STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER
110 STATE STREET
ALBANY, NEW YORK 12236

THOMAS P. DiNAPOLI
COMPTROLLER

GABRIEL F. DEYO
DEPUTY COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY
Tel: (518) 474-4037 Fax: (518) 486-6479

August 19, 2014

Laura Dutton, Superintendent
Members of the Board of Education
Poland Central School District
74 Cold Brook Street
Poland, NY 13431

Report Number: P3-13-30

Dear Ms. Dutton and Members of the Board of Education:

A top priority of the Office of the State Comptroller is to help school district officials manage their resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

We conducted an audit of six school districts in central and northern New York State. The objective of our audit was to determine whether the districts adequately control access to their student information system (SIS). We included the Poland Central School District (District) in this audit. Within the scope of this audit, we examined the District's policies and procedures and reviewed access to the SIS for the period July 1, 2011 through April 30, 2013. We extended our scope period through October 7, 2013 to perform certain tests of the District's access controls.

This report of examination letter contains our findings and recommendations specific to the District. We discussed the findings and recommendations with District officials and considered their comments, which appear in Appendix A, in preparing this report. District officials generally agreed with our findings and recommendations and indicated they planned to initiate corrective action. At the completion of our audit of the six districts, we prepared a global report that summarizes the significant issues we identified at all of the districts audited.

Summary of Findings

The District did not adequately control access to its SIS. Although the Board of Education (Board) established policies related to the confidentiality of computerized information and breach notification requirements, District officials have not established effective procedures for the administration of the SIS to ensure that access rights are assigned only to authorized users and are compatible with users' roles or job duties. While there is a formal process to add, deactivate or modify user accounts, management does not verify user rights assigned and does not periodically monitor user rights to ensure they are current and appropriate. In addition, management does not periodically review change reports or audit logs to identify inappropriate activity in the system. As a result, personal, private and sensitive information (PPSI)[1] in the SIS is at risk of inappropriate access and misuse.

Our audit found that 13 of the 29 user accounts tested (45 percent) included more access rights than necessary for users to fulfill their roles or job duties; these additional rights included changing student demographic information or grades and viewing and modifying health records. Additionally, some users can assume the identity or account of other users, which may give them more access rights than allowed with their own user account. We also compared the District's active employees to a list of current staff users of the SIS and found three generic user accounts that were not assigned to any specific individuals. When generic accounts are used, accountability is diminished and activity in the system may not be able to be traced back to a single user.

We reviewed audit logs for activities of the 13 users who had more access than necessary and the three generic user accounts. We found two of the 13 users changed student demographics when it was not their job duty to do so. No changes were made using the three generic user accounts.

Our audit also disclosed areas where additional information technology (IT) security controls and measures should be instituted. Because of the sensitive nature of these findings, certain vulnerabilities are not identified in this report, but have been communicated confidentially to District officials so they could take corrective action.

Background and Methodology

The District is located in the Towns of Newport, Norway, Ohio, Russia, Salisbury and Webb in Herkimer County; the Town of Deerfield in Oneida County; and the Town of Morehouse in Hamilton County. It operates two schools with approximately 620 students and 120 employees. The District's budgeted appropriations totaled $13.7 million for the 2013-14 fiscal year. These costs are funded primarily through State aid and real property taxes.

The District is governed by a seven-member Board. The Board's primary function is to provide general management and control of the District's financial and educational affairs. A guidance secretary (project manager**)** is responsible for the day-to-day operations of the SIS. The Mohawk

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, customers (students), third parties or citizens of New York in general.

Regional Information Center (MORIC) houses the District's SIS and provides off-site technical support for the SIS.

The SIS commonly contains extensive information about students, including parent and emergency contacts, attendance, disciplinary actions, testing, schedules, grades, and medical information. Therefore, the SIS includes a considerable amount of PPSI, which students and their parents entrust school districts to safeguard. In addition to providing SIS access to teachers, administrators and various staff members, many districts provide parents with limited access to their child's information and students with limited access to their own information.

