New York State Comptroller
THOMAS P. DiNAPOLI

Amherst Central School District

Network User Account Access and Application User Accounts and Permissions

2023M-5 | June 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Amherst Central School District

Audit Objective

Determine whether Amherst Central School District (District) officials secured user account access to the network and managed user accounts and permissions in financial and student information applications.

Key Findings

District officials did not adequately secure user account access to the network or properly manage user accounts and permissions in financial and student information applications. As a result, there is a significant risk that network resources, financial data and student information could be inappropriately altered, accessed, or used. In addition to sensitive control weaknesses that were communicated confidentially, officials did not disable unnecessary:

- Network user accounts or revoke unnecessary network user account access.
  - As many as 1,570 accounts were unneeded but were not disabled.
  - Four accounts had unnecessary network administrative access.
- Application user accounts or properly restrict permissions in the financial and student information applications.

Key Recommendations

- Ensure that unnecessary network user accounts are disabled in a timely manner.
- Limit application permissions based on an account user's job responsibilities.

District officials agreed with our findings and indicated they plan to initiate corrective action.

Background

The District serves the Towns of Amherst and Cheektowaga 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 the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The Chief Information Officer (CIO) and Senior Network Manager, both reported to the Assistant Superintendent of Curriculum, Instruction and Technology (Assistant Superintendent), and are responsible for setting up user account access to the network and user accounts and permissions in the student information and financial applications.

Quick Facts	
Student Enrollment	2,983
Active Employees	554
Total	3,537
Network User Accounts	
Enabled and Reviewed	5,078
Application User Accounts	
Student Information	5,374
Financial	75
Total Reviewed	5,449

Audit Period

July 1, 2020 – July 7, 2022

Network User Account Access and Application User Accounts and Permissions

How Should School District Officials Adequately Secure User Account Access to the Network?

Cybersecurity risks including inadequately secured network user account access and improperly managed application user accounts and permissions 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 school district superintendent, the school board and the information technology (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 account 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 which includes sensitive payroll information (e.g., employee Social Security numbers) or a student information application which includes students' confidential personal information (e.g., dates of birth and grades). Both network and application user 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. 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, such as a generic email account or a help desk account. 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 fulfill their required job duties. To help limit access and ensure individual accountability, all users should have and use their own user account to access a network and/or an 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 who is responsible for the work performed and data changed or deleted.

Officials Did Not Adequately Secure User Account Access to the Network

District officials did not actively manage network user accounts and did not have written procedures for granting, changing and disabling user account access to the network. We reviewed all 5,078 enabled network user accounts and found that 2,902 were assigned to current enrolled students, 1,402 were assigned to students that were not currently enrolled, 575 were assigned to current nonstudents (e.g., employees, contractors, interns), 90 were assigned to former nonstudents, 27 were service accounts and 82 were shared network user accounts.

Unnecessary Network User Accounts – We identified 90 nonstudent network user accounts that were for individuals who previously worked for the District. However, their accounts were not disabled and should have been. For example, user accounts for three teacher aides who each left the District between 2012 and 2016, and a user account for a teacher who retired from the District more than 20 years ago were not disabled. We shared this information with the Senior Network Manager and he told us that he would disable employee network accounts that are not logged into for at least 90 days. We later determined that 71 of the 90 accounts were disabled but 19 were not. We asked the Senior Network Manager why these accounts were not disabled but he did not reply to our inquiry. Former employee network accounts should be disabled on the day the employee leaves District employment.

We identified 90 nonstudent network user accounts that were for individuals who previously worked for the District. However, their accounts were not disabled. ...

We also identified 4,304 student network user accounts. We compared the list of student network accounts to a list of currently enrolled students and identified 1,426 accounts that did not match the enrolled student list. According to the CIO, these accounts were likely for individuals who were registered but never attended the District or attended and subsequently left the District. The CIO and his assistant reviewed all 1,426 student accounts and found that 1,402 student accounts should have been disabled because the account users were no longer students enrolled at the District. When we followed up with the CIO, the Senior Network Manager, and their supervisor, the Assistant Superintendent, we found all but 35 were disabled as a result of our audit inquiry. The CIO stated that going forward, the District would disable any student accounts not used to log into the network for more than nine months. However, unneeded accounts should be disabled as soon as the accounts are not needed.

Service Accounts – The District had 27 enabled service network user accounts, generally used for system functions and web content filtering. After reviewing these accounts with the Senior Network Manager, we identified six unnecessary service accounts which should have been disabled and were disabled as a result of our audit inquiry.

