DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-120

Grand Island Central School District

Network Access and Application User Permissions

NOVEMBER 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Grand Island Central School District

Audit Objective

Determine whether Grand Island Central School District (District) officials adequately secured access to the network and properly managed user permissions in financial and student information applications.

Key Findings

District officials did not adequately secure access to the network or properly manage user permissions in financial and student information applications.

In addition to finding sensitive information technology (IT) control weaknesses that were communicated confidentially to officals, we found that District officials did not:

- Disable 297 unnecessary service and network user accounts.
- Properly restrict user permissions in the financial and student information applications.

Key Recommendations

- Ensure that unnecessary service and network user accounts are disabled timely.
- Limit application user permissions based on a user's job responsibilities.

District officials agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The District serves the Town of Grand Island in Erie County. The Board of Education (Board) is responsible for managing and controlling the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The Director of Instructional Technology (Director) reports to the Superintendent and is responsible for managing the IT department. IT department staff are responsible for managing access to the network and user permissions in the student information application. The Assistant Superintendent for Business and Finance (Assistant Superintendent), her administrative assistant, and the Director have rights to set up user permissions in the financial application.

Quick Facts	
Student Enrollment	2,946
Full-Time Employees	488
Total	3,434
Network User Accounts	
Active and Reviewed	3,843
Application Accounts	
Student Information	508
Financial	74
Total Reviewed	582

Audit Period

July 1, 2020 – May 9, 2022

Network Access and Application User Permissions

How Should District Officials Adequately Secure Access to the Network and Properly Manage Application User Permissions?

Cybersecurity risks should be treated as any other hazard a school district may encounter. School district officials should identify the risks, reduce their vulnerabilities and plan for contingencies. This requires an investment of time and resources and a collaborative work environment among the superintendent, the board and the IT department.

Cybersecurity risks should be treated as any other hazard a school district may encounter.

Network user accounts enable networks, connected computers and certain applications to recognize specific users and accounts, allow network administrators to grant appropriate user permissions and provide user accountability by affiliating network user accounts with specific users and processes. Application user accounts provide access to resources within each application, such as a financial application or a student information application. These accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and view data stored on the network and/or within the application. To minimize the risk of unauthorized network and application access, school district officials should actively manage network and application user accounts and periodically conduct a user account review and any account that cannot be associated with an authorized user or current school district or system need should be disabled.

Service accounts are used solely to run a particular network or system service or application. Service accounts should be limited in use as they are not linked to individual users and therefore may have reduced accountability. For example, service accounts may be created and used for automated backup or testing processes, or generic email accounts such as a service help desk account. Officials should limit the use of service accounts and also routinely evaluate the need for the accounts and disable those that are not related to a current district or system need.

A shared account is an account with a username and password that is shared among two or more people. Because shared accounts are not assigned to a single user, officials may have difficulty limiting the access granted to these accounts and linking any suspicious activity to a specific individual. Some shared accounts may inadvertently grant users more access than needed. To help limit access and ensure individual accountability, all users should have and use their own user account to gain access to a network and application. If shared accounts are needed, officials should have procedures in place to monitor who uses the accounts and when and how they are used. This helps ensure accountability over work performed and data changed or deleted.

School district officials should set up network and application user accounts with only the specific user permissions needed by each individual to perform their job

functions, responsibilities and assignments. Properly assigned user permissions, based on the requirements of each individual, help to preserve an appropriate segregation of duties within the network and applications. School district officials should periodically review network access and user permissions in the financial and student information applications to ensure access and permissions are appropriate and properly limited based on each user's current roles and responsibilities.

School district officials should have written procedures in place to grant, change and disable user accounts and permissions to the network and applications. These procedures should establish who has the authority to grant or change user permissions and allow users to access only what is necessary to complete their job duties. The procedures should define when elevated permissions, such as administrative access, can be granted and under what circumstances these permissions should be revoked when not needed. User permissions should be updated as necessary and unneeded accounts should be disabled as soon as access is no longer needed.

