New York State Comptroller
THOMAS P. DiNAPOLI

Kiryas Joel Village Union Free School District

Network User Account and Shared Network Folder Access

2023M-64 | September 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Kiryas Joel Village Union Free School District

Audit Objective

Determine whether Kiryas Joel Village Union Free School District (District) officials secured user account access to the network and shared network folders to help safeguard personal, private and sensitive information (PPSI).

Key Findings

District officials did not adequately secure user account access to the network and shared network folders to help safeguard PPSI. As a result, there is an increased risk of unauthorized access to the network and PPSI stored on shared network folders. In addition to sensitive information technology (IT) weaknesses communicated confidentially to officials, we found that officials did not:

- Disable 35 unnecessary former employee, shared and service network user accounts which account for 11 percent of the District's enabled accounts. The majority of these accounts belonged to former employees and were last used to log into the network between June 2015 and August 2022.
- Adequately secure shared network folder access, resulting in users having unnecessary access to multiple forms of PPSI in eight shared folders.
- Maintain a data inventory to properly protect IT resources, including data containing PPSI.

Key Recommendations

- Develop procedures to disable network user accounts when no longer needed and periodically check all network user accounts for necessity.
- Conduct a comprehensive data inventory and limit access to shared network folders based on assigned job duties and responsibilities.

District officials generally agreed with our recommendations and indicated they planned to initiate corrective action. Appendix B includes our comment on an issue raised in the District's response.

Background

The District serves the Town of Palm Tree, which is coterminous with the Village of Kiryas Joel, in Orange County. The District is governed by a five-person Board of Education (Board) responsible for managing and controlling the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) is the 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 District has a Service Level Agreement (SLA) with an IT vendor to manage the District's day-to-day IT operations. The IT vendor reports directly to the Superintendent.

Quick Facts	
Total Shared Network Folders	1,812
Enabled Network User Accounts	331
Estimated Annual IT Vendor Contract Amount	$209,000

Audit Period

July 1, 2021 – October 26, 2022

Network User Account and Shared Network Folder Access

A school district relies on its IT assets for maintaining financial, student and personnel records, much of which contain PPSI and are accessed through network user accounts, shared network folders, email and Internet access. 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. If network user account or shared network folder access is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate and repair. While effective controls, such as adequately secured network user account and shared network folder access, will not guarantee the safety of PPSI accessibility and its storage on the network, a lack of effective controls significantly increases the risk of unauthorized use, access and loss of PPSI.

How Should Officials Secure User Account Access to the Network and Shared Network Folders?

School district officials should adequately manage network user accounts as an IT control to help ensure that the accounts and access to shared network folders are necessary. Network user accounts provide access to network resources such as shared folders and should be actively managed to minimize the risk of misuse. If not properly managed, unnecessary network user accounts may not be detected and disabled timely. Unnecessary accounts are additional entry points for attackers to potentially access and attempt to view, modify and/or delete PPSI stored on the network. Therefore, a school district should have comprehensive procedures for granting, changing and disabling access rights to the network.

School district officials should promptly disable unnecessary accounts when they are no longer needed, including user accounts of former employees or employees who have transferred to another area within the District and no longer need access. The District's policy required an annual review of a list of network access rights and that dormant user accounts be removed every 12 months.

If a school district is using a third-party vendor to help manage their network, a well written SLA is a control that can help officials avoid issues securing network user account and shared network folder access to help safeguard PPSI. For example, if district officials contract with an IT vendor to secure network user account access, the SLA should indicate that the IT vendor is responsible for promptly disabling network user accounts upon an employee's separation within a specified timeframe. This should lead to a mutual understanding of the nature and required level of services to be provided.

Shared and service network user accounts should be limited in use, as they may not be explicitly authorized, monitored or used by one individual; therefore, these accounts may have reduced accountability if officials do not ensure they

are granted permissions appropriately, disabled timely and used properly. Shared user accounts have a username and password that are shared among two or more users and are used, for example, to provide access to guests or other temporary or intermittent users (e.g., contracted vendors). Service user accounts are created for the sole purpose of running a particular network or system service or application (e.g., automated backup systems). School district officials should routinely evaluate the need for these accounts and disable those that are not related to a current district or system need. If shared and service accounts are needed, officials should have procedures in place to monitor when and how the accounts are used. This helps ensure accountability over permissions granted, account use and evaluation.

