REPORT OF EXAMINATION | 2020M-121

Lyncourt Union Free School District

Information Technology

FEBRUARY 2021

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

Contents

Report Highlights **1**

Information Technology **2**

Why Should Officials Manage Network User Accounts and Administrative Permissions? 2

Officials Did Not Adequately Manage Network User Accounts and Permissions 3

Why Should the District Have a Disaster Recovery Plan? 5

The District Did Not Have a Disaster Recovery Plan 5

What Do We Recommend? 5

Appendix A – Response From District Officials **7**

Appendix B – Audit Methodology and Standards **10**

Appendix C – Resources and Services **12**

Report Highlights

Lyncourt Union Free School District

Audit Objective

Determine whether Lyncourt Union Free School District (District) officials adequately managed network user accounts and developed a disaster recovery plan.

Key Findings

District officials did not adequately manage network user accounts or develop and adopt a written disaster recovery plan. As a result, District has an increased risk that it could lose important data and suffer serious interruption in operations. District officials should have:

- Disabled 17 of the 113 network user accounts we examined. The 17 user accounts were unneeded and included generic, shared and former employee accounts.
- Revoked permissions for eight of the 12 network user accounts with administrative permissions because the permissions were unneeded.

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

Key Recommendations

- Evaluate all network user accounts to ensure unneeded network user accounts are disabled.
- Assess all network user accounts with administrative permissions and remove unneeded permissions.
- Develop a comprehensive written disaster recovery plan.

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 Salina in Onondaga County and operates one school for students from Pre-kindergarten through Grade 8.

The District is governed by a five-member Board of Education (Board) responsible for the general management and control of educational and financial affairs. The Superintendent is the chief executive officer and responsible, along with other administrative staff, for day-to-day operations.

The District contracts with the Solvay Central School District (Solvay CSD) for its Director of Technology (IT Director) services and a local area network technician (technician). The IT Director is responsible for managing the District's IT assets and network security, including managing network user accounts and permissions. The technician supports the IT Director in his duties.

Quick Facts	
Network User Accounts	397
Non-Student Network User Accounts	113
Computers/Devices	644
Employees	119
Student Enrollment	366

Audit Period

July 1, 2018 – March 13, 2020

Why Should Officials Manage Network User Accounts and Administrative Permissions?

District officials are responsible for restricting user access to only those 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.

Network user accounts provide users with access to the resources on a district's network and user computers and should be actively managed to minimize the risk of misuse.[1] If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI)[2] and intentionally or unintentionally changed and/or compromised by unauthorized individuals on the network.

A district should have written procedures for granting, changing and disabling user permissions to the network. To minimize the risk of unauthorized access, district officials should actively manage network user accounts, including their creation, use and dormancy, and regularly review enabled network accounts to ensure they are still needed. When employees leave District employment, or when user accounts are otherwise no longer needed, officials should ensure that these accounts are disabled in a timely manner. Officials also should routinely evaluate generic network user accounts and disable those that are not related to a current district or system need.[3]

A shared account is an account with a username and password that is shared among two or more people. Because shared accounts are not assigned to a specific user, officials may have difficulty linking any suspicious activity to a specific user. To help ensure individual accountability, all users should have and use their own user account to gain access to a network. If shared accounts are needed, officials should have procedures in place to monitor who uses the accounts and when they are used.

To minimize the risk of unauthorized access, district officials should… regularly review enabled network accounts to ensure they are still needed.

1 Network user accounts provide users with access to resources on a network and are managed centrally by a server and/or domain controller. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application. A domain controller is the main server in the domain (network) that controls or manages all computers within the domain.

2 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.

3 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 processes, training purposes or generic email accounts, such as a service helpdesk account.

To the extent possible, all users should have and use their own user account to gain access to a network. If officials allow users to share accounts, officials should track each user's activity while using the shared accounts. This helps ensure accountability over work performed and data changed or deleted.

Generally, an administrative account has permissions to monitor and control networks and computers, including the ability to add new users and change user passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. As a result, officials must limit administrative permissions to only those users who need them to perform their job functions and responsibilities.

When users have unneeded administrative permissions to a network, 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.

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. If the deceived user has administrative permissions, an attacker could use those elevated privileges to cause greater damage than with a lesser-privileged account.

Officials Did Not Adequately Manage Network User Accounts and Permissions

District officials did not adequately manage network user accounts and permissions for the District's network. Officials did not have written policies or procedures for managing user accounts and permissions. In addition, officials told us that when an employee was hired or terminated, the District Clerk sent an email to the IT Director, authorizing him to grant, modify or disable the employee's network user account. However, because this procedure was not always followed, and officials did not have a written user account management policy to provide guidance to employees and IT personnel, unneeded network user accounts and accounts with unnecessary administrative permissions went unnoticed until our audit.