Officials Did Not Adequately Secure Access to the Network

District officials did not actively manage network user accounts and did not have written procedures for granting, changing and revoking access rights to the network. We reviewed all 3,843 enabled network user accounts and found that 3,012 were assigned to students, 725 were assigned to non-students, 33 were service accounts and 73 were shared network user accounts.

Unnecessary Network User Accounts – We identified 77 non-student network user accounts that were assigned to individuals who previously worked for the District as an employee, a contractor or an intern. However, their accounts were not disabled. For example, one account for a school administrator who retired in July 2021 was not disabled. According to the Director and personnel clerks, the District had a process for granting and disabling users' network access. However, this process was not consistently implemented or followed. This process required that after the Board approved a personnel change, the personnel department would prepare a work order using an electronic work order system. The system would then submit the work order to the IT department to grant or disable network accounts. However, a work order was not generated to disable the network account for the administrator at the time of retirement. One of the personnel clerks told us it must have been overlooked at the time. In addition, the network accounts related to three former employees, whose resignation or retirement were approved at the same Board meeting as the school administrators, were also not disabled. According to the Director, no work order was generated by personnel department employees for these three former employees.

We identified 77 non-student network user accounts that were assigned to individuals who previously worked for the District. …

The Director also told us in the past IT department staff periodically reviewed accounts for non-activity and unnecessary accounts, but that they have not reviewed the enabled network accounts for the past two fiscal years (2019-20 and 2020-21) because of the COVID-19 pandemic and due to limited staffing in the IT department; as a result, many were not disabled. However, we reviewed these 77 former non-student network accounts' last login dates and found that nine had not logged in since before July 1, 2019 and 26 had never logged in. Therefore, these accounts could have been identified if the enabled network accounts had been reviewed. The remaining 42 users had left the District more recently and had logged in to their network accounts after July 1, 2019. All 77 accounts were disabled as a result of our audit inquiry.

We also identified 168 enabled student network user accounts that should have been disabled because they were not associated with currently enrolled students. According to the Director, since approximately 2018, the District had a process for granting and disabling students' network user accounts. However, this process was not consistently implemented or followed. The Director told us that when a student was no longer enrolled with the District, the student registration department was supposed to generate a work order which would then be submitted to the IT department staff to disable the student's network user account. We further analyzed the 168 student user accounts, and identified 54 user accounts that had never logged in and 63 user accounts that were not used to log in since prior to January 2018. We also reviewed the anticipated graduation date for these student users and none of these students graduated from the District and were no longer enrolled. All 168 student user accounts were disabled as a result of our audit inquiry.

Because the District's network had unnecessary enabled network user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to compromise IT resources. Although the District had a process for disabling user accounts, there were no procedures in place to ensure the process was followed. As a result, unnecessary user accounts went unnoticed. Had District officials implemented written procedures to disable network accounts and monitored compliance by periodically reviewing enabled user accounts, these accounts may have been detected and disabled in a timely manner.

Service Accounts – The District had 33 enabled service accounts. The service accounts were used for system functions and content filtering. After reviewing these accounts with the Director, we identified 11 service accounts which should have been disabled and were disabled as a result of our audit inquiry. We questioned why these service accounts were created and not disabled when they were no longer needed. The Director told us that service accounts are established

for many different reasons, and they were not disabled in a timely manner because the IT department has limited staff[1] when compared to the number of devices and users it is responsible for servicing. The IT department prioritized resolving issues for teachers and students and as a result, other tasks, such as disabling unnecessary accounts, have not been performed.

Of the 22 remaining service accounts, 10 of them had not been used to log in to the network in the six months prior to November 15, 2021.[2] According to the Director, service accounts were used by software to perform system functions and do not require a user to sign in for the function to run. The Director did not know what two service accounts were used for, but she told us that she plans to work with Erie 1 Board of Cooperative Educational Services (BOCES) staff to review all of the remaining service accounts. Specifically, she told us that the service accounts that have not been used in over six months would be reviewed to determine whether they were unneeded and would be disabled gradually while monitoring to ensure there are no system malfunctions. The Director indicated that the service accounts were created before she and the current IT staff were employed by the District. The Director started at the District in November 2013, and the network administrator started in August 2015. Although nine of the 33 service accounts were created before November 2013, the majority (24) were created after the Director started working at the District.

