Patchogue-Medford School District

Review of Access Permissions

June 2015

June 2015

The Board of Education
Patchogue-Medford Union Free School District
241 South Ocean Avenue
Patchogue, NY 11772

CERINI & ASSOCIATES LLP
CERTIFIED PUBLIC ACCOUNTANTS

Board of Education:

We have been retained to function as the internal auditor for the Patchogue-Medford Union Free School District (hereinafter, "the District"). Our responsibility is to assess internal control systems in place within the District, and to make recommendations to improve upon certain control weaknesses or deficiencies. In doing so, we hope to provide assurance to the District's Board, management, and residents, that the fiscal operations of the District are being handled appropriately and effectively.

In conjunction with our internal audit responsibility, we assessed the adequacy of access permissions assigned to key applications: Finance Manager (financial management system), eSchool Data (student management system), and IEP Direct (special education management system). Access controls are intended to provide reasonable assurance that computer resources are protected from unauthorized use and modifications. Access to these applications requires a valid ID to access the District's network.

To control electronic access, a computer system or application needs a process to identify and differentiate among users. User accounts identify users and establish relationships between the user and a network, computer, or application. The system administrator creates these accounts. These accounts contain information about the user, such as passwords and access rights to files, applications, directories, and other computer resources. The District's claims auditor reviews a report on a monthly basis of access to the District's network (i.e., a report of firewall activity). The report lists the date, time, user, and duration of access. The claims auditor examines the report and highlights any accesses that may appear to be questionable, such as access during non-work hours. The report also identifies failed logon attempts, which helps the District identify possible unauthorized access attempts. The claims auditor provides the results of the analyses to both the Assistant Superintendent for Business as well as the Director of Technology, and any questionable items are followed up.

To perform this evaluation, we gained an understanding of how access is granted and then verified that the access permissions within each of the three applications are properly restricted, that proper segregation of duties exists, and that access is limited based on the user's job descriptions and responsibilities. The results of this review are documented below.

Cerini & Associates, LLP • 3340 Veterans Memorial Highway • Bohemia, NY 11716
phone 631.582.1600 • fax 631.582.1714 • www.ceriniandassociates.com

FINANCE MANAGER

We obtained a report of all users' access permissions within Finance Manager as of December 23, 2014. Finance Manager contains several modules for performing various financial and human resources functions. The District utilizes the following modules:

- Accounting – purchasing, cash disbursements and payments, budget transfers, journal entries, cash receipts.
- Budgeting – budget development and "what-if" scenarios.
- Human Resources – personnel management (employee attendance, appointment earnings, fingerprint information, health benefit information), professional management (tenure and certification information)
- Payroll – contract earnings, employee deductions, retirement contributions, paychecks.
- Negotiations – centralizes employee contract salaries for negotiation, creation of salary schedules.
- Requisitions – creating and approving purchase requisitions.
- System Manager – ability to add/change/delete access permissions within modules (access to this module should be restricted and limited to a few management personnel).

Finance Manager has the ability to produce a log indicating when, where, and who uses the computer system. It can also generate a log of all changes made to the information included in the vendor master files. Because virtually all District accounting records and reports are computer generated, it is important that District officials review audit logs periodically. Without such a review, the District does not have adequate assurance that changes to its financial information are appropriate and authorized.

Finance Manager allows the District to specify the level of auditing that is to take place as transactions are entered, updated, and deleted in the system. There are three settings of audit logging that the District can set:

- **Low**: the audit process is restricted to selected monetary-related tables. Activities related to maintenance of absence, appointment, assignment, deduction, payroll calendar, pay schedules, projections, seniority entry, user maintenance, and vendor maintenance are the types of transactions that are audited when setting the Audit Policy to Low.
- **Medium**: Along with the activities specifically mentioned above under Low, the system will audit the following types of transactions: maintenance to any of the system codes (attendance codes, certification codes, certification types, etc.), cash disbursement/receipt maintenance, purchase order maintenance, PR emergency contact/dependent maintenance, requisition maintenance, etc. With this setting, the system **WILL NOT** audit any of the global utilities, such as projections move to payroll, payroll calculation, etc. Finance Manager recommends that districts utilize this logging setting.
- **High**: In addition to the user activities mentioned above, the system will audit **ALL** database activities, including global utilities such as the earnings move to

payroll, payroll calculation process, change deduction amounts/limits, etc. This setting is generally not recommended, as this type of audit logging has a significant impact on system performance.

We noted that the District's audit logging is currently set to "medium", which is the recommended setting.

Users are assigned access to specific menus within each module. The menus are correlated to specific functions that can be performed within the system, and are categorized as a report, maintenance, utility, or data entry function. Access to each menu function can be restricted by the ability to add, update, delete, and/or print. Permission is granted once the request for access is completed, reviewed, approved by the Assistant Superintendent for Business. The access permissions in Finance Manager are entered by the Application Specialists, and confirmation of the access entered is sent back to the business office.

The District's claims auditor is in the process of analyzing the permissions in Finance Manager on to ensure that the accesses assigned are appropriate. The analysis involves reviewing the permissions assigned to key District employees, noting the specific access, and comparing the permissions to the District's policy on accessibility. The results of the analysis thus far are being reviewed by the Assistant Superintendent for Business to determine if access within the application needs to be further restricted. In conjunction with this analysis, the claims auditor is reviewing audit trail reports to review the specific accesses that are being performed by key employees. The actions performed by the claims auditor decreases the risk of inappropriate access to financial data occurring.