Authorized users of the District's SIS are parents, teachers, administrators and various other District staff, as well as MORIC employees and the SIS vendor who are involved in supporting the SIS. The District assigns access rights through 23 different user groups[2] in its SIS for 294 users.[3] Private information in the District's SIS application includes demographic, health, course and special education information; student evaluations; student identification numbers; and current and historical grades. The student data entered into the District's SIS can also be transferred to other operating applications used throughout the District for programs such as school lunch, transportation, and special education. Effective controls can help to prevent the misuse and alteration of student information within the SIS and the transfer of incorrect student information to other operating applications within the District.

To achieve our audit objective, we interviewed District officials and staff and examined the District's policies and procedures to control and monitor access to its SIS. We also performed tests to determine if access was properly restricted based on the users' role or job duties and to determine if staff user accounts were assigned to active District employees.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit is included in Appendix B of this report.

Audit Results

District officials are responsible for developing IT controls to protect and prevent improper access to PPSI in the SIS. Policies and procedures should be established to ensure access is limited to only authorized users of the system and that rights assigned to authorized users are compatible with their roles or job duties. Management should periodically monitor user accounts and rights to ensure the rights agree with formal authorizations and are current and updated as necessary. Management should periodically monitor change reports or audit logs from the SIS for any unusual activity to help ensure that only appropriate changes are being made by authorized users of the SIS.

Policies and Procedures – The Board adopted a Computer Resources and Data Management Policy and regulations governing the use and security of the District's computer resources and the management of computer records (e.g., passwords, backup, segregation of duties and disaster

[2] Comprising 22 instructional and non-instructional staff user groups and one parent group
[3] Comprising 152 parent users, 99 staff users, 42 MORIC employees and one vendor

recovery) for financial, personnel and student information. The Board also adopted a Student Records Policy to maintain the confidentiality of student records and an Information Security and Breach Notification Policy that clarifies PPSI and details how District employees would notify affected parties whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

The District has not adopted written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts and monitoring user access. Although the District has a process in place for adding and changing user rights and utilizes a form to document authorized changes, we found this process was not operating effectively. Individuals were assigned more access rights than they needed for their job duties. In addition, District officials do not periodically review users' access rights for appropriateness and do not review audit logs (system-generated trails of user activity) for potentially unauthorized activity. Finally, management does not monitor employees' use of powerful system features that allow them to assume the access rights of other users. Without written procedures over the maintenance of user accounts, staff responsible for these functions may not understand their role, and there is an increased risk that access to the SIS will not be properly restricted.

User Access – When access is not properly restricted, there is an increased risk that sensitive or confidential data will be exposed to unauthorized use or modification. For example, users may be able to view confidential data to which they should not have access or perform functions that they have no authority to do, such as adding a new user account, or modifying student information, such as grades or demographics.

The District has 23 user groups and each group has an associated set of rights and permissions. The user groups include titles such as Administrators, Counseling, Principal and Teachers. The project manager told us all users within a user group have the same rights and permissions to either view or modify data, or both. The District utilizes a form to document the request and authorization to add a new staff user account, deactivate an account or modify an existing account in the SIS.[4] The form is completed by a user and then provided to the project manager who verbally discusses the user's access rights with the Superintendent before designating the user's role (group) and signing the form to authorize the addition of or changes to the user account. The project manager is responsible for adding,[5] deactivating or modifying the user accounts. When a user account is added to the SIS by the project manager, the form is provided to one of the MORIC employees who is responsible for placing the user in the assigned group(s) as authorized on the form. If a staff member needs rights different than those in any established user group, the project manager (with the Superintendent's verbal permission) will either request a new staff user group be created by the MORIC employees or authorize the MORIC employees to assign the staff user into multiple groups to grant additional rights to the user.