We examined all 113 non-student network user accounts to determine whether any were unneeded or had unneeded administrative permissions.

Unneeded Network User Accounts – We found 17 network user accounts that were unneeded and could be disabled, including eight generic network user accounts and nine former employees' network user accounts.

The generic network user accounts included four service accounts previously used to manage computer processes and install updates, two test accounts, an administrative account and a shared substitute teacher account. While these generic network user accounts may have been used in the past, most have not been used in more than six months and are no longer needed.

The shared substitute teacher network user account allowed 29 substitute teachers access to the District's network and student curriculum information. The IT Director told us that substitute teachers have always used a shared account. However, he said he would create individual accounts for each substitute teacher going forward.

When a number of employees share an account without procedures for monitoring the use of the account, the District has a greater risk that PPSI could be changed intentionally or unintentionally or used inappropriately and officials would not be able to identify who performed the unauthorized activities.

Six of the nine former employees' network user accounts were last accessed between December 17, 2015 and June 26, 2019, and the remaining three accounts were never used to log into the network. The Director told us he would disable or delete the unneeded network user accounts we identified.

Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access and view PPSI. In addition, when the District has many network user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network and computer access.

Unneeded Administrative Permissions – We found 12 network user accounts with administrative permissions. These network user accounts also had local administrative permissions on the 10 computers we reviewed. Eight of the 12 accounts had unneeded administrative permissions. The Director told us six of these accounts did not require administrative permissions to function.

We questioned the permissions granted to the remaining two accounts belonging to technology personnel at Solvay. The Director told us the two employees occasionally help out at the District. However, the agreement between the two districts does not mention the two employees. The Director agreed and stated he will revoke administrative permissions for the six service accounts and restrict administrative access for the two Solvay employees.

When employees have unneeded administrative privileges to the network, they could make unauthorized changes that might not be detected, thereby compromising the District's data and IT assets. In addition, a compromise of a network user account with administrative permissions could result in

greater damage than with a lesser-privileged account, including unauthorized manipulation of data or disruption of District operations.

Why Should the District Have a Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event (such as a fire, computer virus or inadvertent employee action) that compromises the availability or integrity of an IT system and data.

To minimize the risk of data loss or suffering a serious interruption of service, district officials should establish a formal written disaster recovery plan. The disaster recovery plan should address the potential for sudden, unplanned catastrophic events that compromise the network and the availability or integrity of district services, including the IT system and data.

To minimize the risk of data loss or suffering a serious interruption of service, district officials should establish a formal written disaster recovery plan.

Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures and periodic backup testing to ensure they will function as intended. Backup data should be stored at a secure offsite location, maintained off-network and encrypted to ensure its integrity. The plan should be periodically tested and updated to ensure key officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

The District Did Not Have a Disaster Recovery Plan

The Board did not develop and implement a formal written disaster recovery plan for its IT environment to describe how officials would respond to disasters. The IT Director told us that data is backed up and stored in different on-site and off-site locations. However, without a formal written plan, the District has an increased risk that it could lose important data and suffer serious interruption in operations.

What Do We Recommend?

The IT Director should:

1. Develop and adhere to written procedures for granting, changing and disabling network user account access.
2. Disable network user accounts of former employees as soon as they leave District employment, periodically evaluate existing network user accounts including generic and shared accounts, and disable any deemed unneeded.

3. Assess administrative permissions for all network users and disable access not appropriate for their job duties and responsibilities.

The Board should:

4. Develop and adopt a comprehensive written disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

Appendix A: Response From District Officials

Lyncourt Union Free School District
2707 Court Street, Syracuse, New York 13208
Phone: (315) 455-7571 Fax: (315) 455-7573
www.lyncourtschool.org

"Great Expectations for Achievement, Respect, and Caring"

James J. Austin
Superintendent

Kimberly A. Davis
Principal

Cathryn L. Marchese
Business Administrator

December 8, 2020

Office of the State Comptroller
Syracuse Regional Office
Rebecca Wilcox, Chief Examiner
State Office Building, Room 409
333 E. Washington Street
Syracuse, NY 13202-1428

Re: Lyncourt Union Free School District Information Technology Report of Examination
Audit Period: July 1, 2018 – March 13, 2020
Audit Report Number 2020M-121

Dear Chief Examiner Wilcox:

The Lyncourt Union Free School District has received and reviewed the draft Information Technology Report of Examination #2020M-121. The audit report will be used as a valuable resource in our continuing efforts to support the District in technology management and security.

The Comptroller's Office performed a thorough examination in a very professional and courteous manner. The District appreciates the time and effort involved in conducting the audit as well as the oversight and feedback that has been provided throughout the process.