Shared Accounts – The District also had 82 enabled shared network user accounts, including 72 accounts that should have been disabled because they were no longer needed. Of the shared accounts that should have been disabled, 26 were for access to computers in the school library and six accounts were used to test the network. The 26 library accounts were created in July 2004 and September 2011 and were last used to log into the network in 2020. According to the Senior Network Manager, those library computers had since been disposed. The six test accounts were used by IT staff to perform some system tests and should have been disabled after testing was done in 2020 and 2021. The remaining accounts were established for various purposes but were no longer needed. As a result of our audit inquiry, all 72 unneeded shared accounts were disabled.

Of the 10 shared network user accounts that were needed, four accounts were set up for a specific employee group at four District schools. Each of the employees from this specific group shared one account at each school. According to the Senior Network Manager, the IT Department changes passwords on these four accounts monthly. While we verified that the passwords for these four accounts were periodically changed, the District did not monitor or record who used the accounts and when or how they were used. Because these employees shared network user accounts without tracking, it could be more difficult for officials to identify single users that may have performed unauthorized activities.

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. We discussed these issues with the CIO, the Senior Network Manager and the Assistant Superintendent. They each agreed that the unnecessary user accounts went unnoticed because the District did not have written policies and procedures to disable network accounts and District officials were not regularly reviewing enabled user accounts to ensure they were still necessary and appropriate. 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.

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.

Network User Accounts with Administrative Access – During our review of the District's network user accounts, we found 15 network user accounts with

administrative access. After discussions with the Senior Network Manager, we determined that three of these network user accounts should not have had administrative access, and one network user account should have been disabled,[1] reducing the number of accounts with necessary administrative access from 15 to 11. We subsequently followed up with the Senior Network Manager and verified that the one account was disabled, and administrative access for three accounts was revoked, as a result of our audit inquiry.

Network user accounts with administrative access can be used to perform activities that include creating new network user accounts and manipulating the security settings configured on the network. These user accounts also can be used to 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 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 CIO, the Senior Network Manager, who started with the District in December 2021, and the Assistant Superintendent told us that the District did not have written policies and procedures defining when administrative access to the network should be granted and revoked and under what circumstances.

When administrative access is granted to network user accounts for users who do not need that level of access to perform their assigned job duties and responsibilities, the District has an increased risk that intentional or unintentional changes could damage network resources. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt network access.

… [T]he District did not have written policies and procedures defining when administrative access to the network should be granted and revoked and under what circumstances.

How Should School District Officials Properly Manage Application User Accounts and Permissions?

School district officials should set up network and application user accounts with only the specific permissions needed by each individual to perform their job functions, responsibilities and assignments. Properly assigned user account permissions, based on the requirements of each individual, help to preserve an appropriate segregation of incompatible duties within the network and applications. School district officials should periodically review network access and user account permissions in the financial and student information applications to ensure network access and application account permissions are appropriate

1 This account is included in 78 service and shared unnecessary accounts addressed above.

and properly limited based on each user's current and assigned roles and responsibilities. School district officials should also periodically review audit logs, which record changes made in the administration of the financial management system, and also records any events where previously recorded (original) data is modified or system parameters are changed, even if temporarily. Audit logs can be an important detection control for possible manipulation of the financial data or other sensitive information.

School district officials should have written procedures in place for granting, changing and disabling user accounts and permissions to the network and applications. These procedures should establish who has the authority to grant or change user account access and permissions and help ensure users are granted access to 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 and these permissions should be revoked when not needed. User account access and permissions should be updated in a timely manner to help ensure they remain consistent with a user's assigned job duties and responsibilities and unneeded accounts should be disabled as soon as access is no longer needed.

Officials Did Not Properly Manage Application User Accounts and Permissions

The District did not properly manage user accounts and permissions for the student information application or the financial application.

Student Information Application – The student information application had 5,374 enabled application user accounts including 3,076 parent accounts, 1,768 student accounts, 516 employee accounts, six accounts classified as both parent and staff accounts, and eight accounts that were not classified within the application as parent, student or employee accounts. After we compared the 522 enabled employee user accounts with a current employee list and followed up with the CIO and Human Resources personnel, we determined that 101 employee user accounts should have been disabled because the individuals associated with these accounts were no longer employed by the District, dating back as far as 2014. We also compared the 1,768 enabled student user accounts to the District's current student enrollment list and determined that 330 student user accounts should have been disabled because the accounts' users were no longer students enrolled at the District. According to the CIO, there were no written policies and procedures to guide the review of student information application user accounts and correlating permissions and District officials were not regularly reviewing them.

