REPORT OF EXAMINATION | 2021M-40

Duanesburg Central School District

Information Technology

NOVEMBER 2021

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

Contents

Report Highlights

Duanesburg Central School District

Audit Objective

Determine whether Duanesburg Central School District (District) officials ensured information technology (IT) systems were adequately secured to protect against unauthorized use, access and/or loss.

Key Findings

District officials did not ensure IT systems were adequately secured and protected against unauthorized use, access and/or loss. District officials did not:

- Adequately manage user accounts and permissions.
- Provide cybersecurity awareness training to employees.

After sharing our findings, the Management Information Systems Director (Director) disabled the 13 (5 percent) of the user accounts we reviewed because they were unneeded. Officials also prepared IT cybersecurity training, which employees completed by February 2021.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendation

- Regularly review network and local user accounts for appropriate permissions and disable those that are unnecessary, and ensure that annually employees receive IT security awareness training.

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

Background

The District serves the Town of Knox in Albany County, the Towns of Charleston and Florida in Montgomery County, the Towns of Duanesburg and Princetown in Schenectady County and the Towns of Schoharie and Wright in Schoharie County.

The District is governed by a seven-member Board of Education (Board) that is responsible for the general management and control of financial and education affairs.

The Superintendent of Schools is the chief executive officer responsible for District administration. The District employs a Director who provides IT support to staff and students.

Quick Facts

	Employed	Network User Accounts
Admin/Staff	161	169
Network Servers		2
Computers		347

Audit Period

January 1, 2019 – November 10, 2020

We extended our scope to February 26, 2021 to include cybersecurity training provided to employees.

Information Technology

Why Should Officials Monitor Network User Accounts and Permissions?

Network user accounts enable networks, computers and applications to recognize specific users, grant appropriate user permissions and provide user accountability by affiliating network user accounts with specific users. However, these accounts are potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI).[1]

District officials are responsible for restricting network user access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and IT assets are protected from unauthorized use and/or modification.

To minimize the risk of unauthorized access, district officials should regularly review enabled user accounts, including generic and local accounts,[2] to ensure they are still needed. Officials should disable unnecessary accounts as soon as there is no longer a need for them. Network and local accounts with administrative permissions can perform activities such as installing software, creating user accounts and manipulating security settings. Therefore, officials must ensure that accounts with administrative permissions are assigned only to those who need them to perform their job duties.

Officials should disable unnecessary accounts as soon as there is no longer a need for them.

Officials Did Not Adequately Manage User Accounts and Permissions

District officials did not develop adequate procedures for managing, limiting and monitoring user accounts and permissions and securing PPSI. A network account creation form is used to establish a user's account, the form is submitted to the Deputy Treasurer who confirms receipt of the form with the Director. The Director then creates the user account and assigns permissions based on the employee's job title. The Director removes or inactivates user accounts when the Deputy Treasurer informs him an employee is no longer employed by the District. New employees are required to sign an acknowledgement of the District's acceptable use policy.

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

2 Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs, and local user accounts are accounts that are stored on a specific computer or server and can only be used to log on and access resources on that computer or server.

Officials also did not establish formal procedures for monitoring user accounts to ensure permissions were still needed or the accounts were still necessary. Because officials did not periodically review user permissions, security risks were left unaddressed.

We reviewed the District's 169 employee network accounts, 92 network generic accounts and seven local user accounts.[3]

- Eight employee network accounts (5 percent) were not associated with current employees. These accounts were associated with former employees. Six accounts had periods of inactivity ranging from approximately one to five years and two accounts had no recorded login activity.
- Two employee network accounts had unnecessary administrative permissions.
- Two generic accounts (2 percent) were unnecessary.
- One unnecessary local user account had unneeded administrative permissions.

The Director said that the unnecessary local account was used to initially set up the committee on Special Education Director's computer and was no longer necessary. Also, the Director told us that all inactive user accounts brought to his attention have since been disabled. After we notified the Director about the employee network accounts with unneeded administrative permissions, he told us he removed them.

...District officials did not have formal procedures for disabling user permissions and regularly reviewing enabled user accounts...

Because District officials did not have formal procedures for disabling user permissions and regularly reviewing enabled user accounts and administrative permissions went unnoticed. In addition, because the District had unused and unneeded active user accounts, there was a greater risk that these accounts could have been used as entry points for attackers to access PPSI and potentially compromise IT resources.

When users have unneeded administrative permissions to the network and computers, they could make unauthorized changes that might not be detected. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

Why Should the District Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training that

3 Refer to Appendix B for our methodology.

explains rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees. The training should center on risks including information theft and social engineering attacks,[4] computer viruses and other types of malicious software, all of which may compromise PPSI.

Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything they need to perform their job duties and understand their responsibilities to protect District data. The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, the importance of selecting strong passwords, requirements related to protecting PPSI, or how to respond to a virus or information security breach.

Officials Did Not Provide IT Security Awareness Training

The District did not provide users with IT security awareness training to ensure they understood the importance of security concepts to protect PPSI. Given the ever-changing risks of attacks on IT systems, training on IT security that addresses the evolving threats is an important safeguard. Officials told us they provided employees with verbal and written directives on how to address specific IT threats such as emails notifying staff of reported threats and how to deal with them.

...[O]fficials did not provide users with formal IT security awareness training ...

District officials believed the verbal and email notifications were sufficient training. However, officials did not provide users with formal IT security awareness training that explained how users should comply with IT policies and procedures and proper use of District IT systems and data during our audit period.