We found weaknesses in the District's process to ensure users do not have more access rights than needed. The project manager discusses user rights to be assigned with the Superintendent; however, there is no formal management approval of the access rights assigned by the project

[4] The District does not add MORIC user accounts to the SIS; these user accounts are added by MORIC.

[5] When a new user account is added to the SIS, the project manager creates the user account and a MORIC employee provides access to the account.

manager. Also, there is no consistent process in place to verify all user's access needs are compatible with the specific rights of the group(s) in which they are placed because the project manager occasionally reviews lists of individual rights granted to each user group, but typically assigns users to a user group based on her historic knowledge of prior users who were assigned the same role. The project manager's ability to assign, create, deactivate, modify and authorize user access rights without any formal indication of management's review increases the risk that users could be assigned more access rights than needed. Lastly, management does not monitor staff user rights on a periodic basis once rights have been assigned, further increasing the risk that user accounts and rights may not be current or appropriate.

As a result of the weaknesses identified, we compared the access rights/permissions of 29 users in 20 groups[6] to their job duties to determine whether their access is compatible and appropriate. We interviewed 18 users who represented each of the groups in our sample to determine what their job duties are and observed them navigating the SIS screens to see what access was available to them. We found 13 of the 29 users (45 percent) tested had more rights than necessary to fulfill their job duties.[7] Further, the user groups that these users were assigned to indicated that, in fact, the number of users with permissions that are not required for their jobs is much larger. The results of our testing disclosed the following:[8]

- The Superintendent told us that only the guidance counselors and the guidance secretary[9] are authorized to change grades from previous marking periods that have been closed out. However, in our sample of 29 users, we found four other users who can also change closed-out grades (the Superintendent, a special education teacher, and two MORIC employees). These four users belong to three different staff user groups. Because the project manager told us user rights and permissions are the same for all users within each user group, all the other users within these three staff user groups are also capable of changing grades. In total, there are 31 users (24 MORIC employees, six staff users and the vendor) who can change grades even though it is not within their job responsibilities to do so.

- The nurse is responsible for viewing and modifying health records; however, two other users in our sample (two MORIC employees) could view and modify health records. These two users are in a group that contains a combined total of 25 users (24 MORIC employees and the vendor) who can view and modify health records even though it is not within their responsibilities to do so.

---

[6] See Appendix B, Audit Methodology and Standards, for details of test selection.

[7] Some staff users had multiple user rights that were not necessary given their job duties. We found that parent access rights were appropriate.

[8] MORIC officials told us MORIC SIS support staff require full access rights to the SIS in order to assist the District with troubleshooting on a day-to-day basis. We did not include SIS support staff as exceptions in our testing. However, we did include the SIS vendor and other MORIC technical staff (e.g., programmers and technicians) in our exceptions because they were granted full access rights to the SIS and they only need occasional access for troubleshooting. Rather than provide full access rights to these users all the time, the District should grant them the necessary access only when they need it.

[9] The Superintendent's secretary and the substitute attendance secretary serve as a backup for the guidance secretary.

- The project manager[10] is responsible for changing student demographic information. However, eight other users in our sample also have the ability to change demographic information such as student age, student user identification number, address and parent contact information. The eight users, included in five staff user groups, are a guidance counselor, Superintendent, elementary school secretary, high school secretary, director of guidance, a clerical substitute and two MORIC employees. Because of the shared user permissions within specific groups, there are 34 users (24 MORIC employees, nine staff users and the vendor) in these five user groups who are capable of making changes to student demographic information even though it is not their job duty/responsibility to do so.

- It is the responsibility of the project manager and MORIC SIS support employees to add new staff user accounts; however, two other users in our sample (two MORIC technical support employees) also have the ability to add new staff user accounts. These two users are in a group that contains a combined total of 25 users (24 MORIC technical support employees and the vendor) who can add new staff user accounts even though it is not within their job responsibilities to do so.