> …[W]e determined that 101 employee user accounts should have been disabled because the individuals associated with these accounts were no longer employed by the District, dating back as far as 2014.

2 Including 14 employee users and one of eight users that were not classified as parent, student or employee users.

We reviewed all 15 student information application user accounts[2] that had the "system administrator" role assigned to them which can be used to add, delete and modify user account permissions, including their own, within the application. Because this functionality can be misused or lead to inadvertent errors, these elevated access rights should be assigned to a limited number of employees, who are assigned the responsibility to administer the application.

According to the CIO, the majority of these 15 student information application user accounts should have been assigned the role of "school administrator" instead of system administrator. System administrators would generally be expected to have more extensive access rights than that of school administrators. While a school administrator might need access rights to modify the accounts of certain students and/or District employees assigned to their department or building, they would not need administrative rights or the ability to modify the access rights of all students or District users.

In addition, there were no written policies to prohibit misuse of student information application user accounts assigned the system administrator role to add, delete or modify user account permissions without authorization. In other words, these 15 user accounts had unmitigated access to modify and grant student information application user account permissions for any user account in the application.

We reviewed user permissions for an additional 22 student information application user accounts.[3] Fifteen were assigned to current employees and the permissions granted were appropriate for these employees to fulfill their responsibilities. However, of the remaining seven user accounts, five should have been disabled. According to the CIO, these accounts were used for testing the student information application. These accounts should have been disabled after testing was done and enabled again when needed. The remaining two accounts were set up and used by the CIO – one for the District registration application to interface with the student information application, and the other to test the interface between the special education and student information application.

Financial Application – The District had 75 enabled financial application user accounts including those for 50 District users, seven Board of Cooperative Educational Services (BOCES) users and 18 application company users. We compared the 50 enabled District user accounts with the current employee list and concluded that the accounts all belonged to active employees.

We further reviewed the seven BOCES and 18 application company user accounts and determined one had never been used to log into the application, four were not used to login for more than 10 years, one was not used in over five

3 Including accounts for 15 employees in different positions and seven user accounts that were not classified within the application as parent, student or employee.

years and 13 had not been used for more than one year. Only six accounts were used to log into the application within the past year. When we questioned what permissions these user accounts had within the financial application, the CIO did not know but followed up with BOCES and determined that these 25 user accounts were set up as "'super users' with access to everything" in the financial application. According to the CIO, the 18 application company user accounts were created by and belong to the application company and these accounts have been there since the District started to use the application. The BOCES user accounts were created by BOCES. According to the CIO, the District had no knowledge of these accounts, no control of their associated permissions and could not delete or modify these accounts. Because these accounts allow third-party users to log into the District's financial application, these accounts could be used to make unauthorized changes to District financial data without being detected by District officials.

We reviewed user account permissions for 14 District users based on their job duties, including all five Business Office employees, all five Employee Services Department employees, two head custodial employees, the Assistant to the Superintendent and the CIO/Deputy Treasurer. We found that three of these employees had application permissions that allowed them to grant and update other user accounts' permissions after a financial application user account was created by a BOCES user. When we asked the Business Administrator and CIO why these three employees had such access, they stated that these three employees' accounts had this access to perform each other's job duties when one or two were off on the same day. However, as a result, two of these three employees had financial application user account permissions which were incompatible with their assigned responsibilities.

An employee involved with functions including processing financial transactions should not have administrative access. Administrative access could potentially allow these users to grant other users permissions incompatible with their job responsibilities including the ability to process financial transactions they are not authorized to perform. We verified through physical observation, that these three users could not change their own financial application user account permissions.

Of the 14 enabled financial application user accounts we reviewed, we found unnecessary and/or incompatible permissions were granted for 11 of 14 users' accounts. For example, six individuals, including two head custodians, could view employees' social security numbers but did not need that information to fulfill their assigned job responsibilities. In addition, seven individuals were granted permissions that were not compatible with other permissions granted because the combination of the permissions granted provide an individual the ability to manipulate transactions. For example, seven individuals had permissions allowing them to print and reprint accounts payable checks, six had permissions to print

and reprint payroll checks, two had permissions to change pay rates and process payroll, and one could enter and approve their own purchase orders.

These financial application user account permission issues were the same issues identified during the District's 2020 internal audit. When we asked what corrective action was taken as a result of the 2020 internal audit, the Assistant Superintendent and the CIO told us that they were not aware of the issues raised in that audit. The Business Administrator told us that she implemented some changes as a result of the 2020 internal audit but could not explain what changes were made or provide evidence of the changes made.