Because the District's network had enabled service accounts that were not needed, or for which the need was unknown, there is a greater risk that these accounts may be used as potential entry points for attackers to compromise IT resources.

Shared Accounts – The District had 73 shared accounts. After reviewing these accounts with the Director, we identified 22 shared accounts which should have been disabled and were disabled as a result of our audit inquiry. The Director told us these accounts were not disabled sooner due to the limited staff in the IT department. Of the 51 remaining shared accounts, nine accounts had not logged into the network in the six months prior to November 15, 2021. The 51 remaining shared accounts were used by substitute personnel, BOCES employees and other vendors for various purposes such as testing the IT systems. Passwords for most shared accounts were established by the Director or network administrator, who also provided that password to the users.

1 There were six full-time positions in the IT department including the Director, a secretary, an audio-visual technician, a microcomputer decision support specialist, a network administrator and two part-time BOCES employees who made up one full-time equivalent position.

2 We obtained information on network user accounts on November 15, 2021. See Appendix B for audit methodology detail.

The IT staff did not keep track of who used these shared network user accounts or how they were used. For example, 11 of the 51 shared accounts were used by substitute teachers and clerical staff. The District had one account for substitute teachers and one for substitute clerical staff at each of the District's five school buildings and one shared account for substitute clerical staff at the District office. The passwords for the substitute accounts were established by the Director or network administrator and provided to each building's main office staff, who provided the passwords to users.

Because employees were allowed to use shared accounts to log into the District network and their specific use was not tracked, it would be more difficult for officials to identify single users that may have performed unauthorized activities.

User Accounts with Administrative Network Access – During our review of the District's network, we found 33 network user accounts with administrative network access. After we discussed with the Director, we identified eight network user accounts which should not have administrative access, and eight additional network user accounts which should have been disabled, reducing the number of accounts with administrative network access from 33 to 17. IT department staff disabled and revoked administrative access for these network user accounts as a result of our audit inquiry.

Users with administrative network access can perform activities that include creating new network user accounts and manipulating the security settings configured on the network. These users also can perform activities that include installing software and viewing any personal, private or sensitive information on networked servers and user computers. If one of these network administrative user accounts is compromised, the attacker (or program developed by the attacker) could have the same permissions as the compromised account.

When we asked the reason that elevated network access was granted unnecessarily or not revoked when the access was no longer needed, the Director stated that most accounts with administrative network access were needed by certain systems that the District no longer uses. These accounts should have been disabled when the District no longer used the system that was using them, but it was overlooked. In addition, the District did not have written policies and procedures defining when administrative network access should be granted and revoked and under what circumstances.

When administrative network access is granted to accounts for users who do not need that level of access, the District has an increased risk that intentional or unintentional changes could damage IT resources.

The IT staff did not keep track of who used these shared network user accounts or how they were used.

Officials Did Not Properly Manage Application User Permissions

District officials did not properly manage user permissions for the student information application and the financial application.

Student Information Application – The student information application had 508 enabled user accounts. After we compared the enabled user account list with a current employee list and followed up with the Director, the Assistant Superintendent, the payroll clerk and human resources personnel, we determined that 20 individuals' user accounts should have been disabled since they were no longer employed by the District. According to the Director, the IT department was not informed these individuals' employment with the District had ended.

We reviewed user permissions for seven active employees[3] who had access to the student information application and found that four employees still had user permissions related to previous positions they held at the District. After we brought our findings to the Director, the Director revoked the unnecessary permissions for three of these employees but told us that the remaining employee needed the extra permissions to assist the employee who had replaced him approximately six months prior. Users' accounts should only have application access that is needed to perform their current job duties.

Financial Application – In the financial application, there were 74 enabled user accounts. We compared the enabled user accounts with the current employee list and followed up with the Assistant Superintendent and concluded that they were all active employees except one administrative account. Three employees had shared access to this one administrative account, which was used to grant and update user permissions following approval by the Superintendent. We questioned the practice of allowing three employees, including the Assistant Superintendent, to have access to this administrative account. Both the Assistant Superintendent and the Director agreed with our concern and stated they would eliminate the Assistant Superintendent's access to this account after the other two become more familiar with the process of granting user permissions within the application. However, since the Assistant Superintendent is involved in the business office functions, administrative financial application access is incompatible with her responsibilities because she approves financial transactions such as journal entries.