Utilizing the Finance Manager report of all users' access permissions, we analyzed those individuals who have add, update, and/or delete privileges within each menu that was categorized as a data entry function. Based on the access capabilities listed, we assessed if the permissions granted are those functions needed to be performed within the selected employees' job duties, and that each employee is restricted from performing multiple aspects of a financial transaction that could compromise proper segregation of duties.

Our review consisted of examining the permissions assigned to 98 users, specifically focusing on permissions that allow a user to add, update, or delete data. Based on the permissions assigned, we assessed whether the access capabilities correlate to the person's job requirements. We also verified that the ability to override a purchase order as well as the ability to increase a cash disbursement was properly restricted. In general, our review of the access permissions assigned within Finance Manager appears to be appropriately assigned, and the accesses granted are based on job functionality.

eSCHOOL DATA

The District utilizes eSchool Data to maintain all student information. The data maintained in this application is exported to the State (e.g. student attendance data) and is used to interface with the District's special education software, IEP Direct, as well as the District's transportation application. The Director of Technology and two application specialists support eSchool Data in the District. Human Resources staff utilize an electronic routing form to request access to eSchool Data. The Director of Technology reviews the request and the eSchool specialists then create the appropriate account and permissions. Any changes in access must be documented in writing and sent to the Director of Technology. Access to student information within eSchool Data is based on the employee's title and function in the area they serve in the District. Specifically, there are groups created for performing certain functions such as attendance, scheduling, grades, and transcripts.

Issue #1: As some employees work in multiple areas within the District, those employees are assigned to various groups and can have varying access within the application. Therefore, it is very cumbersome to review and confirm if access permissions are set up properly.

Level: Moderate

Risk: Access to student information may not be appropriately restricted.

Recommendation: The District is in the process of further defining access permissions by making access based on roles that are predetermined, rather than groups. We commend this effort and recommend that access within eSchool Data be role-based so that permissions can be readily reviewed and approved on a regular basis.

***Management's Response**: The technology department continues to refine the groups and permissions of users within the eSchool Student Management System, as to ensure staff have appropriate permissions for their current roles. We have identified key areas to evaluate and have enacted a systematic approach to continue the permission review process, including the appropriate adjustment, creation or removal of role based groups.*

IEP DIRECT

The software application, IEP Direct, enables the District to document and track special education services provided to District students. This system utilizes the database information from eSchool Data (e.g., student class lists) allowing data to be integrated automatically.

Actions performed within IEP Direct automatically track the user ID and the date of access. IEP Direct has several reporting features that enable the District to verify the records.

The District manually inputs the student's demographic information in IEP Direct and compares to the information listed in eSchool Data on a regular basis to ensure the data matches. Requests for changes in demographic information must be documented, and are entered only by the system administrators. Changes made to a student's IEP are based on the recommendations from the CSE and are reviewed by the staff responsible for the student's IEP before the IEP change is finalized. The IEP cannot be changed except by the systems administrators.

We obtained a list of all users with access rights within IEP Direct as of December 2014. We also obtained a list of group profiles which lists the specific accesses that can be performed within each group. Within each group, users are further grouped according to their job function and are restricted to view only /edit of certain records (e.g. a special education teacher only has access to those students assigned to the teacher's class).

The administrator for IEP Direct can further restrict an individual's access to specific functions within the group based on job responsibility. Utilizing the report of all users' access permissions, we analyzed the individuals assigned within each group. Based on the list of users within each group, we assessed if the permissions granted are those functions needed to perform their job duties, and that the employee is restricted from performing actions that could compromise proper segregation of duties (i.e. a teacher being able to change an IEP of a student that is not assigned to them). We noted that the Administrator reviews the list of users assigned to each group at least twice per year to ensure access is properly restricted. The District also requires that teachers as well as any new vendors sign a confidentiality form.

The District utilizes the following access group profiles:

1. Central Office Level, Supervisor
2. Central office Level, Edit
3. School Building Level, Supervisor
4. School Building Level, Data Entry
5. School Building Level, View Only
6. Student Level, Data Entry
7. Student Level, View Only

We reviewed a sample of 75 user names from the list of users within all the groups and verified that access to IEP Direct was appropriately requested and the user was assigned to the correct access group. We verified that the individual had the appropriate title as indicated in their Board appointment, as well as the required certifications and/or licenses by examining their personnel file. We also verified that teachers only had access

to the students assigned to their class. Based on our review of the access permissions assigned within IEP Direct, as well as comparison to records maintained in personnel files, the accesses assigned within IEP Direct appear appropriate.

We would like to thank the staff at the District for their cooperation and professionalism during our review.

We understand the fiduciary duty of the Board of Education, as well as the role of the internal auditor in ensuring that the proper control systems are in place and functioning consistently with the Board's policies and procedures.

Should you have any questions regarding anything included in our report, please do not hesitate to contact us at (631) 582-1600.

Sincerely,

Cerini & Associates LLP

Cerini & Associates, LLP
Internal Auditors