When District officials do not ensure that users understand IT security policies and procedures and their roles and responsibilities related to IT and data security, they cannot protect the confidentiality, integrity and availability of data and computer systems. Without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, District data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

In addition, the two users with unnecessary administrative permissions did not receive IT security awareness training. This lack of training put the District's network and PPSI at greater risk because an account with administrative permissions compromised by an attacker could cause greater damage than a

4 Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

compromised lesser-privileged account. A user can be deceived into opening a malicious email attachment, downloading and opening a file from a malicious website, or accessing a website programmed to automatically infect the user's computer with malicious software.

During our audit fieldwork, District officials prepared IT cybersecurity training covering protection of PPSI, malicious software prevention, and safe email communications. Employees completed the training by February 2021.

What Do We Recommend?

The Board should:

1. Develop policies to ensure that unneeded user accounts are disabled in a timely manner.

District officials should:

2. Develop procedures to periodically review network and local user accounts and disable accounts that are unneeded and ensure users have appropriate account permissions.

3. Ensure that annually employees receive formal IT security awareness training that reflects risks identified by the IT cybersecurity community and the District's expectations for employee responsibilities related to the use of IT resources.

Appendix A: Response From District Officials

October 12, 2021

Gary Gifford
1 Broad Street Plaza
Glens Falls, NY 12801

Dear Mr. Gifford:

We are in receipt of draft audit findings and have met with representatives from the Office of the State Comptroller to review findings and recommendations. We are in agreement with all recommendations and thank your team for their report. This audit response is also serving as our corrective action plan (CAP) and has been approved by our Board of Education. The CAP has also been submitted to the NYSED Portal at http://portal.nysed.gov/abp/. Please let me know if additional detail is required.

Sincerely,

James Niedermeier

Superintendent of Schools

Duanesburg Central School District
Dr. James Niedermeier, Superintendent of Schools
133 School Rd. | Delanson, NY 12053 | Office: 518.895.2279 x241 | Fax: 518.895.2626

Unit Name: Duanesburg Central School District

Audit Report Title: Information Technology Report of Examination

Audit Report Number: 2021M-40

For each recommendation included in the audit report, the following is our corrective action(s) taken or proposed. For recommendations where corrective action has not been taken or proposed, we have included the following explanations.

Audit Recommendations:

The Board should:

1. Develop policies to ensure that unneeded user accounts are disabled in a timely manner.

District officials should:

2. Develop procedures to periodically review network and local user accounts and disable accounts that are unneeded and ensure users have appropriate account permissions.

3. Ensure that annually employees receive formal IT security awareness training that reflects risks identified by the IT cybersecurity community and the District's expectations for employee responsibilities related to the use of IT resources.

Duanesburg Central School District
Dr. James Niedermeier, Superintendent of Schools
133 School Rd. | Delanson, NY 12053 | Office: 518.895.2279 x241 | Fax: 518.895.2626

Implementation Plan of Action(s):

Recommendations	Agree or Disagree	Intended Actions and Date	Person Responsible
Recommendation 1 The Board should develop policies to ensure that unneeded user accounts are disabled in a timely manner	Agree	The BOE policy committee will meet to discuss incorporating this language into existing policy 5674 (10/21/21). *Complete*	Superintendent
Recommendation 2 District officials should develop procedures to periodically review network and local user accounts and disable accounts that are unneeded and ensure users have appropriate account permissions.	Agree	A written employee exiting procedure will be drafted and incorporated into the District HR manual (11/1/21). The District will adopt an annual procedure that involves supervisors to sign off on the permissions of their employees on various computer systems, but especially our student management system, our financial management system, and our special education records system (11/1/21). *Complete*	Superintendent Asst. Superintendent
Recommendation 3 District officials should ensure that annually employees receive formal IT security awareness training that reflects risks identified by the IT cybersecurity community and the District's expectations for employee responsibilities related to the use of IT resources.	Agree	The District has adopted an online webinar training about cyber security that all employees are required to complete each year. This webinar will contain an assessment tool (Completed as of May 2021). Periodic in-person training focusing on cybersecurity will be offered to employees on superintendent's conference days (11/5/21).	Asst. Superintendent IT Director

Signed: Dr. James Niedermeier

Date: 10/28/21

Duanesburg Central School District
Dr. James Niedermeier, Superintendent of Schools
133 School Rd. | Delanson, NY 12053 | Office: 518.895.2279 x241 | Fax: 518.895.2626

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, contracted employees, NERIC employees and reviewed the District's IT policies to gain an understanding of its IT environment, internal controls and security awareness training.
- We ran a specialized audit script on six computers and the District's two servers. We chose these computers because they were used by non-instructional employees for on-line banking and transmitting sensitive electronic data.
- We examined all network user accounts and shared folders, all seven local user accounts located on six computers, and configured security settings applied to network and local accounts using specialized audit scripts to identify IT security weaknesses.
- We reviewed the network user accounts and compared them to current employee lists to identify inactive and possibly unneeded network user accounts. We reviewed all generic accounts and discussed them with the Director. We reviewed all network accounts and all seven local accounts on our previously selected sample of six computers for unnecessary user permissions. We reviewed shared folders for questionable content and inappropriate access. We reviewed automated settings to identify any settings that indicated ineffective IT controls for both network and local users.

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 2116-1(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 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

GLENS FALLS REGIONAL OFFICE – Gary G. Gifford, Chief Examiner

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

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