New York State Comptroller
THOMAS P. DiNAPOLI

North Tonawanda City School District

Information Technology

2023M-102 | November 2023

Division of Local Government and School Accountability

Contents

Report Highlights

North Tonawanda Central School District

Audit Objective

Determine whether North Tonawanda City School District (District) officials properly secured user account access to the network and managed user account permissions in financial and student information applications.

Key Findings

District officials properly managed user account permissions in the financial application but did not properly secure user account access to the network or manage user account permissions in the student information application. As a result, there is a significant risk that network resources and student information could be inappropriately altered, accessed or used. In addition to sensitive information technology (IT) control weaknesses that were communicated confidentially to officials, we found that District officials did not:

- Disable 246 unnecessary network user accounts.
- Properly manage permissions for 517 user accounts in the student information application by ensuring accounts were locked or disabled when an employee separated from the District.
- Educate users on data privacy and security awareness.
- Develop an IT contingency plan and as a result, District officials lacked preparedness for a cyberattack.

Key Recommendations

- Ensure that unnecessary network user accounts are disabled as soon as they are no longer needed.
- Ensure user accounts in the student information application are locked or disabled when the employee separates from the District.

District officials agreed with our recommendations and indicated that they have initiated or plan to initiate corrective action.

Background

The District serves the City of North Tonawanda in Niagara County. The Board of Education (Board) is responsible for managing the District's financial and educational affairs; the Superintendent of Schools (Superintendent) is responsible for the District's day-to-day management.

The Computer Network Administrator (Administrator) reports to the Executive Director of Educational Services (Director) and is responsible for managing the IT department. The Administrator and IT department are responsible for setting up network user account access. The Chief Information Officer (CIO), who is the appointed Director of Data Security, also reports to the Director and is responsible for managing the District's financial and student information applications' user account permissions.

The Erie 1 Board of Cooperative Educational Services (BOCES) maintains the District's network servers and implements security policies for network user accounts as directed by the Administrator.

Quick Facts	
Student Enrollment	3,368
District Employees	573
Enabled and Reviewed Network User Accounts	
Student	3,405
Nonstudent	888
Shared, Service and BOCES	114
Total	4,407

Audit Period

July 1, 2022 – April 12, 2023

What Is Properly Secured Network User Account Access and Management of Application User Account Permissions?

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 Board, Superintendent and IT department.

Network user accounts are created for various purposes, including allowing access to shared resources and facilitating system functions. Application user accounts provide access to resources within a specific application, such as a financial application or student information application. All network and application users should have and use their own user accounts to gain access to a network and application. If users share accounts or account users cannot be identified, accountability could be diminished and activity in the system may not be able to be traced back to a single user.

To minimize the risk of unauthorized access to school districts' network and applications, officials should actively manage network and application user accounts and periodically conduct a review of user account permissions and network user accounts. Unneeded user accounts should be disabled and unnecessary permissions should be revoked as soon as they are deemed unneeded.

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 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 routinely evaluate the need for the accounts and disable those that are not related to a current school district or system need.

A shared user account has a username and password that is shared among two or more users, 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 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 to monitor who uses the accounts and

Cybersecurity risks, including inadequately secured network user account access… should be treated as any other hazard a school district may encounter.

when and how they are used. This helps ensure who is responsible for the work performed and data that is changed or deleted.

Well-informed users are essential to securing the data and IT systems accessible through network user accounts and application user account permissions. School districts cannot protect the confidentiality, integrity and availability of data and systems without ensuring that users understand IT security policies and procedures and are provided with the knowledge and skills to help secure network user account access and manage application user account permissions. School districts are required to provide data privacy and security awareness training to their officers and employees with access to student, teacher or principal personally identifiable information as required by New York State Education Department regulations. Studies show that human error accounts for a significant share of all cybersecurity breaches. Therefore, school districts should develop a comprehensive IT contingency plan that provides detailed guidance for continuing operations as normal as possible during and after a major, unplanned incident such as a network user account security compromise or a student data breach resulting from the misuse of an application user account's permissions.

