REPORT OF EXAMINATION | 2022M-26

Valhalla Union Free School District

Network User Accounts

JUNE 2022

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

Contents

Report Highlights

Valhalla Union Free School District

Audit Objective

Determine whether Valhalla Union Free School District (District) officials adequately managed network user accounts in order to help prevent unauthorized use, access and/or loss.

Key Findings

District officials did not adequately manage the District's network user accounts to help prevent unauthorized use, access and/or loss. In addition to sensitive information technology (IT) control weaknesses which we communicated confidentially to officials, we found District officials should have:

- Disabled 67 unneeded network user accounts. These unnecessary accounts had last log-on dates ranging from January 3, 2012, to September 3, 2021, and account for 15 percent of the District's network user accounts.
- Ensured District procedures were followed to communicate network user account changes to the IT vendor.

Leaving unneeded network user accounts enabled on the network increases the risk of unauthorized access.

Key Recommendations

- Disable unnecessary network user accounts as soon as they are no longer needed and maintain a list of authorized network users to periodically review network user accounts for necessity.
- Review the written procedures the District has in place for the process to communicate employee change in status to the IT vendor to ensure access to the District network is up-to-date.

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

Background

The District is located in the Towns of Greenburgh, Mount Pleasant and North Castle, in Westchester County. The District is governed by an elected seven-member Board of Education (Board).

The Superintendent is appointed by the Board and is the chief executive officer responsible for the District's day-to-day management, under the Board's direction.

The District contracts with an IT vendor through a service level agreement (SLA) to operate and maintain the District's IT system.

Quick Facts

Network User Accounts	
Generic	122
Non-Student	326
Total (Reviewed)	448
Unneeded and should have been disabled	67
2020-21 Payment to IT vendor	$491,532

Audit Period

July 1, 2019 – August 17, 2021. We extended our audit period forward to September 30, 2021, to complete IT testing.

Network User Accounts

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

Officials should ensure unnecessary network user accounts are disabled as soon as they are no longer needed.

How Should Officials Manage Network User Accounts?

Network user accounts provide access to a district's network resources and should be actively managed to minimize the risk of misuse. If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access the network and view PPSI on the network. In addition, officials must regularly review enabled network user accounts to ensure they are still needed and to minimize the risk of unauthorized access, officials should ensure unnecessary network user accounts are disabled as soon as they are no longer needed. Officials should ensure all IT policies are adhered to. For example, the District established written procedures in which the IT vendor must be notified to disable an employee's network user account when an employee leaves the District, therefore, officials must confirm the notification and subsequent disabling of the network accounts occurs.

Generic user 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 and disable any generic accounts that are not related to a specific district or system need. When numerous generic user accounts are enabled on a network, officials could have difficulty managing the accounts, including granting access specific to users' job duties, and disabling those no longer necessary. This is because it may not always be clear exactly who uses the accounts and whether the access is still needed. If not properly managed, user accounts could be potential entry points for attackers because they could be used 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.

Officials Did Not Adequately Manage Network User Accounts

Officials did not adequately manage the District's network user accounts, which increases the risk of unauthorized access, use and/or loss. The District does not maintain and review a current list of authorized users and their network access levels. Further, unnecessary network user accounts were not disabled by the District. Although the District has a process to communicate changes to employee status, District officials did not always provide a written directive to the IT vendor, per the District's process, to disable user accounts that are no longer needed. As a result, former employees had active accounts within the District's network.

Unneeded Network User Accounts – We reviewed all 326 enabled non-student network user accounts and found 21 unnecessary network user accounts that were for former employees or third-party contractors who no longer worked at the District. These unnecessary accounts had last log-on dates ranging from January 3, 2012, to September 3, 2021. In addition, we reviewed all 122 enabled generic network user accounts and found another 46 unneeded network user accounts that had never been used and should have been disabled. For example, some of these unneeded user accounts were created in 2012 and never used.

Although the District has a process to communicate changes in employee status to the IT vendor, District officials did not always follow the written process in place and failed to notify the IT vendor to disable network user accounts when employees left the District or when third-party contractor services were no longer needed. District officials indicated that the process was not being followed due to significant employee turnover within key District positions. Current District officials indicated that they were not following the written procedures in place because they were focusing their resources on the return from remote learning back to in-person instruction. Due to limited resources, they were unable to prioritize the written procedures over getting the work accomplished. However, our analysis was performed several months after the District had returned to in-person learning. In addition, four of the unnecessary network user accounts were attributed to employees who had left the District several years prior to the remote-learning migration. As a result, former employees, and third-party contractors, who no longer provided services to the District had enabled accounts within the network and unnecessary network user accounts were not disabled by the District.

