NEW LEBANON
CENTRAL SCHOOL DISTRICT

New Lebanon Central School District School
Network User Accounts Audit
Audit Report Number: 2021M-30
August 30, 2021

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 Recommendation:

- Develop and implement written procedures for granting, changing, and disabling user permissions
- Design and implement procedures to monitor employee computer use and implement procedures to monitor for compliance with policy
- Provide periodic IT security awareness training to all employees who use IT resources that includes guidance on the importance of appropriate computer use

Implementation Plan of Action(s):

1.) The district has created a procedure manual that includes written procedures for granting, changing, and disabling user permissions. These procedures can be found on page 2 and 3 of the attached "NL IT/Network and Systems Engineer Procedures"

2.) Also included in this procedure manual are procedures to monitor employee computer use based on district policy:

"The network administrator will monitor employee and student Internet use regularly. Network Admin will set aside a day a month to examine employee Internet browsing history. This information will be gathered by the network administrator and the supervisor of the employees or principal of the student who is not following the acceptable use policy will be contacted and the incident will be documented."

3.) Also included in our procedure manual is a plan for security awareness:

"The superintendent will provide yearly IT security awareness training at the first

Superintendent's conference day each September. This training will explain district IT policies and procedures to all employees and communicate the proper rules for using district Internet and its systems. This PD will review requirements to protect private and sensitive information.

The Network administrator will provide two additional virtual trainings for all employees on the following topics: emerging trends on information theft, social engineering attacks, computer viruses, and other types of malicious software, dangers of Internet browsing/downloading files & programs from the Internet, requirements related to PPSI and how to respond if an information security breach is detected."

Network administrator will proactively phish and assess employee's Internet and email security throughout the school year.

Implementation Date:

1.) "NL IT/Network and Systems Engineer Procedures" manual created and completed August 2021

2.) Procedures shared and reviewed with all faculty and staff on – September 1, 2021

3.) All new procedures and protocols put into effect starting at the beginning of the 2021-2022 school year.

4.) Implementation will be monitored regularly and be on going

Person Responsible for Implementation:

Andrew Kourt - School Superintendent, is responsible for overseeing this action plan.

Ethan Race – Network and Systems Engineer, is responsible to ensure all procedures are being implemented

New Lebanon CSD IT/Network and Systems Engineer Procedures:

New Lebanon Central School District

August 2021

I.) Cyber and Network Security:

1.) Password Procedures -

- Lockout settings should be set to 7consecutive attempts. Failed log in will result in the system being locked out for 15 minutes, unless unlocked manually by an administrator.
- All network passwords should expire every 60 days for all employees and students. All users will have to create a new password every 60 days.
- Passwords should be a minimum of 8 characters and should not include names or words that can be easily guessed or identified. Each password should include letters, at least one number, and at least one symbol.
- An exception will be made for students in grades PK through grades 2 - Passwords can be modified and these young children do not have to change their passwords. A unique password should still be maintained.
- Reversible encryption option should be disabled when storing password

2.) Network Security Settings -

- Networks should be configured to prevent anonymous "unauthenticated" users from being able to convert or translate security identifiers into their related usernames. The translation setting must be configured.
- Users sessions district wide should be timed out after 15 minutes of inactivity, requiring a password to be re-entered to gain access to the computer or device.
- Network setting that turns off the Autoplay feature for all computer drives should be enabled.
- Remote Desktop Protocol or access is limited only to the district's IT manager or must be approved by the superintendent.
- Remote network access must be configured to limit remote access to authorized administrators.
- RDP settings must be configured to ensure users are prompted for passwords upon connection or prohibits users from saving their passwords

3.) Network User Accounts:

- Network administrator will receive an email from the superintendent's secretary, which will notify him when he has to create a new employee network and email account
- Network administrator will receive an email from superintendent's secretary, which will notify him when he has to disable an account
- The high school and elementary school registrars will email the network administrator to let him know when a new student registers and withdraws from the district. The network administrator will immediate activate or deactivate the student's account
- Network administrators should review user accounts monthly with school librarians to make sure that all student and employee accounts are up to date.
- Network Administrator will completely delete teacher and support staff accounts when the superintendent's secretary emails him about an employee leaving (administrator will contact IT if anything in account has to be saved.
- Administrators or office staff accounts will be kept in a deactivated/suspended state for 1 year

4.) Acceptable Use Policy:

- All employees, parents, and students must sign an acceptable use policy at the beginning of each school year. This policy will define the procedures for computer, Internet, and email use and will describe what constitutes appropriate and inappropriate use of IT resources.
- Student acceptable use policies will be collected, maintained, and kept in each building's office.
- Faculty and Staff acceptable use policy will be shared yearly and each member will sign off on receipt

Monitoring Acceptable Use Policy:

- The network administrator will monitor employee and student Internet use regularly. Network Admin will set aside a day a month to examine employee Internet browsing history. This information will be gathered by the network administrator and the supervisor of the employees or principal of the student who is not following the acceptable use policy will be contacted and the incident will be documented.

