New York State Comptroller
THOMAS P. DiNAPOLI

Eastchester Union Free School District

User Accounts and Information Technology Contingency Planning

2022M-142 | March 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Eastchester Union Free School District

Audit Objective

Determine whether Eastchester Union Free School District (District) officials established adequate controls over user accounts to help prevent unauthorized use, access, and loss, and whether officials established an adequate information technology (IT) contingency plan.

Key Findings

District officials did not establish adequate controls over user accounts to help prevent unauthorized use, access and loss nor did they establish an adequate IT contingency plan. Sensitive IT control weaknesses were also communicated confidentially to officials. Officials did not:

- Develop comprehensive procedures for managing network and financial application user accounts nor did they periodically review all network user accounts and permissions to determine if they needed to be disabled. As a result, we identified the following unneeded network user accounts:
  - 181 for students no longer in the District. These students left the District between June 2020 and August 2021.
  - Six for two former employees, two former Board members and two former interns. These users left District employment between 2016 and 2021.
- Adopt a comprehensive IT contingency plan to minimize the risk of data loss or prevent a serious interruption of services.

Key Recommendations

- Develop written procedures for managing network and financial application user accounts.
- Develop, adopt, distribute and periodically review and test a comprehensive IT contingency plan.

District officials agreed with our findings and indicated they are initiating corrective action.

Background

The District is located in Westchester County and governed by a nine-member Board of Education (Board) responsible for the District's overall governance.

The Superintendent is the chief executive officer and responsible, along with other administrative staff, for day-to-day operations.

The District's IT Director is responsible for strategic planning, development and management of automated information and communication systems and various technologies.

The District contracted with the Lower Hudson Regional Information Center (LHRIC) to operate and maintain the District's IT system with oversight from the IT Director.

Quick Facts	
Students	3,143
Employees	567
Network User Accounts	
Student	3,190
Generic	143
Non-student, non-generic	600
Total Accounts	3,933

Audit Period

July 1, 2020 – August 19, 2021. We extended our scope forward to September 23, 2021 to complete IT testing.

User Accounts and Information Technology Contingency Planning

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

School district officials should develop written procedures for granting, changing and disabling access to the network and financial application resources.

How Should School District Officials Manage Network and Financial Application User Accounts?

To minimize the risk of unauthorized access, school district officials should actively manage network and application 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.

School district officials should develop written procedures for granting, changing and disabling access to the network and financial application resources. These procedures should establish who has the authority to grant or change access and allow users to access only what is necessary to complete their job duties and assignments.

Network and financial application user accounts provide access to a school district's network and application resources and should be actively managed to minimize the risk of misuse. If not properly managed, unnecessary user accounts may not be detected and disabled timely, and they could be additional entry points for attackers to inappropriately use, access and/or delete PPSI on the network or within the financial application.

District Officials Did Not Adequately Manage Network or Financial Application User Accounts

District officials did not develop comprehensive procedures for managing network and financial application user accounts, such as procedures to grant, change and disable access to the network and financial application, periodically review user accounts and disable network and financial application user accounts when access was no longer needed and ensure permissions to the financial application were necessary for users to complete their job duties and assignments.

The IT Director said that the process to grant, change and disable access to the network and financial application is currently manual and relies on updating a student's status from the school building officials, guidance or registrar and

1 Personal, private and sensitive information (PPSI) is any information where 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.

the employee status from Human Resources. However, the District is looking to automate the process. We reviewed network user accounts and financial application user accounts and permissions and found the following deficiencies:

Unneeded Nonstudent, Nongeneric User Accounts – We reviewed all 600 nonstudent, nongeneric network user accounts to determine if any of these accounts were unneeded. We identified six user accounts that were not needed and should have been disabled. These six user accounts include two former employees, two former Board members, and two summer interns not currently working for the District. These users left District employment between 2016 and 2021.

Unneeded Student User Accounts – We reviewed all 3,190 student network user accounts and identified 181 student user accounts that were unneeded and should have been disabled because they were assigned to students no longer enrolled at the District. These students left the District between June 2020 and August 2021. The IT Director said not removing them was an oversight.