We reviewed all five Business Office employee accounts' user permissions in the financial application. We found unnecessary permissions were granted for all five accounts. We also reviewed an additional four employee accounts'[4] user permissions and found these user permissions were appropriate. The Assistant

3 See Appendix B for sampling methodology.

4 See Appendix B for sampling methodology.

Superintendent told us that user permissions are set up with BOCES' assistance using permission profiles and there is no way to assign specific permissions to individual employees' accounts. They were aware of this limitation and stated that some mitigating methods were put in place. For example, a report of new vendors was generated periodically and reviewed by another employee to mitigate the risk of fictitious vendors. They also stated that District officials will work with BOCES staff to update these profiles.

By not properly restricting user permissions and access rights within the student information and financial applications, there are increased opportunities for users to access and make unauthorized or improper changes, improperly access students' private and personal information and/or modify accounting records to conceal malicious transactions.

Because officials did not adequately secure access to the network and applications, the District has a greater risk that its network resources, financial data or student information could be changed intentionally or unintentionally or be used inappropriately.

District officials indicated the weaknesses identified in this report are, in part, the result of an insufficient amount of time and resources dedicated to cybersecurity. The reliance on technology, communication and interconnectivity has changed, and expanded the potential vulnerabilities and increased possible risk to operations. An appropriate investment should be made to evaluate the acceptable level of risk and facilitate the ongoing monitoring of that risk.

An appropriate investment should be made to evaluate the acceptable level of risk and facilitate the ongoing monitoring of that risk.

What Do We Recommend?

The Board and District officials should:

1. Develop and adopt a written user permissions policy and develop comprehensive written procedures detailing the process to add, modify and disable user permissions, including administrative access, to the network and applications.
2. Ensure users follow the written procedures once they are established and establish a process for monitoring compliance.
3. Ensure that unnecessary network user accounts are disabled as soon as they are no longer needed and periodically review user accounts for necessity and appropriateness.
4. Review the remaining service accounts and disable any unnecessary service accounts.
5. If shared network user accounts are needed, have procedures in place to monitor who uses the accounts and when and how they are used.

6. Limit student information and financial application user accounts' access rights and permissions based on a user's responsibilities and to properly segregate duties, and periodically review application access rights and permissions for necessity and appropriateness.

7. Ensure that application user accounts that are no longer needed are disabled.

8. Limit access to and use of the shared financial application administrative account to the Director or another designated employee who is not involved in the District's financial operations and consider using separate accounts for each individual user to maintain accountability.

Appendix A: Response From District Officials

Grand Island Central School District
1100 Ransom Road • Grand Island, New York 14072
Telephone (716) 773-8800 • Fax (716) 773-8843
www.grandislandschools.org

Office of State Comptroller Audit Response
November 2, 2022

Office of State Comptroller Audit Report Title:
School District Website
Report of Examination
Period Covered: July 1, 2020 – May 9, 2022

Office of State Comptroller Audit Report Number:
2022M-120

The Grand Island Central School District is in receipt of the draft *Network Access and Application User Permissions* (Report of Examination) issued by your office for the period of July 1, 2020 – May 9, 2022. The District would like to thank the Comptroller staff for their professionalism and courtesy in conducting their duties associated with this audit.

The Grand Island Central School District Board of Education and Administration take its fiduciary responsibilities seriously. We are committed to ensuring that our professional procedures are administered responsibly and in the student's best interest and the community with accuracy and transparency.

1. **Audit Recommendation:**
   Develop and adopt a written user permissions policy and develop comprehensive written procedures detailing the process to add, modify and disable user permissions, including administrative access, to the network and applications.

   District Response: The Data Networks and Security Access Policy (#5674) is currently being reviewed by our Policy Committee and will go to a full BOE vote soon. That policy expresses the need to grant, change and terminate user access rights based on the necessity of employee job duties.

