

Arlington Central School District

Network User Accounts

OCTOBER 2021



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

Contents

- Report Highlights 1**

- Information Technology 2**
 - How Should Officials Ensure Network User Accounts
Are Necessary? 2

 - District Officials Did Not Adequately Manage and Secure
Network User Accounts 2

 - What Do We Recommend? 3

- Appendix A – Responses From District Officials 4**

- Appendix B – Audit Methodology and Standards 5**

- Appendix C – Resources and Services 6**

Report Highlights

Arlington Central School District

Audit Objective

Determine whether Arlington Central School District (District) officials ensured network user accounts were adequately configured and secured.

Key Findings

District officials did not ensure network user accounts were adequately configured and secured. In addition to sensitive information technology (IT) control weaknesses which we communicated confidentially to officials, we found District officials should have:

- Disabled 150 of the 9,989 network user accounts we examined. The 150 accounts include 116 generic accounts, 27 employee accounts, five contractor accounts, one former employee account and one account the IT Director could not identify to whom it belonged. These accounts have been unnecessarily active ranging from August 2007 to January 2020.
- Developed methods to determine who is using each shared user account at a given time.

Key Recommendations

- Regularly review enabled user accounts and ensure that unneeded user accounts are immediately disabled.
- Restrict the use of shared network user accounts and develop procedures to monitor the use of these accounts.

District officials agreed with our recommendations.

Background

The District serves the Towns of LaGrange, Pleasant Valley, Beekman, Union Vale, Poughkeepsie, East Fishkill, Hyde Park, Wappinger and Pawling in Dutchess County.

The District is governed by an elected nine-member Board of Education (Board) 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 managing day-to-day operations under the Board's direction.

The Director of Innovative Technology (IT Director) is responsible for monitoring network user accounts.

Quick Facts

Student Network Accounts	7,813
Non-Student Network Accounts	2,176
Employees	2,055
Students	7,990

Audit Period

July 1, 2019 – January 11, 2021

Information Technology

The District's IT system and data are valuable resources. The District relies on its IT assets for Internet access, email and maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI).¹ If the IT system is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

How Should Officials Ensure Network User Accounts Are Necessary?

Network user accounts provide access to network resources and should be actively managed and secured to minimize the risk of misuse. If not properly managed and secured, user accounts could be potential entry points for attackers to inappropriately access and view PPSI on the network. In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network user accounts to ensure they are still needed. Officials should disable unnecessary accounts as soon as there is no longer a need for them.

Generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service helpdesk account. Officials should routinely evaluate generic network user accounts and disable those that are not related to a system need. Further, when multiple users are allowed to share network user accounts, a district has an increased risk that PPSI could be intentionally or unintentionally changed and/or compromised by unauthorized individuals. Furthermore, accountability is diminished and activity in the system may not be able to be traced back to a specific user. Therefore, use of these accounts should be restricted. When shared accounts are necessary, officials should develop methods to determine who is using the account at a given time. Officials should routinely evaluate and disable any generic accounts that are not related to a specific system need.

District Officials Did Not Adequately Manage and Secure Network User Accounts

District officials did not adequately manage and secure network user accounts for the District's network. We reviewed all 9,989 network user accounts and identified 603 network user accounts that have not been used in more than six months. We

If not properly managed and secured, user accounts could be potential entry points for attackers to inappropriately access and view PPSI on the network.

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

reviewed all of these network user accounts comprised of 580 non-student and 23 student accounts and discussed these accounts with the IT Director to determine if the accounts were still needed. Based on this discussion, we identified 150 accounts (25 percent) that were not needed. This included 116 generic accounts, 27 employee accounts, five contractor accounts, one former employee account and one account that the IT Director could not identify to whom it belonged. These accounts have been unnecessarily active ranging from August 2007 to January 2020. District officials stated that they did not prioritize eliminating user accounts during the pandemic. However, they are in the process of purchasing and implementing software to help with this and other functions. Although we understand that the IT Director started in August 2020 during the pandemic and had to address multiple concerns, the increase in people telecommuting along with the hybrid learning environment put the IT system at greater risk of an individual gaining unauthorized access.

In addition, we discussed all 531 generic accounts with the IT director to determine if they were shared accounts and found that 258 accounts (49 percent) were shared accounts, meaning they are used by more than one individual. Therefore, officials could have difficulty managing these accounts and removing or disabling those no longer needed because it may not always be clear exactly who uses these accounts and whether the access is needed. We then followed-up to determine if officials had a way to track who was using these accounts at a given time. District officials informed us that they do not have a method for determining who is using the account at a given time. These accounts were set up by the previous IT Director, who did not implement a method for tracking who is using them.

If not properly managed and secured, network user accounts are potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network. In addition, because shared accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user.

What Do We Recommend?

District officials should:

1. Regularly review enabled user accounts and ensure that unneeded user accounts are immediately disabled.
2. Restrict the use of shared network user accounts and develop procedures to monitor the use of these accounts.

Appendix A: Response From District Officials



ARLINGTON CENTRAL SCHOOL DISTRICT

Dr. David Moyer, Superintendent of Schools

144 Todd Hill Road • LaGrangeville, NY 12540
Phone 845-486-4460 • Fax 845-350-4087

October 4, 2021



Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

The Arlington Central School District agrees with the Public Facing Report of Examination's key findings and recommendations.

Sincerely,

Dr. Dave Moyer
Superintendent of Schools

Our mission is to empower all students to be self-directed, lifelong learners, who willingly contribute to their community and lead passionate, purposeful lives.

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 reviewed the District's IT policies and procedures and interviewed the IT Director to gain an understanding of the District's network user accounts and determine the adequacy of the policies and procedures.
- We ran a computerized audit script to examine the District's domain controller. We then analyzed each report generated by the script, looking for weaknesses in user account management and network setting configurations.
- We followed-up with District officials on potentially unneeded accounts, shared accounts and automated settings that indicated ineffective controls.

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.

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 to 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

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Sullivan, Ulster,
Westchester counties



Like us on Facebook at facebook.com/nyscomptroller

Follow us on Twitter [@nyscomptroller](https://twitter.com/nyscomptroller)