) network. The scope of this work was September 2004 through February 2006.

To ensure that the State’s technology applications standards are being taught and that youth develop the computer skills generally needed for employment, the youth in TYC’s care are granted access to computers in school as a part of the education process. With the goal of all youth gaining a basic level of computer literacy, the agency attempts to place every youth into a Business Computer Information Systems (BCIS) class and provides access to computers in other academic settings.

Because youth computer access is in the schools, education staff (teachers, teacher aides) have the primary responsibility for ensuring they do not misuse the technology. Additionally, local Network Specialists and the Central Office Information Resources Division (IRD) also share responsibility for the physical and logical security of the computers. The Network Specialists have the hands-on responsibility for maintaining the computers and investigating allegations of inappropriate use and the IRD is responsible for establishing the overall security for the computers and ensuring that inappropriate sites and information are blocked.

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

Controls to ensure that youth do not gain access to inappropriate or confidential information are effective.

Texas Youth Commission facilities have computers located throughout their campuses for use by the staff and students. Securing both staff and classroom computers against misuse by the youth is important in ensuring that youth are not able to gain access to inappropriate or confidential information. For the agency to operate, staff must have access to computers for a variety of purposes including: entering incident reports, writing Individual Case Plans (ICP) and counseling notes, entering student information into the Correctional Case System (CCS), and recording their timekeeping, leave and other personnel-related information. Incidents of youth accessing staff computers have the potential to be more serious due to the confidential nature of the information available on those computers.

Computers for youth use are located in classrooms, where they are given limited access to help further their education. Youth at each facility use a generic student logon to access classroom computers. The security features connected to the student logon restrict the youth to a controlled selection of education-related programs and websites. Use of the student logon, whether in the school or on a staff computer, places the same level of restrictions on what the user can access, making it more difficult for youth to gain access to inappropriate information.

Security policies have been established to limit youth computer access in the classroom. The Education Manual establishes the responsibilities of education staff for ensuring youth computer use in the classroom is appropriate. It outlines what access is permitted and gives guidance to staff on monitoring. Both staff and youth are required to read and sign forms annually that inform them of the appropriate use policies. By signing the form, youth acknowledge that they understand the rules for computer use and the consequences for breaking the rules. The form signed by staff details what the agency considers appropriate use of computers in the classroom and the expectations for staff.

In July 2005 a policy was put in place requiring teachers to have students fill out a sign-in log when they use the computers in the classroom, noting which computer they were on and at what times. The logs allow the teachers to hold the youth accountable for any attempted security breaches or damage to the computers that occur during the time the youth was documented as being on the computer.

In a survey of TYC principals concerning security practices, respondents included use of the sign-in logs, in accordance with this policy, among their expectations of the teachers. Further discussions with teachers indicated that most are using the sign-in logs and for most of the classrooms visited during the audit the forms were being used. In those instances where the teachers were not using the logs, other mitigating controls were in place. For example, in one BCIS classroom visited, where the youth spend the entire class period on the computers, instead of a sign-in log the teacher uses a seating chart noting which youth is assigned to which computer. Other teachers who were not using the form noted that they very rarely allowed the youth access to the computers in their classrooms and would monitor the youth closely when they did. While those not following policy were providing adequate supervision of computer use, all teachers should be following policy to ensure instances of misuse can be tracked to the individual youth through documented means. This will be more important with the TYC Education department's initiative to increase use of computers in the classrooms by encouraging teachers to integrate computers more into their curriculum.

The Central Office Information Resources Division has established security features that prohibit youth from accessing inappropriate or confidential information on classroom computers. While the local Network Specialists are responsible for the day-to-day maintenance of the classroom computers, the Central Office IRD is responsible for setting and maintaining the security features statewide. This helps ensure that security is uniform across campuses and allows for changes in the security settings to be applied as needed and put into effect.

To ensure youth do not access inappropriate information, the agency has established significant restrictions on the sites and programs youth have access to in the schools. The school computers are loaded with only those programs deemed necessary for educational purposes – no games and no points of access into the settings for the computer. The youth are limited to basic programs such as Word, Excel, Access, General Education Development (GED) prep courses, and programs related to their class work. In addition, access to the internet is limited. Rather than using a security system that includes a list of restricted sites, TYC's internet access for youth is based on a list of sites approved by the Central Office IR and Education departments. The approved sites are cached daily by IRD and the youth access this cache rather than the actual internet site. As a result, even when accessing these approved sites the youth are not actually on the internet. Attempts by audit staff to circumvent security and access non-approved sites were unsuccessful.