The Superintendent told us that she was not aware that these users had more permissions than necessary. The majority of these users are MORIC technical staff (e.g., programmers and technicians) and the SIS vendor who rarely access the SIS to assist the District with troubleshooting and, therefore, do not need all the user rights they have been granted in the SIS. It is important for the District, in conjunction with MORIC, to review and update user permissions in order to help reduce the risk that sensitive or confidential student information could be compromised.

We also compared a list of all the District's active employees to a list of the 99 current staff users of the SIS to determine if any users of the SIS are not District employees or if any former employees remain on the current user list. Of the 99 users, three were not on the list of active employees and had generic user names that were not assigned to any one individual. The project manager told us the accounts were created as sample or test accounts. When generic accounts are used, accountability is diminished and activity in the system may not be able to be traced back to a single user. District officials should deactivate these generic user accounts to prevent unauthorized use.

User Activity – Given the weaknesses we identified in the District's process for granting user access rights, we reviewed the District's audit logs[11] for unauthorized user activity during our audit period.

Our review of the audit log activity of the 13 users in our audit sample who had more capabilities in the SIS than their job duties required found that two users (a guidance counselor and a MORIC employee) changed student demographics on three occasions even though it is not their responsibility to make these changes. Our review of the audit log entries for the other 11 users

[10] The Superintendent's secretary and the substitute attendance secretary serve as a backup for the project manager.
[11] Audit logs are automated trails of user activities, showing when users enter and exit the system and what they did.

did not disclose any unauthorized activity. In addition, we reviewed the audit log activity for the three generic user accounts and found no changes were made using these accounts.

We also selected a judgmental sample of 10 final grade changes as shown in the audit log. The 10 grade changes were performed by a user who is authorized to make grade changes and included one change from 63 to 65, two changes from 64 to 65 and two changes from 53 and 54 to 65. Although District officials provided us with verbal explanations for all 10 grade changes selected, they had no formal process for documenting grade changes, including who authorized the changes and the reason for the changes, and for retaining the information on file. Without documented authorizations to support grade changes and periodic monitoring of audit logs, there is an increased risk unauthorized users could make inappropriate changes to student information without detection.

"Assume-Identity/Assume-Account" Features – The ability to grant or modify user rights in the SIS should be strictly controlled. Individual users should not have the capability to assign themselves additional user rights beyond those already authorized. However, the District's SIS allows certain users to assume the identity or the account of another user.

- The assume-identity feature allows a user to retain their own rights/permissions while accessing student information for students assigned to the user whose identity they assume. During our testing of the sample of 29 users, we identified eight users[12] in five user groups with the ability to assume identities of another user. In total, these five user groups comprise 34 users (24 MORIC employees, nine staff users and the vendor) who can perform this assume-identity function.

- The assume-account feature is similar to the assume-identity feature in that the user retains their own rights/permissions. However, it allows a user to assume the account of another user and also inherit all the given rights/permissions of that user. Of the eight users in our sample who have the ability to assume the identity of another user, six users can also assume the account of another user.[13] In total, there are 29 users (24 MORIC employees, four staff users and the vendor) who can perform this powerful function.

Audit logs generated from the SIS appropriately track the activity of users when they assume someone else's identity or account and the logs show changes made by the actual user. However, the audit logs do not show the user whose identity or account has been assumed and they do not clearly differentiate what actions are completed under a user's assigned account rights versus what actions are taken under an assumed identity or account. This makes it difficult for management to evaluate how often users are using these features and whether they are using them to make changes or view information that they would otherwise not have access to through their own user account.

[12] Project manager, Superintendent's secretary, attendance secretary, guidance counselor, nurse, the Superintendent and two MORIC employees

[13] The Superintendent and nurse do not have access to the assume-account feature.

Report Monitoring – Audit logs or change reports[14] maintain a record of activity or show changes or deletions made in a computer application. District officials should review these reports to monitor for unusual activity. These reports provide a mechanism for individual accountability and for management to reconstruct events.