II. Security Awareness Training

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

The superintendent will provide yeary IT security awareness training at the first Superintendent's conference day each September. This training will explain district IT policies and procedures to all employees and communicate the proper rules for using district Internet and its systems. This PD will review requirements to protect private and sensitive information.
The Network administrator will provide two additional virtual trainings for all employees on the following topics:emerging trends on on information theft, social engineering attacks, computer viruses, and other types of malicious software, dangers of Internet browsing/downloading files & programs from the Internet, requirements related to PPSI and how to respond if an information security breach is detected.

Network administrator will proactively phish and assess employee's Internet and email security throughout the school year.

III. Creating User Accounts:

- The Superintendent's Secretary will email the Network Engineer when a new employee is hired for account set up
- Network Engineer will set up the account and email
- The Network Engineer will send a confirmation email to the superintendent's secretary on completion

IV. Deleting User Accounts:

- The Superintendent's Secretary will email the Network Engineer when an employee is leaving for account deletion.
- Network Engineer will delete the account and email
- The Network Engineer will send a confirmation email to the superintendent's secretary on completion.

- The Network Engineer will work with building librarians and the superintendent's secretary to review employee and student accounts to make sure accounts are to date.

V. Beginning of School Year IT Procedures:

There is a lot of technology set up needed each September to ensure our teachers and classrooms have what they need for the upcoming school year. Attached are expectations in a checklist form that the systems Engineer is expected to complete by the start of each school year… See Network and Systems Engineer Beginning of the year checklist

VI. IT Help Desk Procedures:

- School employees must put the Item in the Ticket System.
- Priority is getting the teachers teaching, classroom issues rank first.
- The systems manager will be responsive, fix it fast, or at least let the person know that you are working on the issue.
- The system manager will be responsive and will communicate with the person, give updates, and follow up with the person who made the ticket

VII. Firewall and Wifi Maintenance

- Maintain the least access possible, include a default block, then whitelist.
- Login at least once per month to check the logs for abuse and too much use.
- Check the integrated filter for student access, make sure it's appropriate.
- Notify an administrator if needed.

VIII. Inventory of all District Computers and Devices

- An inventory of district owned desktops, laptops, devices, graphing calculators, Smart Boards, projectors, and printers will be maintained by the Network Engineer. This information will be kept on a spreadsheet and should include the following information: Type of equipment, year purchased, Vin number, warranty information/date expired, expected life expectancy, location of equipment (room # or person)

- When the information is updated, the Network Engineer should print out the spreadsheet and keep all sheets in a binder called IT inventory. This information should be updated regularly. The binder should be housed in the superintendent’s office.

IX. Computer and Device Replacement Plan

- Based on district owned inventory, technology life expectancy, and student need the Network engineer should present a computer and device replacement plan to the superintendent each fall. This plan should include specific recommendations for purchase and justification why the replacement is needed. This should be presented to the superintendent by November 1st of each school year.

XI. Phone Maintenance

- Each summer check with principals on room assignments and what faculty or staff member are assigned to which phone
- When someone is new to a specific phone - wipe out the system and delete any old information
- Change the person's name on the system so that it reads properly on the phone screens
- Make sure extensions are assigned to the correct person
- When there is a mid year employee change - please repeat above so that our phones are always updated and accurate.
- When setting up phone for employees - be sure to set voice mail to each employee's email

XII. Camera Maintenance and Monitoring

- Cameras should be routinely checked for proper angle review
- Notify maintenance via work order when routine cleaning, repair, or pest mitigation is needed
- If a camera is down - work to remedy the situation as soon as possible and be sure to let administration know.

XIII. Fob/Access Cards

- When system's manager receives the email from the superintendent's secretary system's manager should go into access control and delete the person from the account

- When a new person is hired, the system manager will assign the person a Fob with the appropriate access permissions. This Fob will be given to the building secretary for distribution.

Systems Engineer Beginning Year Checklist:

- ________ - Make sure all student and staff Chrome books are updated, charged, and in working condition by September 1st of each school year.

- ________ - Check with building principals and CSE Chairperson to see where Chromebook carts should be delivered and held in anticipation of the start of the school year.

- ________ - Once a classroom or office is cleaned by custodial staff. Make sure all classroom desk tops are put back together and in working condition by September 1st (unless the classroom is not yet cleaned).

- ________ - Once a classroom is cleaned by custodial staff. Make sure all classroom smartboard and projector stations are put back together and in working condition by September 1st (unless the classroom is not yet cleaned).

- _________- Once a classroom is cleaned by custodial staff. Make sure all phones are put back together and in working condition by September 1st (unless the classroom is not yet cleaned).

- _________ - Make sure all printers and photocopiers in each building are set up and working properly

- _________ - Double check that all newly hired faculty and staff are set up with usernames and accounts

- _________ - Make sure all phones are updated based on new staff and room office changes (Get room/office changes from principals). If a new person is assigned to a new classroom or office, clear out the old employee's phone and set up the new name in the system. Please complete this by September 1st.