After we notified District officials of these unnecessary network user accounts, officials indicated they were working with the IT vendor to identify and disable all unnecessary network user accounts. We verified that the IT vendor disabled the 67 unneeded network user accounts by observing the updated network user accounts after we brought them to their attention.

Leaving unneeded network user accounts enabled on the network increases the risk of unauthorized access because any account on a network is a potential entry point for attackers. There is an increased risk that intentional or unintentional changes could occur without detection or that these accounts could be used as entry points to access PPSI and compromise IT resources. Of particular risk are network user accounts for former employees and third-party contractors, as these could potentially be used by those individuals or others for malicious activities.

Leaving unneeded network user accounts enabled on the network increases the risk of unauthorized access. …

What Do We Recommend?

District officials should:

1. Notify the IT vendor to disable network user accounts of former employees and other users as soon as they are no longer needed and maintain a list of authorized network users that can be used to periodically review network user accounts for necessity.
2. Review the District's written procedures in place for the process to communicate employee change in status to the IT vendor to ensure access to the District's network is up-to-date and communicate the procedures to all staff responsible for employee status changes.

Appendix A: Response From District Officials

VALHALLA
UNION FREE SCHOOL DISTRICT
316 Columbus Avenue
Valhalla, New York 10595
(914) 683-5040 fax (914) 683-5075

Mr. Kevin McLeod
Superintendent of Schools

Mrs. Miriam Dobbs
School Business Official

May 19, 2022

Ms. Dara Disko-McCagg
Chief Examiner of Local Government and
School Accountability
Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103,
New Windsor, New York 12553

Dear Ms. Disko-McCagg:

The Valhalla Union Free School District is in receipt of the DRAFT Audit Report, Information Technology for the period of July 1, 2019 – September 30, 2021. On behalf of the Valhalla UFSD, we would like to thank your team for their professionalism and courtesy during our audit. It was a thorough and extensive process requiring detailed information and documentation. The examiners were always professional and respectful of our staff and the daily work that needed to be completed to keep school running.

The first priority of the Valhalla UFSD is to ensure the consistency and integrity of our educational programs for students while safeguarding our community's resources. We take our fiduciary responsibility to this district and community very seriously and we appreciate the opportunity to continually improve our policies and procedures.

At the time of the audit our IT vendor was in the process of addressing some of the issues identified in the audit. Furthermore, findings were resolved once brought to the districts' attention. Your feedback is helpful to us as we continue the ongoing process of making sure that our IT systems meet the highest standards for performance and security. Although we do not dispute the findings of the report, we do think it's important to understand the effects of COVID-19 and the necessary pivot to a remote learning environment. The district will utilize the recommendations from the report to further strengthen our IT environment.

In closing, I want to once again thank you for the professionalism of your staff and the opportunity to have clear and specific guidance on what the District needs to address.

Sincerely,

Mr. Kevin McLeod
Superintendent of Schools

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, employees and the on-site IT vendor and reviewed IT policies and procedures to gain an understanding of the District's network user account management and to determine the adequacy of internal controls over network user accounts.
- We reviewed the District's SLA with the IT vendor to gain an understanding of the services provided.
- On September 30, 2021, we ran a computerized audit script on the District's domain controller, which is the server used to help manage network user accounts and network resource access. We analyzed the data produced to assess network user accounts, permissions assigned to the accounts and the related security settings applied to the accounts.
- We compared all 326 enabled non-student network user accounts to the active employee list to identify accounts for former employees and/or other unneeded accounts. We identified enabled non-student network user accounts which were not on the District's master listing. We reviewed all those identified network user accounts based on last log-in and user permissions and asked the District officials whether the network user accounts were needed and to provide reasons for the needed network user accounts.
- We reviewed all 122 generic network user accounts and asked the District officials whether each generic network user account was needed and to provide reasons for the needed network user accounts.
- We reviewed network user access rights for the District's network to determine whether network user accounts were needed and if access was properly assigned based on users' job duties and responsibilities.

Our audit also examined the adequacy of certain 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

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, 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: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

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