Although District officials are aware that audit logs are available in the SIS to review changes made by users, they do not monitor user activity in the SIS with these logs. Because we found that user access was not always assigned according to job duties, it is even more important that the District monitor user activities to ensure appropriate use. When audit logs or change reports are not generated and reviewed, management cannot be assured that unauthorized activities, such as grade changes or adjustments to user account access, are detected and adequately addressed.

Recommendations

1. District officials should review current procedures for assigning user access rights and strengthen controls to ensure that individuals are assigned only those access rights needed to perform their job duties. District officials should monitor user access rights periodically.

2. The Board should adopt written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts and monitoring user access.

3. District officials should evaluate the user permissions currently assigned to each user group, develop a process to verify that individual users' access needs are compatible with the rights of the assigned groups and update the permissions or groups as needed.

4. District officials should remove all generic or unknown accounts from the SIS.

5. District officials should restrict the ability to make grade changes in the SIS to designated individuals and ensure that documentation is retained to show who authorized the grade change and the reason for the change.

6. District officials should consider whether the assume-identity and assume-account features are appropriate for use. If they decide to use these features, they should work with the SIS vendor to determine if the audit log report format can be modified, or change reports produced, to clearly show user activity performed and all accounts involved when these features are used.

7. District officials should periodically review available audit logs for unusual or inappropriate activity.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the Education Law, and Section 170.12 of the

[14] Change reports track specific types of changes made to the system or data.

Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and forwarded to our office within 90 days. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

We thank the officials and staff of the District for the courtesies and cooperation extended to our auditors during this audit.

Sincerely,

Gabriel F. Deyo

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following pages.

Poland CENTRAL SCHOOL DISTRICT
Prepared, Productive, Proud
DISTRICT OFFICE 74 Cold Brook Street Poland, New York 13431 • Phone: (315) 826-7900 • Fax: (315) 826-7516

Laura Dutton
Superintendent of Schools
Ext. 203

Donna Wellington
District Clerk
Ext. 203

BUSINESS OFFICE
Chad Hess
Business Official
Ext. 204

Charlene Gross
District Treasurer
Ext. 205

MIDDLE/HIGH SCHOOL
Jason Mitchell
Principal
(315) 826-7900 Ext. 200
FAX: (315) 826-5227

ELEMENTARY SCHOOL
Christopher Clancy
Principal
(315) 826-7900 Ext. 201
FAX: (315) 826-3393

TRANSPORTATION
Jeff DeLucia
Director
(315) 826-7900 Ext. 226
FAX: (315) 826-3597

FOOD SERVICE
Deborah Newman
Director
(315) 826-7900 Ext. 216
FAX: (315) 826-0353

SPECIAL EDUCATION
Mary Doyle
CSE Chair
(315) 826-7900 Ext. 220
FAX: (315) 826-7942

GUIDANCE OFFICE
Janice Watrous
Director
(315) 826-7900 Ext. 214
FAX: (315) 826-7499

HEALTH OFFICE
Rosanne Ozog
Nurse
(315) 826-7900 Ext. 208
FAX: (315) 826-5509

WWW.POLANDCS.ORG

April 25, 2014

Rebecca Wilcox, Chief Examiner
333 East Washington Street
Syracuse, NY 13202

Dear Chief Examiner Wilcox,

RE: CORRECTIVE ACTION PLAN
Unit Name: Poland Central School District
Audit Report Title: Technology Audit of the Student Information System
Audit Report Number: P3-13-30

For each recommendation included in the audit report, the information below is intended to explain and identify corrective actions taken and proposed.

Recommendation
1. District officials should review current procedures for assigning user access rights and strengthen controls to ensure that individuals are assigned only those access rights needed to perform their job duties. District officials should monitor user access rights periodically.

