DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-113

Nyack Union Free School District

Network User Accounts

JANUARY 2022

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

Contents

Report Highlights

Nyack Union Free School District

Audit Objective

Determine whether Nyack Union Free School District (District) officials adequately managed and monitored network user accounts.

Key Findings

District officials did not ensure that network user accounts were adequately managed and monitored. Officials did not:

- Monitor compliance with the District's computer acceptable use policy.
- Maintain a current authorized user list.

Sensitive information technology (IT) control weaknesses were communicated confidentially in a separate letter to officials.

Key Recommendations

- Monitor compliance with the computer acceptable use policy.
- Develop written procedures for managing system access that include periodically reviewing user access and disabling unnecessary network user accounts.

District officials agreed with our recommendations and indicated they will take and have taken corrective action.

Background

The District is located in the Towns of Clarkstown and Orangetown in Rockland County.

The District is governed by the Board of Education (Board) which comprises seven elected Board members. The Board is responsible for the general supervision of the District through setting policies and expectations.

The Superintendent of Schools is appointed by the Board and is responsible for day-to-day management.

The Director of Technology & Innovation (Director) is responsible for all IT functions and manages all IT infrastructure.

Quick Facts

Network User Accounts Reviewed	
Staff	464
Non-Employee	254
Generic	171
Total	889

Audit Period

July 1, 2018 – December 1, 2020

We extended the audit scope through March 15, 2021 to complete our IT testing.

Network User Accounts

IT systems and data are valuable resources. The District relies on its IT assets for Internet access, email and for maintaining financial, personnel and student records. If the IT assets are compromised, the results could range from inconvenience to catastrophic and could 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 that data, hardware and software systems may be lost or damaged by inappropriate access and use.

How Should District Officials Manage Network User Accounts?

District officials are responsible for providing users with accounts to access resources on a district's network and user computer. A district should have written procedures for granting, changing and disabling user access. 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 or unneeded accounts as soon as there is no longer a need for them, including user accounts of former employees.

Officials should disable unnecessary or unneeded accounts. ...

The Director is responsible for ensuring that user accounts are managed appropriately. If not properly managed, user accounts could be potential entry points for attackers as they could be used to inappropriately access and view personal, private and sensitive information (PPSI) on the network. Further, unnecessary accounts create additional work to manage network access, along with the risk of errors that could result in users being inadvertently granted more access than needed.

Furthermore, the Director should limit generic accounts. 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 purposes, 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.

District Officials Did Not Adequately Manage Network User Accounts

District officials did not establish procedures to manage network user accounts or maintain a current list of authorized network users to compare to the employee master file. Officials did not provide reasons for not establishing procedures to manage network user accounts, but stated that going forward they will develop procedures. We reviewed all 889 non-student enabled user accounts to confirm they were needed.

Unneeded Non-Student Accounts – Because District officials did not maintain a current list of authorized users or perform periodic reviews of enabled network user accounts, we compared the 889 enabled nonstudent network user accounts to the employee master list and assessed the need for the 254 non-student accounts that did not match the current employees list. Our assessment identified 96 enabled user accounts (38 percent) that belonged to former District employees and three additional accounts that were no longer necessary. When these accounts were brought to the Director's attention, 38 of these accounts were disabled immediately and the District is reviewing the remainder to determine who accesses the accounts if they should also be disabled.

Unneeded network user accounts can be potential entry points for attackers because if they are not monitored or used and, if accessed by an attacker, possibly could be used to inappropriately access and view PPSI. Also, when a District has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access.

If not properly managed, user accounts could be potential entry points for attackers. ...

Unneeded Generic Accounts – Generic accounts are not linked to individual users and may be needed for certain networks services or applications to run properly. We reviewed all 171 generic accounts and inquired whether these accounts were still needed. We determined 96 of the accounts are no longer needed. The Director stated that the District does not maintain some of the generic accounts as they are managed by individual or groups of individual users, however the Director did not know who specifically managed these accounts. However, District officials should know at all times who has access to and is managing these accounts.

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.

How Should Officials Monitor and Enforce Compliance with the Computer Acceptable Use Policy?

A computer acceptable use policy should be developed to describe what constitutes appropriate and inappropriate use of IT resources, along with the Board's expectations concerning personal use of IT equipment and user privacy. The District's acceptable use of computers policy states that all users of the District's computer network and Internet must understand that use of technology in education is an essential component of learning, and that use entails responsibility. Additionally, the use of computers and computer-related technology is solely for the purpose of advancing and promoting learning and teaching.

...[A]ll users of the District's computer network and the Internet must understand that use of technology in education is an essential component of learning, and that use entails responsibility.

However, the policy does outline the users are permitted to incidental personal use before school, during lunch and after school. Failure to comply, may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

Monitoring compliance with a computer acceptable use policy involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, acceptable use policies or standard security practices. Automated mechanisms may be used to help facilitate this process and can help security professionals routinely assess computer security and perform investigations during and after an incident.

Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity, or availability. District officials can reduce the risks to PPSI and IT assets by monitoring Internet usage and by configuring web filtering software to block access to unacceptable websites and limit access to sites that comply with a district's computer acceptable use policy.

Officials Did Not Monitor Compliance with the Computer Acceptable Use Policy

The Board adopted computer acceptable use policy states the use of computers and computer-related technology is solely for the purpose of advancing and promoting learning and teaching. However, it also states incidental personal use is permitted during certain times (before school, during lunch and after school) to certain types of websites.

We reviewed the web browsing history of six computers to determine whether they were used in accordance with District regulations and found District computers were used to access websites for personal use (Figure 1) outside of the permitted times outlined in the policy.

Figure 1: Figure 1: Examples of Personal Internet Use

Type	Site
Online Shopping	Bloomingdales.com
Social Media	Pinterest.com
Health & Wellness	Livestrong.com
Pets	Stinkydog.com
Home Decor	Cornercandlestore.com
News & Entertainment	Prevention.com
Real Estate	Zillow.com
Social Networking	Snapchat.com
Travel	Expedia.com

District officials did not monitor employee Internet use or implement procedures to monitor for compliance with the District's computer acceptable use policy.

Although the District uses web filtering software to block access to some prohibited websites, certain categories of websites that could be accessed for purposes other than learning and teaching, such as shopping, real estate and travel, are not blocked because they are occasionally used for instruction. Despite this limitation, the Director did not ensure logs of Internet use were periodically reviewed for appropriateness. When employees access websites for nonbusiness or inappropriate purposes while logged in with a district network user account, in violation of the District's computer acceptable use policy, productivity is reduced and there is an increased risk that IT assets and users' information, such as PPSI and financial data, could be changed intentionally or unintentionally, lost or used inappropriately.

By not monitoring the personal use of District computers, the District increased the risk their computers and network would be exposed to attacks and malicious software. Consequently, PPSI and other computerized data, including financial records and grades, contained on the computers or accessed from users' accounts had a higher risk of breach, loss and/or misuse.

What Do We Recommend?

The Board should:

1. Ensure officials monitor compliance with the computer acceptable use policy.

The Director should:

2. Develop written procedures for managing system access that ensure network access and permissions are revoked immediately once they are no longer needed and include periodically reviewing user access and disabling user accounts when network access is no longer needed.
3. Maintain a list of authorized network users and routinely evaluate and disable any unnecessary accounts.
4. Ensure all network users have and use their own unique network user accounts to access the District's network.
5. Monitor Internet use and implement procedures to ensure employees comply with the computer acceptable use policy.

Appendix A: Response From District Officials

Building Bridges for today's students to cross into tomorrow's world with equity, innovation and optimism

Administration Building • 13A Dickinson Avenue • Nyack, NY 10960 • (845)353-7000
Phone: (845) 353-7015 • Fax: (845) 353-0508 • Email: ebudhai@nyackschools.org

Eudes S. Budhai
Superintendent of Schools

January 6, 2022

Lisa A. Reynolds, Chief Examiner
Office of the New York State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

Dear Ms. Reynolds:

The Nyack Union Free School District is in receipt of the draft Report of Examination regarding its Network User Accounts for the period July 1, 2018 — March 15, 2021. Please accept this letter as the District's response to the draft Report.

The District and its Board of Education takes their obligations to maintain security of the District's computer network very seriously. In this regard, we note that the District has multiple layers of security protection in place, including a firewall with the capability of automatically isolating infected devices on the network, intrusion detection systems, web filtering, DNS (Domain Name System) filtering and anti-virus scanning. Each security system is also enhanced with a cloud AI (artificial intelligence) component for added protection.

We acknowledge the findings and recommendations set forth in the draft Report. The Board of Education and Central Office Administration view such findings and recommendations as an opportunity to continue their ongoing efforts to improve governance and operations in the District. We will prepare our Corrective Action Plan and will submit it after review and approval by the Board of Education.

The District has already complied with the recommendations to develop written procedures for managing system access and has also developed a plan to monitor compliance with the computer acceptable use policy. As always, the District will continue to implement policies and procedures that provide users, employees and the school community a safe, sound and beneficial educational IT environment.

We appreciate the time and effort undertaken by the Comptroller's Office.

Sincerely,

Eudes S. Budhai
Superintendent of Schools

cc: Board of Education
Gloria Menoutis, School Business Executive

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 policies and procedures to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed District officials to gain an understanding of the processes and procedures for the IT system and applications.
- We ran a computerized audit script on the District's network on January 29, 2021. We then analyzed each report generated by the script, looking for weaknesses in user account management, privilege and group definition and network setting configurations.
- We used our professional judgment to select a sample of six computers from the District's 990 computers and laptops. We selected computers of users who had access to PPSI and financial software. We reviewed web history reports from these computers to evaluate whether Internet users were following the computer user's policy. We also reviewed web history reports for accessed websites that could put the network at risk.

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 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 – 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: : Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

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