Dr. Kathleen Davis
Superintendent of Schools

Baldwinsville
Central School District
Achieving our full potential together.

Kimberly A. Vile
Assistant Superintendent for
Management Services
29 East Oneida Street
Baldwinsville, NY 13027
315-638-6055(Office), 315-635-3970 (Fax)

The 2022-23 fiscal year internal audit was performed by D'Arcangelo & Co., LLP for the Baldwinsville Central School District. The audit findings are summarized below and can be reviewed in detail in the full audit reports that are also attached. The items listed below were found as opportunities for strengthening internal controls and operating efficiency. The audit committee reviewed the full reports on June 5, 2023 and discussed corrective action steps as noted below in italics. In addition the Audit Committee was provided with and reviewed a copy of the District's 2022-23 Internal Audit Report.

Internal audit recommendations and corrective action:

Accounting Procedures Manual
Recommendations

We recommend that the District develop a comprehensive accounting procedures manual that is separate from Board Policy and Superintendent Regulations. Such a procedures manual would ensure that procedures are consistently applied throughout the District. It would effectively notify all accounting personnel of their duties and improve lines of communication. In developing the accounting procedures manual, the District should consider the following elements:

- Written job descriptions for each accounting position. These descriptions should be provided to each employee and serve as a guideline for hiring and evaluating personnel. The District already has many of these job descriptions documented.
- Appropriate descriptions of all financial policies, accounting procedures, internal controls over payroll, cash disbursements, and cash receipt cycles.
- A segregation of duties matrix for each of the main transaction cycles that provides an overview of the role of each position in the internal control process.
- A list of standard forms and system generated reports used in the School with a detailed explanation of their purpose and preparation.

The accounting procedures manual should be updated annually and should be distributed to all accounting personnel and other appropriate personnel. It should evolve to meet the needs of the District and should provide an accurate reflection of the current system of accounting.

Corrective Action: *The District will strive to continue efforts to develop a procedure manual with the understanding that this is a living document that needs to be reviewed annually. The intent is to review this annually and continue to update it annually beginning June 30, 2023.*

Conflict of Interest Statements
Recommendation
We recommend the District add a reviewer signoff to form, and formalize a procedure to document communication of the results to the appropriate individual.

Corrective Action: *The District will update the form prior to June 30, 2023 to include a signoff by the District Clerk for all conflict of interest statements that are completed for the 2023-24 school year. The Board of Education will be notified by September 1, 2023 of any potential conflicts.*

Information Technology - Governance
State Privacy Regulation Implementation
Recommendations

1. Proceed with the remaining NIST CSF framework implementation project initiatives consisting of establishing a consolidated control gap list and remediation plans.
2. Continue with initiatives to establish for data protection and privacy standards
3. Proceed with establishing a data classification standard and determine data classifications assigned to applications and IT Services used by the District.
4. For the critical vendors which host District inscope ED-2 data, in which the District has a direct contract with these third parties (i.e., excludes contracts that BOCES manages in which they include a required ED-2 contract clauses), submit ana contract amendments to these vendors which includes the missing ED-2 required provisions.
5. Establish a project to interpret the LGS 01 standard from a business and Instructional record standpoint to determine which applications systems would be subject to data retention requirements. For any of the applications that are hosted by third-party vendors, the District should send a formal communication to question whether they are meeting the LGS 01 retention requirements. In addition, IT should confirm the retention of data for IT areas directly under their responsibility.

Corrective Action: *The District will continue to develop remediation plans based on the NIST CSF framework. This is an ongoing and continuous process. The Technology Department has developed Standards for the following areas as of June 30, 2023:*

a. Remote Access
b. Information Security
c. Account Management / Access Control
d. Patch-Management

We will continue to develop standards for other areas controlled by the Director of Technology. We will send amended ED2 contracts to identified vendors with additional provisions and send formal communication to question whether they are meeting the LGS 01 retention requirements. The Director of Technology will expand the current data classification and risk assessment database and send amendments by June 30, 2024.

