December 15, 2009

Connie L. Derr
Audit Coordinator
Division of Budget
Bureau of Budget and Fiscal Management
Department of Education
333 Market St- 4th Floor
Harrisburg, PA 17126-0333

Re: Performance Audit Report Response and Corrective Action Plan

At the regularly scheduled meeting of the Erie County Technical School Joint Operating Committee held on December 15, 2009 the following audit response resolution was reviewed and adopted.

The Joint Operating Committee resolved to adopt the attached response and corrective action plan to the Performance Audit Report issued by the Office of the Auditor General for the years ended June 30, 2008 and 2007.

Respectively submitted,

Michele Campbell
Superintendent of Record
Erie County Technical School

Paul D. Fritz
Secretary
Joint Operating Committee
Erie County Technical School

OBSERVATION – Performance Audit Report

Unmonitored Vendor System Access and Logical Access Control Weaknesses

The Erie County Technical School uses software purchased from an outside vendor for its critical student accounting applications (membership and attendance). The software vendor has remote access into the School's network servers.

Based on our current year procedures, we determined that a risk exists that unauthorized changes to the School's data could occur and not be detected because the School was not able to provide supporting evidence that they are adequately monitoring vendor activity in their system. However, since the School has adequate manual compensating controls in place to verify the integrity of the membership and attendance information in its database, that risk is mitigated.

Reliance on manual compensating controls becomes increasingly problematic if the School would ever experience personnel and/or procedure changes that could reduce the effectiveness of the manual controls. Unmonitored vendor system access and logical access control weaknesses could lead to unauthorized changes to the School's membership information and result in the School not receiving the funds to which it was entitled from the state.

During our review, we found the School had the following weaknesses over vendor access to the School's system:

1. The School does not have a non-disclosure agreement with the vendor.

2. The School's information technology (IT) security policy does not address syntax requirements for passwords.

3. School employees and students are not required to sign that they agree to abide by the IT security policy.

4. The School does not require that the vendor employees sign that they agree to abide by the IT security policy.

5. The School does not use written forms to add, delete, or change a user ID.

6. The software system does not require users to change their passwords every 30 days; rather it requires the change every 70 days.

7. The School's technology manager reviews the log of vendor activity in the system, but there is no written documentation of the review.

8. There is not a formal complete list of personnel who have access to the physical location of the server.

9. There are no formal written procedures regarding membership data reconciliation procedures.

Audit Report Recommendations and the Joint Operating Committee Response and Corrective Action Plan:

1. AG Recommendation: Execute a non-disclosure agreement with their membership software vendor.
    a) JOC Response: The current vendor SchoolDESX will be asked before January 1, 2010 to sign a non-disclosure agreement similar to the agreement in place with the budgetary accounting software vendor ProSoft. The school is planning to seek proposals for a replacement vendor for a student information system software package during school year 2010-2011 at which time the non-disclosure agreement will be a requirement for the new vendor.

2. AG Recommendation: Revise the School's IT security policy to address syntax requirements for passwords.
    a) Response: The school technology manager developed a set of rules for password complexity effective for school year 2009-2010. A memo was distributed to all faculty and staff and posted on the employee bulleting board. The memo contained instructions for staff and students when prompted to change passwords.

3. AG Recommendation: Require School employees and students to sign that they agree to abide by the IT security policy.
    a) Response: All employees are expected to abide by approved board policies currently in effect including Policy 815-Acceptable Use of Internet. This policy also outlines expectations regarding all computer network resources. The school will develop a statement and require all employees to sign that they agree to abide by Policy 815 effective with the 2010-2011 school year. The ECTS Student handbook contains Section III: Computer/Network/Internet Usage Guidelines. Effective with school year 2009-2010 all high school students and parents sign a student information card that includes a statement that they have reviewed and are familiar with the policies and procedures in the ECTS Student Handbook.

4. AG Recommendation: Require vendor employees to sign that they agree to abide the IT security policy.
    a) Response: The current software vendor School DESX will be asked by January 1, 2010 to sign a statement that their employees agree to abide by the school security policies. The school is planning to seek proposals for a replacement vendor for a student information system software package during school year

2010-2011 at which time the new vendor will be required to sign an agreement that all employees will abide by the school security policies.

5. AG Recommendation: Develop policies and procedures to require written authorization when adding, deleting or changing a user ID.
    a) Response: The school will develop policies and procedures to require written authorization when adding, deleting or changing a user ID to be effective July 1, 2010.

6. AG Recommendation: Require users to change their passwords every 30 days.
    a) Response: The school maintains that the current policy is sufficient with passwords changes required every 70 days.

7. AG Recommendation: Ensure that the School's technology manager produces written documentation of the review of the log of vendor activity in the system.
    a) Response: Effective January 1, 2010, the school will use the current process of Help Desk Request Service Tickets to monitor vendor access. The software vendor is required to open a help desk request ticket to access the school network. The request can be in the form of an email request that is copied to a help desk request by a technology department employee. The help desk ticket is then closed after the Technology Manager reviews and deems the work done is acceptable.

8. AG Recommendation: Ensure that there is a formal complete list of personnel who have access to the physical location of the server.
    a) Response: Effective, January 1, 2010, the Facility Manager will create a list of all key holders to the Network Equipment Room. The door to this room will be kept locked at all times with a sign prominently posted for authorized use only.

9. AG Recommendation: Ensure that there are formal written procedures regarding membership data reconciliation procedures.
    a) Response: The school has developed a written procedure documenting the school district membership data reconciliation procedure. The school Registrar is responsible for the generation of ADM reports and reconciling any differences communicated from the school districts.