Financial Application User Accounts and Permissions – We reviewed all 69 financial application user accounts. We found eight former employees whose financial application user accounts had not been disabled, and four current employees with unnecessary financial application user permissions that were inconsistent with their current job responsibilities. The former employees left District employment between 2014 and 2020. The following users had unnecessary permissions:

- Two individuals in the Human Resources Department and the Assistant Superintendent had access to view, create, delete and update New York State and Local Retirement System and New York State Teachers' Retirement System reports, but they do not have any related job duties.
- A secretary had access to view payroll, including the notes for employee and payroll information, but does not have job duties related to payroll.

The Assistant Superintendent said that user accounts and permissions are usually replaced in the financial application, but this was not done for the eight former employees, and it was an oversight. Of the four individuals with unnecessary permissions, one individual was filling in temporarily for the payroll clerk while the payroll clerk was on leave. Additional duties were given to these four individuals a few years ago when the District was just between payroll clerks. The Assistant Superintendent stated she did not realize they still had those permissions.

Without comprehensive written procedures for managing enabled network and financial application user accounts and permissions, the District had a greater risk that the unneeded access could be compromised or used for malicious purposes. Unneeded network and financial application user accounts and permissions

should be disabled promptly to decrease the risk of unauthorized use, access and loss and eliminate additional entry points for attackers.

Why Should School District Officials Establish an Adequate IT Contingency Plan?

An IT contingency plan is a school district's recovery strategy, composed of the procedures and technical measures that help enable the recovery of IT operations after an unexpected incident. An unexpected incident could include a power outage, software failure caused by a virus or malicious software, equipment destruction, inadvertent employee action or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such events.

The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the school district's operations and IT environment. Proactively anticipating and planning for IT disruptions help prepare personnel for the actions they must take in the event of an incident. The goal of an IT contingency plan is to help enable the recovery of a computer system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

The goal of an IT contingency plan is to help enable the recovery of a computer system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

Because IT resources often support key business processes, planning specifically for disruptions is a necessary part of contingency planning. A comprehensive IT contingency plan should focus on strategies for sustaining a school district's critical business processes in the event of a disruption.

The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity. Backup policies and procedures are also critical components and ensure that information is routinely backed up and available in the event of a disruption.

An IT contingency plan can also include, among other items deemed necessary by school district officials, the following:

- Roles and responsibilities of key personnel,
- Periodic training regarding the key personnel's responsibilities,
- Communication protocols with outside parties,
- Prioritized mission critical processes,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan,

- Backup methods and storage policies, and
- Details concerning how the plan will be periodically tested.

The District's Plan Was Not Adequate, Distributed or Recently Tested

Although officials had a disaster recovery plan (plan) in place, which can include some aspects of an IT contingency plan, it was inadequate and not comprehensive. It only focused on the financial application as a critical operation and did not mention the network as a whole or other potentially critical systems, such as the student management system.

In addition, the plan appeared to be a standard template provided by the LHRIC. The annual review section of the plan was left blank stating "MONTH." It has not been updated since 2016 and listed the former payroll clerk and Treasurer as being in charge of critical operations to recover from a disaster and a part of the emergency planning team.

Furthermore, the District checklist of staff responsible was left blank. The plan states that the LHRIC will back up critical records, but does not state anything regarding a backup plan, how often backups will occur or that backup restoration will be periodically tested.

Additionally, there were no details provided on how often the plan should be tested or updated. Further, the plan did not include, and the District did not have, a backup policy or procedures describing how officials would restore critical IT system data.

We also found that the plan was not distributed to employees or periodically tested to ensure key officials and District contractors understood their roles and responsibilities in a disaster situation and to address changes in security requirements. The IT Director was unaware the District had this plan. He told us there was no plan that he could find when he started with the District approximately six years ago. He said he is aware the District needs a plan and is working to create one. However, if the IT Director believed there was no plan in place when he became the IT Director, he should have developed one at that point. We requested a copy of his in-progress plan and he stated he did not have anything he could provide us. The Assistant Superintendent provided us a copy of the 2016 disaster recovery plan at the end of fieldwork when we were discussing our findings. She was listed as an emergency contact in the disaster recovery plan created in 2016.