The Lyncourt Board of Education and District Administration welcomes the opportunity to reply to the findings and offer our response to the audit recommendations. **This correspondence serves as both the District Response and Corrective Action Plan.**

A very thorough review of the audit report was conducted on August 19th and November 17th, 2020 with the Office of the State Comptroller Syracuse Regional Office. As stated in the report it is very important to restrict network access, user accounts, and properly manage password and account permissions to eliminate risk of data and technology breach. Documenting policy and procedures involving Information Technology management has been overlooked and requires attention by the district. The District acknowledges the weaknesses identified in our IT security controls. The District acknowledges receipt of both the Report of Examination and Management Letter. All key recommendations have been addressed, including those shared confidentially.

Recommendation #1.
The Information Technology Director should develop and adhere to written procedures for granting, changing and disabling network user account access.

Corrective Action Plan:
The District has worked to develop a formal password policy that will be presented to the Board of Education for adoption by February 9, 2021. The policy includes important measures to protect the security of the District's computer system. Included in this policy are specific password criteria, attempt lock-out, forced password change timeframes, guidelines requiring password confidentiality, and log-in/screen protection practices. This will be Lyncourt Union Free School District Policy #5674, under Non-Instructional/Business Operations.

Recommendation #2.
The Information Technology Director should disable network user accounts of former employees as soon as they leave District employment, periodically evaluate existing network user accounts including generic and shared accounts, and disable any deemed unneeded.

Corrective Action Plan:
As part of the employee exit paperwork and processes, the business office will notify IT of any employee termination or change in status as soon as it is known. IT will disable the account(s).

The process is included in an office check-off list on our formal exit form.
User accounts will continue to be audited at least once a quarter to assure that employee status has not changed and users have the correct access.

Recommendation #3.
The Information Technology Director should assess administrative permissions for all network users and disable access not appropriate for their job duties and responsibilities.

Corrective Action Plan:
The IT Director has completed the recommendation to clean up all administrator permissions on network accounts. Going forward, the IT Director will manage network accessibility by limiting user access only to those resources necessary to complete their jobs. Continued oversight of this will be maintained through a consistent audit, at least quarterly, to insure changes to user accounts are current and appropriate.

Recommendation #4.
The Board of Education should develop and adopt a comprehensive written disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

Corrective Action Plan:
The Lyncourt Union Free School District partners with the Solvay Union Free School District for its District Computer System (DCS). This partnership includes contracting services for a .25 IT

Director, a .40 LAN Technician, as well as housing our DCS servers. Lyncourt does not have a DCS on premise. It was understood the Solvay UFSD Data Recovery Plan would cover Lyncourt's data that is housed there. The Lyncourt UFSD will develop its own independent data recovery plan. The plan will encompass the Solvay UFSD recovery plan as it too will have to be followed in the event of necessity. This recommendation will be completed by May 11, 2021. Going forward, the written disaster recovery plan will be distributed to all responsible parties, periodically tested and updated as needed.

The Board of Education represents the community in working together with the administration and staff toward the mission of sound management practices. The Board of Education and District Administration would like to thank you for the professional manner in which the audit was completed and for the valuable recommendations and feedback that resulted. We will use the experience and information in our continuing efforts to provide a secure, responsible and progressive educational plan for our students at Lyncourt Union Free School District.

Sincerely,

Mr. James J. Austin
Superintendent

Mrs. Cathryn L. Marchese
Business Administrator

Dr. Lawrence Salamino
School Board President

Mr. David Florczyk
School Board Vice-President

Mr. Michael Leonardo
School Board Trustee

Mr. Anthony Maggi
School Board Trustee

Mrs. Kimberly Vespi
School Board Trustee

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 reviewed the District's IT related policies to gain an understanding of the IT environment and internal controls and to determine whether the District had a written disaster recovery plan.
- We used specialized audit software to examine the District's domain controller and 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 the 113 nonstudent network accounts to the active employee list to identify accounts for former employees and/or unneeded accounts.
- We used our professional judgment to select a sample of 10 District computers assigned to 10 employees. We chose these employees because they had access to PPSI. We examined these computers using specialized audit software to determine whether network user accounts had administrative permissions.
- We compiled a list of the folders and sub-folders shared from the server, along with the related user accounts and groups. We reviewed the District's list of shared folders that may contain PPSI data by searching with key words such as financial, business office, guidance or grades. We reviewed users with permissions to those folders to determine whether access was appropriate.

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/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

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?title=&body_value=&field_topics_target_id=263206&issued=All

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/sites/default/files/local-government/documents/pdf/2020-05/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?title=&body_value=&field_topics_target_id=263211&issued=All

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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

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