Security features are also in place on the classroom computers to limit what can be accessed with a staff's username and password. In the event that a youth obtains a staff's username and password, they are unable to use them to access the internet or other confidential agency programs on the classroom computers. During the course of this audit, audit staff logged on to classroom computers using staff usernames and were unable to access the internet. We were also unable to open the TYC intranet page, which precluded access to programs such as the Correctional Care System (CSS), Human Resources Information System (HRIS), the various report features, and other agency information available to staff through the intranet.

Local practices have been established for monitoring youth computer use in the schools. Interviews with teachers and principals and observation by audit staff identified that teachers conduct constant monitoring of youth activity in their classrooms, including monitoring youth who are on the computers. The teachers indicated that they rarely get a chance to sit down during classes as they are constantly moving throughout the classroom to answer questions and to ensure the youth stay on task.

In addition to monitoring by the teachers, both the principals and network specialists do walk-through monitoring in the schools. The principals at the facilities visited for the audit reported that they walk through the building on a daily basis to watch the teachers and offer feedback on any issues they note. This includes looking at what the youth are doing on the computers and how the teacher is monitoring that use. The network specialists interviewed conduct similar monitoring when they are in the school buildings. They regularly work on the computers in the schools and use that as an opportunity to review information in the computer's cache and on the hard drive to ensure youth have not saved or accessed any inappropriate information.

Finally, a walk-through of facilities by audit staff noted that the placement of the classroom computers allowed for a good line of site for the teachers. The computers were located in such a way that the teacher could see what was on the screen from their desk. Computers were also generally visible from other locations throughout the classroom as the teacher walked through the room to work with students.

Best Practice:

- A survey of principals reported that most meet informally with their network specialists. However, one facility noted that they conduct a formal, monthly meeting between the principal and network specialists to identify any computer security concerns. Interviews with the relevant staff indicated that they find this meeting useful and have used it to solve a variety of technology issues. They are able to identify issues and brainstorm solutions.

Youth generally do not have access to staff computers. To access inappropriate websites or confidential information requires that the youth have access to both a staff computer and a staff username and password. Incidents of youth obtaining access to staff computers are very rare; a review of incident reports from September 2004 through February 2006 identified a total of 14 incidents of youth improperly accessing computers outside of school. Both physical security measures and the security programs within the staff computers themselves contribute to the low number of incidents.

At the facilities visited, staff computers are not placed in the common areas of the dorm, but instead are kept in locked offices. This includes the computers the Juvenile Correctional Officer (JCO) staff use for entering their timekeeping information. The offices are kept locked when staff are not present and youth are not allowed in them unescorted. Regular checks of office locks are conducted as a part of required monthly inspections to ensure that the locks are not damaged and are working properly.

Because staff computers contain confidential information it is important to ensure that accessing them is made as difficult for youth as possible. The agency's policy requiring staff computers to "lock" and go to a screen saver after no more than three minutes of inactivity is one way youth access is made more difficult. Youth access is also limited by security features on the staff computers that prohibit youth from using their student log-in to access any program or information that they would not have access to on one of the classroom computers. Attempts by audit staff to use student log-ins on staff computers identified that youth only have access to the internet through Internet Security and Acceleration Services (ISA), the same program used in the school. As well, any attempts to open programs on staff computers that are not available on the school computers (i.e. the Correctional Care System (CCS) used to store student data or games) resulted in an access denied message.

Best Practices:

- At one institution visited during this audit, the Business Manager routinely checks staff computers to ensure they are locked. As a part of his monthly inspection of the facility, and at other random times when he is moving around the campus, the Business Manager checks that the computers in staff offices are secure. If not, he emails himself from the staff's computer and then replies to them when he gets back to his own office reminding them to always lock the computer when they are out of the office. If this happens a second time he emails that staff's supervisor. During discussion with the Business Manager, he noted that this has significantly reduced the

number of computers he finds unlocked, indicating that staff have a good understanding of the agency's security practices and are following them.

- Another means of ensuring good security on staff computers is providing proper training on the security policies and practices of the agency. One institution visited during the audit includes the Network Specialists as a part of providing on-the-job training (OJT) for new staff who will have computer access. To ensure that staff understand the agency's expectations regarding keeping the information on their computers secure, the Network Specialist reviews the computer use policies and basic information security practices such as how to set and change a password, that passwords may not be shared, how and when to lock the computer and the importance of staff locking their office when they away from their desk.

There are no recommendations for management action.