The Business Administrator told us this may have happened because the application allowed an existing user account's permissions to be copied and pasted when granting permissions to a new user account and some permissions may have been given to employees who serve as the backup person for individuals who regularly perform such duties.

By not properly restricting user account permissions 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 user account access to the network and properly manage application user accounts and permissions, there is a significant risk that the District's network resources, financial data and student information could be intentionally or unintentionally changed or be used inappropriately.

These financial application user account permission issues were the same issues identified during the District's 2020 internal audit.

What Do We Recommend?

The Board and District officials should:

1. Develop and adopt a written user account and permissions policy and develop comprehensive written procedures detailing the process to add, modify and disable user accounts and permissions, including those granting administrative access, to the network and applications.

2. Ensure District users follow the written procedures once they are established and implement a process for monitoring compliance with the procedures.

3. Ensure that unnecessary network user accounts are disabled as soon as they are no longer needed and periodically review all enabled network user accounts, including service and shared accounts, for necessity and appropriateness.

4. Monitor application company user and BOCES ‘super user’ accounts by periodically reviewing audit logs detailing the activity of these users and require District approval for all such accounts and their associated application permissions.

5. Have procedures in place for necessary shared user accounts to monitor who uses the accounts and when and how they are used.

6. Limit student information and financial application user accounts’ permissions, including those granting system administrative access, based on an account user’s responsibilities and to properly segregate incompatible duties, and periodically review application permissions for necessity and appropriateness.

7. Ensure that unnecessary application user accounts, including any for non-District users, are disabled as soon as they are no longer needed.

8. Limit elevated financial application permissions to the CIO or another designated employee who is not involved in the District’s financial operations.

9. Ensure issues identified as a result of District internal audits are investigated and rectified timely.

Appendix A: Response From District Officials

Amherst Central School District

Anthony J. Panella
Superintendent

Lynn Shanahan, Ph.D.
Assistant Superintendent
Curriculum, Instruction & Technology

Michael Belle-Isle
Assistant Superintendent
Student & Staff Services

April 27, 2023

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

Re: Appendix A - Response from District Officials
Unit Name: Amherst Central School District
Audit Report Title: Network User Account Access and Application User Accounts and Permissions
Audit Report Number: 2023M-5

Dear Deputy Comptroller Auerbach,

Please accept this letter as Amherst Central School District's official response to the above referenced comptroller's audit which began in March 2022. We appreciate your service and we believe your findings and recommendations are valid. Cybersecurity is an area our district continuously works to strengthen and we welcomed the in-depth look from the comptroller's office. As noted in the audit, we had already put corrective actions into place during the course of the audit process. The district is committed to putting corrective actions into place for any findings listed in the final report.

The Amherst Central School District will continue ongoing evaluation and enhancements of our cybersecurity programs to maintain the confidentiality, integrity and availability of all student, staff and financial data within the district.

Sincerely,

[redacted]

Anthony J. Panella
Superintendent of Schools

55 Kings Highway, Amherst, NY 14226-4330 ◆ Phone: 716-362-3000 ◆ Fax: 716-836-2537 ◆ www.amherstschools.org

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, practices and internal controls related to securing user account access to the network and managing user accounts and permissions in the financial and student information applications.
- We provided a computerized audit script to the Senior Network Manager to run on the domain controller on April 11, 2022. We analyzed each report generated by the script to identify enabled network user accounts and granted administrative access.
- 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 enabled network accounts were for either enrolled students or District employees.
- We examined the list of user accounts generated by the CIO from the student information application on March 25, 2022 and the list of user permissions on April 5, 2022. We used our professional judgment to select a sample of 37 application users' accounts that may be more high risk, including those users with accounts assigned the system administrator role within the application as well as other employees who we would not expect to need access to student information. We examined the permissions granted to the 37 application users' accounts to determine whether permissions within the student information application were appropriate based on their assigned job duties.
- We obtained a report of District financial application users' accounts and permissions received from the CIO on April 5, 2022 and a report of all financial application user accounts generated by BOCES on April 22, 2022 that included all users with access to the District's financial application. We used our professional judgment to select a sample of 39 application users' accounts. We selected accounts for users 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 need access to financial information. We examined the permissions granted to the 39 application users' accounts to determine whether permissions within the financial application were appropriate based on their assigned job duties.

Our audit also examined the adequacy of certain sensitive network user account access 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 of Municipal Audits

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