School district officials should develop written policies and procedures for storing, classifying access to and disposing of PPSI stored in shared network folders. The policy should define PPSI; explain the district's reasons for collecting PPSI; and describe specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities. Users should only be given access to PPSI that is necessary to perform their job duties and responsibilities. Additionally, officials should maintain an inventory that classifies the data stored in shared network folders according to its sensitivity and identifies where the data is stored.

Shared network folders are hosted on a computer and shared on the network for one or more users to access. These folders may be accessed using mapped network drives (e.g., M: or H: drives) or their standard paths (i.e., universal naming convention). Network user account access to shared network folders should be secured to help safeguard any PPSI contained therein. To accomplish this, shared network folders should be set up with appropriate permissions to restrict network user accounts from accessing information or documents that they should not have access to. Network account access to shared folders should be assigned based on assigned job duties and responsibilities if the folders are used to store PPSI. Users should not be given network account access to resources outside their assigned job responsibilities. For example, employees should not be given access to confidential information if they are not required to have it as part of their assigned job duties.

Officials Did Not Adequately Secure User Account Access to the Network

District officials and the IT vendor did not adequately secure user account access to the network because they did not disable accounts when they became unnecessary or perform periodic reviews of all enabled District network user accounts to identify unnecessary accounts. We reviewed all 331 network user accounts and identified 35 network user accounts that were unnecessary. Specifically:

- 22 network user accounts were for former employees that had last network log on dates ranging between June 20, 2015 and August 4, 2022.
- 13 shared and service accounts no longer served a District purpose. These shared and service accounts included a template account used to add pre-school teachers with similar access needs to the network, test accounts used by the IT department and service accounts for hardware. The IT vendor confirmed that these accounts were no longer needed.

Although District policy required a review every 12 months of all network user accounts to identify which accounts are dormant, it did not indicate who was responsible for performing the review or define what is considered a dormant account. Additionally, the SLA with the IT vendor identified roles and tasks for each party; however, the SLA does not explicitly state who is responsible for adding and disabling network user accounts. Currently, school principals and supervisors email the IT vendor requesting that accounts be enabled or disabled. However, we found that the process did not operate effectively because former employee accounts were still enabled on the network.

The IT vendor stated that some of the unnecessary network accounts were subsequently disabled as a result of our audit inquiry. We ran a subsequent script on the District's primary point of network authentication to review 13 of the 35 unnecessary accounts to determine whether they were disabled. We found that the IT vendor did not disable 10 of the 13 accounts reviewed. The IT vendor restricted the access rights for two of the 10 remaining unnecessary network user accounts because the two accounts belonged to former employees, and he said that restricting access effectively mitigated the risks associated with an unnecessary account remaining enabled on the network. However, disabling the network accounts would help ensure there is a minimal risk of unauthorized access to the account and PPSI accessible by those accounts. For the remaining eight unnecessary network user accounts, the IT Director indicated that he intended to review and disable them, however had not done so prior to our subsequent script.

Leaving former employee and unneeded shared and service 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. Enabled network user accounts of former employees are of particular risk because they could potentially be used by those individuals or others for malicious activities without timely detection. Because some of these unneeded network user accounts had access to PPSI such as student data, an attacker able to compromise one of those accounts could leverage the accessible student data for personal gain (e.g., selling student data or identity theft) if they were to gain unauthorized access to the network. Furthermore, former employees would have familiarity with the location of PPSI stored on the District's network and could utilize their

enabled network user account to access and potentially exploit sensitive financial, employee and/or student information for malicious intent or personal gain.

Officials Did Not Adequately Secure User Account Access to Shared Network Folders

District officials used shared network folders to store and share information and documents that included PPSI. However, we found that District officials did not adequately secure user account access to the shared network folders to help ensure that users only had access to information required to complete their assigned job duties and responsibilities. Specifically, we found that 120 network user accounts within their respective network domains had unnecessary access to 10 of the 12 shared folders reviewed,[1] including eight folders that stored multiple forms of PPSI.