…214 network user accounts were unnecessary and should have been disabled. …

Officials Did Not Properly Secure Network User Account Access

District officials did not properly secure network user accounts because they did not adequately communicate expectations by having written policies and procedures for granting, changing and disabling user account access to the network. We reviewed all 4,407 enabled network user accounts, including 3,405 student accounts, 888 nonstudent accounts, 75 shared accounts, 23 service accounts and 16 BOCES accounts.

Unnecessary Student and Nonstudent Network User Accounts – We determined that 214 network user accounts were unnecessary and should have been disabled, including 159 student accounts for users who previously attended the District and 55 nonstudent accounts that were assigned to individuals who previously worked for the District as an employee, a contractor or an intern. For example, officials did not disable one user account assigned to a substitute teacher who left the District in 2019.

The Administrator told us that network user accounts were created and disabled automatically. Network user accounts for staff were created after a new employee's information was entered into the financial application by a human resources clerk. Student network user accounts were created once enrollment information was added to the student information system by a clerk in the student registration office. In both cases, the network management system would automatically process a data file overnight from each application and create a user account for the student or employee. Employee network user accounts were automatically disabled 30 days after a final payroll date was selected by a human

resources clerk and student accounts were disabled based on graduation dates. For the example above, since the employee was a substitute teacher, the last pay she received was not selected as a final payroll date since the human resources clerk was not aware at the time.

The Administrator relied on supervisors from contracted agencies[1] to provide employment status updates regarding contractors every summer in order to manually modify or disable individual network user account access as necessary. The Administrator informed us she was not notified about status updates for these contracted employees; therefore, their accounts remained enabled on the network. The Administrator also said she manually created and disabled intern network user accounts because they were not on the District's payroll; therefore, these accounts were not disabled timely because she was not informed when they left the District.

As a result of our audit inquiries, all 159 unnecessary student network user accounts and 55 nonstudent network user accounts were disabled. While the Administrator told us that IT officials did not regularly review network user accounts for unnecessary accounts, had regular reviews of network user accounts been performed, IT officials would likely have identified and disabled these accounts timely.

Service Accounts – The District had 23 enabled service network user accounts, generally used for system functions and content filtering. We determined that three service accounts were unnecessary and should have been disabled and the Administrator disabled them as a result of our audit inquiry.

We asked why these service accounts were created and not disabled when they were no longer necessary. The Administrator told us that service accounts are established for different reasons, and they were not disabled timely because the IT department does not regularly review them to confirm they are needed. The Administrator said that because there has not been a cybersecurity attack on service accounts, the unnecessary accounts were left unnoticed. However, waiting for an indication of a network service account compromise does not negate the risk that these accounts remained on the network as additional entry points that attackers could leverage now or in the future.

BOCES Accounts – The District had 16 enabled BOCES network user accounts that were all necessary; six user accounts were used by BOCES personnel and assigned administrative permissions to provide technical support for the District and 10 user accounts were used by BOCES personnel to manage certain District third-party applications.

1 The District used contracted agencies for services such as occupational therapy, universal pre-kindergarten and nursing. Contracted agencies' employees needed user account access to the District's network to provide these services to students.

Shared Accounts – While the District's network users generally have and use their own network user accounts, the District had 75 enabled shared network user accounts. We determined that 29 shared accounts were unnecessary and should have been disabled. The Administrator disabled these accounts as a result of our audit inquiry. The Administrator also removed unnecessary administrative permissions from one of the remaining enabled shared accounts after our discussion. The Administrator told us that shared accounts are created for various reasons (e.g., shared library and cafeteria network access) and most of them have limited network access, such as an additional email account for a department or access to the District's website. However, IT department staff did not keep track of who used shared network user accounts or how they were used. Shared accounts provide entry points to the District's network and because it is difficult to trace shared accounts to a single user, it is difficult to detect when a shared account has been compromised.