We asked officials currently in those key roles if they received training or a copy of the plan and the current Treasurer and accounts payable clerk stated they did not receive training or a copy of the plan. The Assistant Superintendent had a copy

of the plan and received training in 2016 but stated she has not received training since then.

The IT Director and LHRIC representative told us backups were completed weekly and periodic restoration testing was performed. However, the officials did not provide documentation showing the test backups were periodically restored successfully to ensure the process is functioning as intended and that data would be available in an emergency.

Without a comprehensive IT contingency plan in place that is distributed to all responsible parties and periodically tested for effectiveness, District officials have less assurance that employees will react quickly and effectively to maintain business continuity in the event of a disruption or other event impacting operations. In addition, without backup procedures and periodic testing of backup restoration, officials cannot ensure the recovery of necessary data to continue operations if a security breach or system malfunction occurs. IT disruptions can occur unexpectedly. As a result, important financial and other data could be lost, or the District could suffer a disruption to operations.

What Do We Recommend?

District officials should:

1. Develop and enforce written procedures for managing network and financial application user accounts. These procedures should include granting, changing and disabling access to the District's network and financial application, and periodically reviewing user access and disabling user accounts as soon as access is no longer needed.
2. Periodically review financial application access and limit access to ensure that access is based on job function.
3. Develop, adopt, distribute and periodically update and test a comprehensive IT contingency plan that identifies the key personnel responsible and includes detailed guidance for continuing operations and procedures for the recovery of IT operations.

Appendix A: Response From District Officials

EASTCHESTER
UNION FREE SCHOOL DISTRICT
SOARING TO EXCELLENCE

Ronald D. Valenti, Ph. D.
Superintendent of Schools

March 9th, 2023

To Whom It May Concern,

The Eastchester Union Free School District had an Instructional Technology Audit performed by the New York State Office of the State Comptroller between July 1, 2020 and August 19th, 2021. To ensure complete testing of information technology systems, the audit was extended until September 23, 2021. This audit focussed specifically on user accounts and information technology contingency planning. The district was provided a draft public report on February 9th, 2023.

The public report conveyed key findings and corresponding recommendations. They are:

To develop comprehensive procedures for managing network and financial application user accounts.

To develop a comprehensive information technology (IT) contingency plan

To develop, adopt, distribute, and periodically review and test a comprehensive IT contingency plan.

The District understands these three key recommendations and is in agreement with the methodology used to realize these recommendations. The Lower Hudson Regional Information Center (LHRIC), one of 12 regional information centers across the state of New York, supports the Eastchester school district on the management of information technology systems. Since receiving the draft report, the district and LHRIC have started to address each of the recommendations contained in the audit report. Further, the district intends to create a formal corrective action plan to ensure all of the recommendations contained within the audit are appropriately addressed.

Ronald D. Valenti, Ph.D.
Superintendent of Schools

580 White Plains Road • Eastchester, NY 10709 • (914) 793-6130, ext. 4201 • Fax (914) 787-2362
rvalenti@eufsdk12.org

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 LHRIC representatives to gain an understanding of the District's IT operations and reviewed IT-related policies to gain an understanding of the IT environment, including those for user accounts.
- We used a computerized audit script to examine the District's domain controller[2] on August 23, 2021. We then analyzed the report to determine whether all enabled and unexpired network user accounts were for users who were currently employed by or enrolled in the District. We analyzed all accounts not recently used; specifically, employee accounts, generic accounts and student accounts. We then reviewed network user accounts.
- We reviewed user account permissions for all 69 enabled financial application user accounts to determine whether they were appropriate and based on job functions.
- We used our professional judgment to select a sample of five of 11 District computers that had access to PPSI. We ran a computerized audit script on each of the five selected computers on August 19, 2021 or September 23, 2021 to review user accounts for adequacy.
- We obtained the disaster recovery plan from District officials and reviewed the plan to determine whether it was comprehensive, recently updated, distributed to staff and periodically tested to ensure critical issues are identified.

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 GAGAS (generally accepted government auditing standards). 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

2 The domain controller is a server computer used to help centrally manage all computer and user accounts within the domain (network) and their access to network resources.

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 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 of Municipal Audits

33 Airport Center Drive, Suite 102 • 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