District policy required that all personal data be treated as confidential information and all storage mediums be classified to the highest level of information they may contain. However, the policy did not require or include guidance on maintaining a data inventory or classification scheme. As a result, District officials did not maintain a data inventory. District officials cannot properly protect their IT resources, including data containing PPSI, if they do not know what data they have and where such data resides within shared network folders. The failure to limit user account access and maintain detailed, up-to-date data inventory records exposes PPSI to an increased risk of loss, theft or misuse.

What Do We Recommend?

The Superintendent and officials should:

1. Work with the IT vendor to develop procedures to disable network user accounts of employees immediately upon leaving the District and periodically check all network user accounts for necessity.

2. Work with the IT vendor to conduct a comprehensive data inventory that classifies the data stored in shared network folders according to sensitivity, identifies where the data resides on the network and limits user account access to shared network folders based on assigned job duties and responsibilities.

1 Refer to Appendix C for details regarding our testing methodology.

The Board should:

3. Develop policies and procedures that explicitly state the responsibilities of the District and IT vendor in the management of network user accounts.
4. Periodically examine the SLA with the IT vendor to ensure it meets the needs of the District and IT environment.
5. Revise the IT policy to define PPSI; explain the District's reasons for collecting PPSI; and describe specific procedures for the classification, use, access to, storage, inventory and disposal of PPSI involved in normal business activities.

Appendix A: Response From District Officials

KIRYAS JOEL UNION FREE SCHOOL DISTRICT

48 Bakertown Road, Suite 401 Monroe, NY 10950 • (845) 782-2300 / Fax (845) 782-4176

JOEL PETLIN
Superintendent of Schools

HARRY POLATSEK
Board President

August 22, 2023

Dara Disko-McCagg, Chief of Municipal Audits
Newburgh Regional Office of the NY State Comptroller
33 Airport Center Drive, Suite 102
New Windsor, NY 12553

Re: Audit 2023 M-64

Dear Ms. Disko-McCagg

The Kiryas Joel Union Free School District is in receipt of the draft Report of Examination for the audit period of July 1, 2021 - October 26, 2022, focusing on Network User Accounts and Shared Network Folder Access.

At the outset, let me extend my thanks to your staff for their professionalism exhibited throughout the audit process. They were thorough during their risk assessment sampling review of transportation, fixed assets, tax collection, cash receipts, payroll, sick time, medical buy-outs, purchasing, claims, financial condition, board governance and information technology. In the focus area of this audit, we are pleased to confirm that your auditors found no evidence of fraud or malfeasance.

See Note 1 Page 8

We acknowledge the findings and recommendations noted in your report, and we view them as an opportunity to make improvements in our systems. In fact, we have already begun to implement some of the recommendations made in your report, and we intend to address all of the issues in our forthcoming corrective action plan.

We appreciate all of your efforts in conducting this audit and we thank you for giving us that opportunity to demonstrate our commitment to quality, compliance and transparency in the business operations of the Kiryas Joel School District.

Respectfully,

Joel Petlin
Superintendent

Cc: Board of Education
Business Office Personnel
IT Department

Appendix B: OSC Comment on the District's Response

Note 1

The audit focused on the security of network user accounts and while we conducted a limited review of some aspects of the District's operations during the risk assessment phase of our work, a broad conclusion regarding fraud or malfeasance cannot be drawn.

Appendix C: 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 policy and procedures and interviewed the Superintendent, Treasurer and IT vendor to gain an understanding of the IT environment and internal controls over network user account and shared network folder access.
- We ran a computerized audit script on the District's network on September 1, 2022 and on September 8, 2022 to identify all enabled network user accounts. We compared all 331 enabled network user accounts to the active employee list to identify unused and other possibly unneeded accounts and followed up with the IT vendor, Superintendent, and Treasurer to determine whether the accounts were needed or should have been disabled.
- We ran an additional computerized audit script on the District's primary point of network authentication on October 26, 2022. We analyzed the previously found unnecessary accounts to determine whether they were disabled by District officials.
- We ran a computerized audit script on three District network servers on September 28, 2022 to identify all network folders shared from the servers. Using our professional judgment, we selected 12 folders whose names indicated they might contain PPSI and were accessible by all network user accounts within the respective network domain. We reviewed the contents of each folder to identify any PPSI and determined whether the users with access to these folders needed this access to perform their job duties and responsibilities.

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

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix D: 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 of Municipal Audits

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