Actions
The District has reviewed current procedures for assigning user access rights and has strengthened controls to ensure that individuals are assigned only to rights needed to perform job duties and functions. Duties regularly change for employees depending on instructional and support assignments. Therefore, additional assurances including improved documentation of initial access, documentation to support adjustments to access, and documentation when access should be discontinued due to retirement or resignation have been initiated. Additionally, the user rights to individuals and groups have been clarified with the MORIC and monitoring has initiated.

Recommendation
2. The Board should adopt written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts, and monitoring user access.

Actions
The Board of Education subscribes to the BOCES Policy Service as a primary support for ensuring Poland's policies and procedures for school governance

Poland CENTRAL SCHOOL DISTRICT
Prepared, Productive, Proud
DISTRICT OFFICE 74 Cold Brook Street Poland, New York 13431 • Phone: (315) 826-7900 • Fax: (315) 826-7516

Laura Dutton
Superintendent of Schools
Ext. 203

Donna Wellington
District Clerk
Ext. 203

BUSINESS OFFICE
Chad Hess
Business Official
Ext. 204

Charlene Gross
District Treasurer
Ext. 205

MIDDLE/HIGH SCHOOL
Jason Mitchell
Principal
(315) 826-7900 Ext. 200
FAX: (315) 826-5227

ELEMENTARY SCHOOL
Christopher Clancy
Principal
(315) 826-7900 Ext. 201
FAX: (315) 826-3393

TRANSPORTATION
Jeff DeLucia
Director
(315) 826-7900 Ext. 226
FAX: (315) 826-3597

FOOD SERVICE
Deborah Newman
Director
(315) 826-7900 Ext. 216
FAX: (315) 826-0353

SPECIAL EDUCATION
Mary Doyle
CSE Chair
(315) 826-7900 Ext. 220
FAX: (315) 826-7942

GUIDANCE OFFICE
Janice Watrous
Director
(315) 826-7900 Ext. 214
FAX: (315) 826-7499

HEALTH OFFICE
Rosanne Ozog
Nurse
(315) 826-7900 Ext. 208
FAX: (315) 826-5509

WWW.POLANDCS.ORG

effectively support and safeguard district operations. Audit findings have been shared with the Labor Relations Office and the MORIC. Suggestions for amendments to existing technology policies are anticipated from the BOCES Labor Relations Office and MORIC for best practice recommendations.

As received, the Board will review policy recommendations to identify appropriate changes. In the absence of these policies, local control already in place will create additional safeguards.

Recommendation

3. District officials should evaluate the user permissions currently assigned to each user group, develop a process to verify that individual users' access needs are compatible with the rights of the assigned groups, and update the permissions or groups as needed.

Actions

The District is working with the MORIC to identify the pathway of rights granted to each user group. As permissions are evaluated, eliminating the access to additional or unnecessary rights to any user will be remedied.

Recommendation

4. District officials should remove all generic or unknown accounts from the SIS.

Actions

The District has removed unknown accounts that had once been created for ease of functioning and off-campus support. Staff members who require SIS access have been given direct access specific to their needs.

Recommendation

5. District officials should restrict the ability to make grade changes in the SIS to designated individuals and ensure that documentation is retained to show who authorized the grade change and the reason for the change.

Actions

The District has identified key personnel who will be authorized to make grade changes through SIS and has restricted access to the grade change function. The district has initiated a paperwork trail for grade changes that requires the prior approval of three of the following: the building administrator, teacher, counselor, or superintendent. Written documentation specific to the need for the grade change will be maintained in the guidance office.

