



Amherst Central School District

Anthony J. Panella
Superintendent

Lynn Shanahan, Ph.D.
Assistant Superintendent
Curriculum, Instruction & Technology

Michael Belle-Isle
Assistant Superintendent
Student & Staff Services

August 16, 2023

Office of the New York State Comptroller
Division of Local Government & School Accountability
PSU-CAP Submission
110 State, Street, 12th Floor
Albany, NY 12236

To Whom it May Concern,

The Amherst Central School District is in receipt of the New York State Office of the State Comptroller's Network User Account Access and Application User Accounts and Permissions Report, covering the period of July 1, 2020-July 7, 2022. The Board of Education and the District Administration of the School District would like to thank the Comptroller's office for their professionalism and courtesy in conducting their audit. The District appreciates the recommendations, both written and verbal, that were offered as part of the audit. The Amherst Central School District is committed to keeping our students and all employees safe by reducing risks and vulnerabilities within our systems.

Note: As per New York State Education Law §2-d the New York State Education Department adopted the National Institute of Standards and Technology Cyber Security Framework (NIST-CSF) for districts to use as the standard for data security and privacy. Educational agencies, such as Amherst Central School District, were required to use the NIST CSF framework beginning July 1, 2020. Throughout our response we refer to the required framework using the acronym NIST CSF. Below we address each recommendation to ensure the safety of all users.

Audit Recommendation 1:

Develop and adopt a written user account and permissions policy and develop comprehensive written procedures detailing the process to add, modify and disable user accounts and permissions, including those granting administrative access, to the network and applications.

Description of actions planned to be taken:

A User Access Policy will be written in accordance with NIST- CSF guidelines which details procedures for how user permissions and accounts are granted, modify and/or disable network and application account access. Assigning elevated permissions will be clearly defined in the policy to follow the practice of least privileged access.

Date Action Completed or will be completed:

A new User Access Policy will be written by August 30, 2023.

Name of responsible party:

Senior Network Manager and District Data Coordinator

Audit Recommendation 2:

Ensure District users follow the written procedures once they are established and implement a process for monitoring compliance with the procedures.

Description of actions planned to be taken:

An Audit Policy will be written in accordance with NIST CSF guidelines. This policy will detail how, when, and why the district reviews log data as well as user account information.

Date Action Completed or will be completed:

The Audit Policy will be written and adopted by January 2024.

Name of responsible party:

Senior Network Manager and District Data Coordinator

Audit Recommendation 3:

Ensure that unnecessary network user accounts are disabled as soon as they are no longer needed and periodically review all enabled network user accounts, including service and shared accounts, for necessity and appropriateness.

Description of actions planned to be taken:

New software has been purchased which will allow the district to track employee onboardings, transfers, and exits in a much more effective manner. This tool will be deployed in July of 2023 with the expectation of being fully implemented at the beginning of the school year, September 2024. The new software added to the infrastructure along with the adopted User Access Policy will address recommendation # 3.

Date Action Completed or will be completed:

Recommendation 3 will be addressed by September 2024.

Name of responsible party:

Senior Network Manager, Assistant Superintendent of Student and Staff Services and District Data Coordinator

Audit Recommendation 4:

Monitor application company user and BOCES 'super user' accounts by periodically reviewing audit logs detailing the activity of these users and require District approval for all such accounts and their associated application permissions.

Description of actions planned to be taken:

Wincap (Harris Computer) has reported that both they and BOCES use the 'super user' accounts for various maintenance and support activities for districts. For the purpose of monitoring these accounts, the Amherst Central School District will develop a schedule to run reports that will detail use of these accounts to confirm that the usage is appropriately associated with the application permissions.

Date Action Completed or will be completed:

By the end of June of 2024.

Name of responsible party:

This will be administered by the technology department, led by the Senior Network Manager, in accordance with the User Access Policy, Audit Policy, and all configuration changes will be subject to the Change Management Policy.

Audit Recommendation 5:

Have procedures in place for necessary shared user accounts to monitor who uses the accounts and when and how they are used.

Description of actions planned to be taken:

Audit recommendation # 5 is related to audit recommendations and responses to recommendations # 1 and # 2. Information around shared user accounts will be clearly defined in the User Access Policy. Monitoring the use of said accounts will be defined in the Audit Policy in finding two's response.

Date Action Completed or will be completed:

By the end of January 2024.

Name of responsible party:

Senior Network Manager and Assistant Superintendent of Curriculum, Instruction, and Technology

Audit Recommendation 6:

Limit student information and financial application user accounts' permissions, including those granting system administrative access, based on an account user's responsibilities and to properly segregate incompatible duties, and periodically review application permissions for necessity and appropriateness.

Description of actions planned to be taken:

In accordance with the Users Access Policy and Audit Policy, the Amherst Central School District Technology Department will review all elevated access accounts to ensure each user has the lowest possible system rights necessary to perform their duties. The district will develop a schedule to review on a regular basis the accounts with elevated access.

Date Action Completed or will be completed:

By the end of January 2024.

Name of responsible party:

Technology Department led by the Senior Network Manager in accordance with the User Access Policy and Audit Policy.

Audit Recommendation 7:

Ensure that unnecessary application user accounts, including any for non-District users, are disabled as soon as they are no longer needed.

Description of actions planned to be taken:

Develop a Change Management Policy which will define actions that are taken when there is a transfer, new hire, and exit. This policy will impact student, staff, and 3rd party accounts.

Date Action Completed or will be completed:

The Change Management Policy will be written and adopted by March 2024.

Name of responsible party:

Senior Network Manager with the Assistant Superintendent of Staff and Student Services

Audit Recommendation 8:

Limit elevated financial application permissions to the CIO or another designated employee who is not involved in the District's financial operations.

Description of actions planned to be taken:

The district will develop a schedule to review any accounts that have elevated access on a yearly basis. Additionally, a matrix detailing what positions receive what access level, based on their job responsibilities so that assigned access is commensurate with the job responsibilities.

Date Action Completed or will be completed:

By January of 2024.

Name of responsible party:

Senior Network Manager, Assistant Superintendent of Student and Staff Services and District Data Coordinator

Audit Recommendation 9:

Ensure issues identified as a result of District internal audits are investigated and rectified timely.

Description of actions planned to be taken:

The Audit Policy will outline steps to resolve all findings of audits within one year of receiving the audit report. The findings from the audits will be reviewed by a subcommittee of the Safety Committee on an annual basis.

Date Action Completed or will be completed:

Audit Policy will be completed by January 2024.

Name of responsible party:

Senior Network Manager, Assistant Superintendent of Staff and Student Services, & Assistant Superintendent of Curriculum, Instruction, and Technology

Sincerely,



Anthony J. Panella
Superintendent