Unnecessary network user accounts provide additional entry points, when compromised, for attackers to gain unauthorized access to the District's network and any accessible data therein. Shared accounts also put the District's network at an increased risk because their use is more difficult to trace to a single network user. The District had no written policies or procedures to disable network accounts and the Administrator did not ensure network accounts were disabled as soon as they were no longer needed. IT officials did not regularly review enabled network user accounts to ensure they were necessary and appropriate, which caused the unnecessary network user accounts to go unnoticed. The Administrator told us that because there had not been a cyberattack or data leak in the District for the more than 20 years she had been in this position, it was not necessary to develop written policies and procedures to add, modify and disable network user accounts. However, cybersecurity risk management should be elevated as a top priority because school district systems have increasingly been breached, with data deleted, misused or held for ransom. Furthermore, certain cyberattacks may go undetected for lengthy periods of time.

Kindergarten through grade 12 (K-12) schools have reported significant educational impacts due to cybersecurity incidents, such as ransomware attacks. Cyberattacks can cause monetary losses for targeted schools due to the downtime and resources needed to recover from incidents. Officials from State and local entities reported that the loss of learning following a cyberattack ranged from three days to three weeks, and the recovery time ranged from two to nine months. While the precise national magnitude of cyberattacks on K-12 schools is unknown, the United States Government Accountability Office (GAO) has reported the number of students affected by ransomware attacks was over 2.6 million between 2018 and 2021. In addition, according to data from the Multi-State Information Sharing and Analysis Center (MS-ISAC), reported ransomware incidents against K-12 schools increased significantly in August and September

Cyberattacks can cause monetary losses for targeted schools due to the downtime and resources needed to recover from incidents.

2020. Fifty-seven percent of all ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28 percent of reported ransomware incidents around the end of the 2019-20 school year.

Had District officials communicated their expectations, implemented written procedures to disable network user accounts and periodically reviewed enabled user accounts, these accounts may have been disabled in a timely manner, helping to reduce the risk of a network data breach, misuse or loss.

Officials Did Not Properly Manage Application User Account Permissions

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

Student Information Application – The District had 565 enabled student information application user accounts, including 517 unique user accounts and 48 user accounts that, while associated with unique user accounts, provided those account users access to the application from additional school buildings. We determined that the 48 associated application user accounts were not used and 37 unique user accounts were locked within the application to prevent the user from logging in because they were associated with individuals who had separated from the District. However, we determined that one of these unique application user accounts was for a former employee who resigned in November 2022 but had a last login date in February 2023. While this account had minimal permissions within the application, the account was not locked immediately after this employee resigned. The CIO was unaware that this account was not locked timely. In addition, we determined that one enabled test account with administrative permissions was never used to log in to the application and was unneeded. The CIO locked the test account as a result of our audit inquiry.

The CIO and Director told us that the CIO typically locked an account once he was verbally notified that an employee separated from the District. The CIO would lock rather than disable unnecessary application user accounts because disabling an account would cause certain application data associated with that account to be disabled. At the end of each summer before school started, the CIO generally disabled any account locked within the application. However, we discovered that 10 of the 37 locked accounts were assigned to employees who separated from the District after July 1, 2022. Additionally, we determined that 24 of the 37 locked accounts had not been accessed since July 1, 2022 and three of these accounts were never accessed; these 27 locked accounts were unneeded and should have been disabled.

Financial Application – We identified 43 enabled user accounts in the District's financial application and determined that all accounts were for active employees

and had the necessary user account permissions needed to fulfil their assigned job duties. While the District's financial application user account permissions were properly assigned, the CIO told us that they have not developed procedures to actively manage and review user account permissions in the financial application because user account permissions generally do not change.

Clearly establishing expectations and having written policies and procedures in place to guide officials to manage and periodically review user account permissions in student information and financial applications can help minimize risks of unauthorized access as a result of not disabling unnecessary user accounts or permissions to the application in a timely manner.

Officials Did Not Educate Users on Data Privacy and Security Awareness or Implement an IT Contingency Plan

The position of several District officials, including the Administrator, Director and CIO, was that they were providing sufficient resources to protect the District from potential data breaches and private, personal, and sensitive information (PPSI)[2] leaks by requiring employees to electronically sign an acceptable use policy acknowledgment form each year. However, the form did not have sufficient information to provide users with the knowledge and skills to help secure network user account access. The form also did not educate users on how to help mitigate the risk of cybersecurity breaches which could allow unauthorized user account access to the District's network or applications, and therefore did not fulfill the data privacy and security awareness training requirement.