Poland CENTRAL SCHOOL DISTRICT
Prepared, Productive, Proud
DISTRICT OFFICE 74 Cold Brook Street Poland, New York 13431 • Phone: (315) 826-7900 • Fax: (315) 826-7516

Laura Dutton
Superintendent of Schools
Ext. 203

Donna Wellington
District Clerk
Ext. 203

BUSINESS OFFICE
Chad Hess
Business Official
Ext. 204

Charlene Gross
District Treasurer
Ext. 205

MIDDLE/HIGH SCHOOL
Jason Mitchell
Principal
(315) 826-7900 Ext. 200
FAX: (315) 826-5227

ELEMENTARY SCHOOL
Christopher Clancy
Principal
(315) 826-7900 Ext. 201
FAX: (315) 826-3393

TRANSPORTATION
Jeff DeLucia
Director
(315) 826-7900 Ext. 226
FAX: (315) 826-3597

FOOD SERVICE
Deborah Newman
Director
(315) 826-7900 Ext. 216
FAX: (315) 826-0353

SPECIAL EDUCATION
Mary Doyle
CSE Chair
(315) 826-7900 Ext. 220
FAX: (315) 826-7942

GUIDANCE OFFICE
Janice Watrous
Director
(315) 826-7900 Ext. 214
FAX: (315) 826-7499

HEALTH OFFICE
Rosanne Ozog
Nurse
(315) 826-7900 Ext. 208
FAX: (315) 826-5509

WWW.POLANDCS.ORG

Recommendation

6. District officials should consider whether the assume-identity and assume-account features are appropriate for use. If they decide to use these features, they should work with the SIS vendor to determine if the audit log report format can be modified, or change reports produced, to clearly show user activity performed and all accounts involved when these features are used.

Actions

The District has limited both the "assume" functions. The District is working with the SIS to determine if the audit log report can accurately capture user activity in the "assume" setting or if the full function of "assume" rights needs to be eliminated.

Recommendation

7. District officials should periodically review available audit logs for unusual and/or inappropriate activity.

Actions

The District will work with the MORIC to access and review audit logs to help identify unusual or inappropriate activity and increase checks and balances.

Conclusions

The full audit report has been shared with the Mohawk Regional Information Center to support the District in remedying any additional weaknesses and vulnerabilities. The information has also been shared with the Technology Director.

Best practices to limit weakness and vulnerabilities to SIS including regular review of practices for passwords, methods for log-in, and ongoing awareness and education for all Poland staff members and the District's Technology Coordinator that are responsive to the ever-changing needs and intricacies of technology will be supported.

Signed:

Laura Dutton, Superintendent — 4/25/14, Date

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

We reviewed access to the District's SIS for the period July 1, 2011 through April 30, 2013. We extended our scope period through October 7, 2013 to perform certain tests of the District's access controls.

To achieve our audit objective and obtain valid audit evidence, we performed the following audit procedures:

- We interviewed District officials and staff, as well as MORIC staff, to gain an understanding of the District's SIS application and authorized users, assignment and monitoring of user access rights to the SIS, and IT policies and procedures.

- We compared a list of current active employees to a list of current SIS staff users to determine if any users of the SIS are not District employees or if any former employees remain on the current user list. We obtained the most recent employee user list from the SIS and obtained an employee master list from the Payroll Department. We also compared a list of employees who left District employment during our audit period to the list of current SIS users to verify they were no longer active SIS users.

- We selected 29 users of the SIS to compare the users' job duties with user group assignment and individual user rights to determine if access rights are compatible with job duties. We obtained a master list of SIS users and randomly selected 10 percent of instructional and non-instructional staff users for a total of 14 users and judgmentally selected 15 users that we considered to have higher risk. Higher risk users included administrative users, users with add/modify permissions and users who can change closed-out grades.

- We interviewed 18 users to determine what their job duties are and observed them navigating the SIS screens to see and understand what access was available to them.

- We reviewed parent users' permissions to verify they have just view-only rights as a group using the group permissions file generated from the SIS.

- We reviewed the audit logs to determine whether the users identified as exceptions in our tests performed any function that is not part of their job duties or accessed the system after they left the District.

- We selected 10 grade changes that occurred during our audit period and determined whether these grade changes were authorized, documented and supported. We focused our testing on the high school for changes made to final grades in marking periods that had already been closed out.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.