Information Technology - Governance
Vendor Management
Recommendations

1. The District should request access to this SOC report from CNYRIC to ensure the services they use were included in the scope of the audit and all existing exceptions identified in the report presented no risk to the District. This review should be formalized using pre-defined criteria.

2. The District should perform vendor oversight review of Tyler Technologies using predefined criteria which would need to be established.
3. Review the results of the CNYRIC vendor oversight review of Mindex Technologies when they are available for review for formal District acceptance.

Corrective Action: *The District will request access to this SOC report from CNYRIC, request that Tyler Technologies provide the results from the independent assessment of their NIST CSF implementation or; perform vendor oversight review using predefined criteria established by September 1, 2023. The District will review the results of the CNYRIC vendor oversight review of Mindex Technologies by September 1, 2023.*

Information Technology - Governance
Security Awareness
Recommendation

Proceed with the plan to conduct an email phishing test to ensure the District's staff does not fall prey to phishing attacks.

Corrective Action: *The District will conduct annual email phishing tests commencing after October 30, 2023 but before June 30, 2024.*

Acceptable Use of Technology Resources
Recommendation

Update the Acceptable Use Policies to govern the use of cloud based technologies.

Corrective Action: *The District will update its Acceptable Use Policy to include cloud based technologies by June 30, 2023.*

Information Technology -Application Controls
Application Logon Security
Recommendations

1. The District is exploring the possibility of migrating the cafeteria services to Mosaic which has advanced logon security capabilities. The District will be requesting a report from Heartland Solutions which provides a list of invalid logon attempts which would be reviewed by the District.

2. The District is working on alternate solutions to provide more effective School Tool logon security controls In the interim, to mitigate the risk, the District has established a logging process to capture invalid logon attempts and will use AlienVault SEIM to initiate alerts to IT for their follow up analysis to identify potential brute force attacks in the attempt to takeover District School Tool accounts.

Corrective Action: *As of May 5th, 2023**,** the Director of Technology has determined that Nutrikids is a devices-specific service and it can only be accessed from the workstation that the software is installed on, therefore minimizing the risk of infiltration from the outside. The District is undergoing testing the logging of login attempts. The District has started to gather data and the next step is to interpret the events and build reports and alarms. The District will use Alienvault to assist with this process.*

Information Technology - Disaster Recovery
Disaster Recovery Planning
Recommendations

1. Since the District building network design are point to point from each building to the Data Center, establishing an alternate processing site would not provide the typical benefits because all buildings would need to have network capabilities built out to reach this alternate site. However, an analysis should be performed of how an alternative Active Directory environment can be established to allow for School Tool logon authentications to occur when the District's Data Center is not accessible
2. Consider deploying a backup generator at the District Office to ensure the phone system remains operational in the event of a power failure. Alternatively, the connections can be moved from the District Office to the server room.
3. Contact vendors which host District systems and obtain formal RTO commitments to determine whether they meet stated District RTO requirements. For any instances in which these vendors are not able to meet District RTO requirements, this risk should be escalated to the Audit Committee for possible risk acceptance.

Corrective Action: *The District will work with CNYRIC to determine feasibility of duplicating our AD environment off-premise as of June 30, 2023. The District will review options with regards to a backup generator and determine feasibility by June 30, 2024. The District will contact vendors and obtain formal RTO commitments by June 30, 2024.*

Information Technology- Network Security
Physical Security to Data Center
Recommendations

1. The District should install water sensors in the data center which provides alerts when there is water on the floors.
2. The District should invest in racks where all equipment can be raised.
3. The District should consider installing alarms when the door leading to the Special Education offices are opened.

Corrective Action: *The District will gather quotes and review the costs associated with these recommendations and make a determination by September 30, 2023 as to whether to install the recommended devices**.***

Network Vulnerability Management
Recommendation

Run an industry accepted vulnerability scanner to identify any security vulnerabilities identified within the District's external IPs and apply any required remediation.

Corrective Action: *The District will contract with a vendor to run an industry accepted vulnerability scanner to identify any security vulnerabilities identified within the District's external IPs and apply any required remediation by June 30, 2024.*