Furthermore, the Administrator indicated that District officials did not implement an IT contingency plan to describe how IT personnel and officers should continue normal operations and recover lost data in the event of an unexpected IT incident because the District has not previously experienced a major, unplanned incident such as a network user account security compromise or student data breach.

Although the Administrator stated that they conducted daily incremental backups, full backups of the District's network weekly and quarterly, and BOCES managed the District's application backup systems, they did not have a plan to define when and how backup restoration and other contingency-related procedures should be followed to sustain critical business functions during and after a disruption. Without an IT contingency plan, District officials lacked preparedness for a cyberattack such as addressing how employees would communicate, where they would go and how they would continue to do their jobs during a disruption.

Without an IT contingency plan, District officials lacked preparedness for a cyberattack such as addressing how employees would… continue to do their jobs during a disruption.

2 PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

What Do We Recommend?

The Board and District officials should:

1. Develop and adopt a written user account and permissions policy and comprehensive written procedures detailing the process to grant, change and disable user accounts and permissions to the network and applications.

2. Develop data privacy and security training plans and implement training for data privacy and security awareness annually for District network or application users, in addition to the current acceptable use agreement required to be signed annually.

3. Develop and adopt a comprehensive written IT contingency plan including detailed guidance for continuing operations during and after a major, unplanned incident and ensure it is distributed to all responsible parties.

The Administrator should:

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

The Director and CIO should:

5. Ensure all network user accounts and permissions in the student information and financial applications are locked and/or disabled timely when an employee or student separates from the District or when the user no longer needs the access they were granted.

Appendix A: Response From District Officials

NORTH TONAWANDA CITY SCHOOL DISTRICT
176 Walck Rd. ♦ North Tonawanda, New York 14120-4097 ♦ (716) 807-3500 ♦ FAX (716) 807-3525

Gregory J. Woytila
Superintendent of Schools

October 24, 2023

Office of the State Comptroller - Buffalo Regional Office
Division of Local Government and School Accountability
295 Main Street, Suite 1032
Buffalo, New York 14203-2510

Unit Name: North Tonawanda City Schools

Audit Report Title: Information Technology

Audit Report Number: 2023M-102

To Whom It May Concern,

This correspondence is being submitted in response to the preliminary draft findings of the recently completed examination of the North Tonawanda City School District's (the District's) technology audit for the period of July 1, 2022 – April 12, 2023.

The North Tonawanda City School District partners with Erie1 BOCES to provide Managed Information Technology Services. Using Erie1 BOCES allows for additional security and oversite of technology. While this technology support also provides the ability to apply "best practices" the audit also highlights areas of potential risk that the District must address that are not covered in the partnership with Erie1 BOCES. It should be noted that most of the issues that were identified during the audit were addressed immediately. These enhancements will be part of the corrective action plan drafted in response to the findings.

We appreciate the comprehensive approach taken by the audit team and will implement safeguards to minimize risks related to the Network User Accounts and Information Technology Contingency Planning as a result.

Sincerely,

Gregory J. Woytila
Superintendent of NTCSD

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 the 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, and network and application user account related IT controls, including IT contingency planning and training.
- We provided a computerized audit script to the Director to run on the domain controller on January 31, 2023. We analyzed each report generated by the script to identify enabled network user accounts and permissions.
- We compared the District's employee master list, generated on January 31, 2023, to the enabled network user accounts identified by the audit script to determine whether user accounts were only for active employees.
- We compared student information application user account and permissions reports to the employee master list and to resignation and termination reports, generated on January 31, 2023, to determine whether enabled student information application user accounts were only for active employees.
- We compared financial application user accounts and permissions reports, generated on December 15, 2022, to the employee master list to determine whether enabled financial application user accounts were District employees who needed financial application user permissions.

Our audit also examined the adequacy of certain information technology 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.

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