   The District currently has processes to add, modify and disable user permissions. These will be written down in detailed procedures and shared with appropriate personnel. These procedures will be reviewed annually to ensure they keep up with new applications, permissions, and structures.

2. **Audit Recommendation:**
   Ensure users follow the written procedures once they are established and establish a process for monitoring compliance.

District Response: Personnel involved with the user permissions procedures will meet annually to review the procedures and update them where necessary. This will allow all parties involved to understand the procedures and updates. The District Data Protection Officer will periodically review account rights in various applications for individual users to ensure procedures are followed.

3. **Audit Recommendation:**
   Ensure that unnecessary network user accounts are disabled as soon as they are no longer needed and periodically review user accounts for necessity and appropriateness.

   District Response: The IT department disabled accounts during the process of the audit that were found to be no longer used. The IT department will annually review accounts for usage and appropriate rights. Procedures when creating substitute accounts will be changed to include expiration dates for Active Directory (network) accounts.

4. **Audit Recommendation:**
   Review the remaining service accounts and disable any unnecessary service accounts.

   District Response: The IT department reviewed the remaining service accounts and disabled unnecessary ones.

5. **Audit Recommendation:**
   If shared network user accounts are needed, have procedures in place to monitor who uses the accounts and when and how they are used.

   District Response: A procedure will be implemented whereby substitute teacher and substitute clerical accounts will be tracked in the school buildings where these accounts are distributed to those personnel.

6. **Audit Recommendation:**
   Limit student information and financial application user accounts' access rights and permissions based on a user's responsibilities and to properly segregate duties, and periodically review application access rights and permissions for necessity and appropriateness.

   District Response: Reports will be pulled from the student information service periodically to review rights for users. Procedures will be implemented to facilitate the flow of information from Personnel to IT regarding staff role changes. For the financial application, business office staff access rights and permissions have already been changed to allow for the segregation of duties properly. This will be periodically reviewed for necessity and appropriateness.

7. **Audit Recommendation:**
Ensure that application user accounts that are no longer needed are disabled.

District Response: Reports will be pulled from the student information service periodically to review the length of time since the last log-in. Procedures when creating substitute accounts will be changed to include expiration dates for IC accounts. Procedures will be implemented to facilitate the flow of information from Personnel to IT regarding staff who leave the district.

8. **Audit Recommendation:**
Limit access to and use of the shared financial application administrative account to the Director or another designated employee who is not involved in the District's financial operations and consider using separate accounts for each individual user to maintain accountability.

District Response:
The District will work to identify an employee who will manage the system's administrative account for the financial application. This will be someone who does not have a current user account/role in the financial system to allow for proper segregation of duties.

Signed: [redacted] Date: 11/2/22
Dr. Brian Graham
[redacted]

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve our audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed District officials and employees and reviewed Board policies, regulations and meeting minutes to gain an understanding of the District's policies, procedures, network and application related IT controls.
- We provided a computerized audit script to the Director to run on the domain controller on November 15, 2021. We analyzed each report generated by the script to identify enabled network user accounts and permissions.
- We compared the District's current student enrollment list and employee master list to the enabled network user accounts identified by the audit script to determine whether active network account users were either enrolled students or District employees.
- We examined reports of user accounts and user permissions generated by the student information application on November 15, 2021 and determined which permissions were granted. We used our professional judgment to select a sample of seven users' accounts that may be more high risk, including those for business and personnel office employees as well as other employees who we would not expect to have access to student information. We examined the user permissions for these seven employees' accounts to determine whether access to the student information application was appropriate based on their job duties.
- We examined reports of user accounts and user permissions from the financial application received on November 30, 2021, and determined which permissions were granted. We used our professional judgment to select a sample of nine users' accounts. We selected accounts for users that may be more high risk, including business office employees as well as other employees who we would not expect to have access to the financial application. We examined the user permissions to determine whether access to the financial application was appropriate based on their job duties.

Our audit also examined the adequacy of certain sensitive IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. 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 CAP should be posted on the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

BUFFALO REGIONAL OFFICE – Melissa A. Myers, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller