

**Elwood Union Free School District
Report on Information Technology
For the Fiscal Year Ended June 30, 2025**



TABLE OF CONTENTS

Executive Summary	1
Overview, Procedures Performed, Observations, and Recommendations	2 – 6
Corrective Action Plan	7

Board of Education
Elwood Union Free School District
100 Kenneth Avenue
Greenlawn, NY 11740

We have been engaged by the Board of Education (the “Board”) to provide internal audit services to Elwood Union Free School District (the “District”) with respect to the internal controls related to information technology for the fiscal year ended June 30, 2025.

The objectives of the engagement were to evaluate the efficiency, effectiveness, and compliance of the District’s internal controls related to information technology with relevant policies, procedures, and regulatory requirements, where applicable.

Our procedures were not designed to express an opinion on internal controls related to information technology, and as such, we do not express such an opinion. Our audit of the District's information technology program identified areas of strength as well as opportunities for improvement. By implementing the recommended improvements, the District can further enhance the efficiency and effectiveness of its information technology processes. The results of our procedures are presented on the following pages.

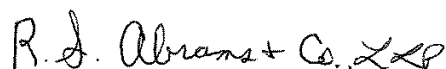
This report is intended solely for the information and use of the Board, the Audit Committee, and management of the District and is not intended to be and should not be used by anyone other than those specified parties.

We would like to acknowledge the courtesy and assistance extended to us by personnel of the District.

We are available to discuss this report with the Board or others within the District at your convenience.

Our observations and recommendations are directed at the improvement of the system of internal controls and should not be considered a criticism of, or reflection on, any employee of the District.

Very truly yours,



R.S. Abrams & Co., LLP
August 29, 2025

ELWOOD UNION FREE SCHOOL DISTRICT
Report on Information Technology
For the Fiscal Year Ended June 30, 2025

**OVERVIEW, PROCEDURES PERFORMED, OBSERVATIONS, AND
RECOMMENDATIONS**

AREA: INFORMATION TECHNOLOGY (IT) POLICIES AND GOVERNANCE

Overview: School districts are legally required to implement information technology (IT) policies that ensure data privacy, cybersecurity, and compliance with state and federal regulations. Key policies include data privacy, security breach and notification policy, Parents' Bill of Rights, and an acceptable use policy for internet and technology use. Policies must cover data breach notification, disaster recovery, network access controls, and security measures to protect student and staff information. These policies are regularly reviewed, updated, and made publicly available.

Relevant Board Policies Examined:

- Policy #8635, *Information and Data Privacy Security Breach and Notification*
- Policy #8630, *Computer Resources and Data Management*
- Policy #4526, *Computer Use in Instruction*
- Policy #4526.1, *Internet Safety*
- Policy #8635-E, *Parents' Bill of Rights for Student Data Privacy and Security*

Procedures Performed:

- Conducted interviews with key District personnel to assess the IT governance framework, policy development, and risk management practices.
- Reviewed published Board policies for compliance with state and federal data privacy and cybersecurity regulations.
- Reviewed the Parents' Bill of Rights as published on the District's website to ensure compliance with FERPA (Family Educational Rights and Privacy Act).
- Reviewed the internet safety policies to ensure compliance with CIPA (Children's Internet Protection Act).
- Reviewed eight (8) IT vendor contracts to confirm that agreements include:
 - Data security and privacy provisions.
 - Signed copies of the Parents' Bill of Rights.

Observation: No observations noted.

Recommendation: No recommendations noted.

AREA: NETWORK SECURITY CONTROLS

Overview: The network security controls are designed to protect student, staff, and administrative data while ensuring compliance with state and federal regulations. Key security measures include firewalls, intrusion prevention systems (IPS), multi-factor authentication (MFA), encryption, and content filtering to safeguard against cyber threats and unauthorized access.

ELWOOD UNION FREE SCHOOL DISTRICT
Report on Information Technology
For the Fiscal Year Ended June 30, 2025

The District has implemented role-based access controls to limit system access based on job roles, secured Wi-Fi networks, and network segmentation to separate student, staff, and guest traffic. Security monitoring tools are in place to detect and respond to threats.

The District conducts annual acceptable use policy training and data privacy security training for all employees through the Global Compliance Network (GCN). The District also takes a proactive approach to cybersecurity by providing ongoing phishing drills to educate employees on identifying, responding to, and reporting cyber threats.

Procedures Performed:

- Reviewed the District's policies and procedures regarding network access and security controls.
- Inquired with key District personnel to obtain an understanding of the network and network access procedures.
- Verified that the District's network firewall is operational, regularly reviewed, and configured to block unauthorized access.
- Verified the District regularly performed updates and security patches to servers, workstations, and network devices.
- Verified access to District systems are secured by multi-factor authentication.
- Confirmed that separate networks exist for students, staff, and guests (network segmentation).
- For one selected server room location, verified physical controls such as access restrictions, temperature controls, fire suppression systems, and extinguisher placement in the server room exist and are operational.

Observation: We noted the District does not currently have a process in place for the regular installation of software patches and updates.

Recommendation: Failure to install patches on a regular basis increases the risk that the District's network and computing systems may be exposed to security vulnerabilities, including viruses and other malicious threats. We recommend the District establish and implement a formal patch management process to ensure timely and consistent application of software updates and security patches.

Observation: We noted that formal cybersecurity training is not currently provided or required for District employees. However, we noted that periodic notifications are sent to District employees pertaining to cybersecurity best practices and emerging threats. Additionally, the District is in the process of implementing a formal cybersecurity training program on Superintendent's Conference Day starting in September 2025.

Recommendation: We recommend the District develop and implement a formal cybersecurity training program, including a process to track employee participation. Additionally, alternative training sessions should be offered for employees unable to attend on Superintendent's Conference Day to ensure that all staff complete the required cybersecurity training on an annual basis.

Observation: We noted that the District's server room does not have surveillance cameras or access logging mechanisms (e.g., keycard entry logs, sign-in sheets, or access control systems) to monitor or restrict physical access. The server room door is secured with a standard lock, but there is no record maintained of who accesses the room or when.

ELWOOD UNION FREE SCHOOL DISTRICT
Report on Information Technology
For the Fiscal Year Ended June 30, 2025

Recommendation: We recommend the District implement enhanced physical security controls for its server room, including:

- Installing surveillance cameras to monitor all entry points and the interior of the server room.
- Implementing an access logging mechanism (e.g., keycard system or sign-in protocol) to record and review physical access to the area.
- Developing procedures for periodic review of access logs and video footage, with access limited to authorized personnel only.

AREA: USER ACCESS CONTROLS

Overview: Employees are assigned role-based access controls based on the job responsibilities and duties. The District reviews user account permissions to ensure inactive or terminated employees are removed from the system timely. Each user has their own set of login credentials secured by password in accordance with District policy.

Procedures Performed:

- Verified administrative privileges are restricted to IT personnel.
- Reviewed policies and procedures included in the District's Disaster Recovery Plan, which was most recently updated in January 2025.
- Reviewed active user accounts in the District's network (those individuals with District email addresses) and compared to a selection of twenty (20) employees terminated from the District between July 1, 2023 through June 30, 2025 to ensure that no terminated employees remain as active users.
- Reviewed a listing of current District employees and compared to a selection of forty (40) active user accounts to ensure that user accounts are appropriately associated with a current employee.
- Assessed whether automated alerts are in place to notify IT personnel of suspicious login activity (e.g., logins from unknown devices or unusual locations).
- Assessed whether system logs are reviewed to determine if unauthorized login attempts were detected.
- Reviewed permissions within *nVision* (the District's accounting information system) to ensure that permissions for individuals with journal entry, budget transfer, cash receipt, and requisition/purchase order permissions are appropriate based on their respective job functions/titles.
- Inquired with the District regarding policies and procedures around the deactivation of user accounts when employees are terminated from the District.

Observation: We noted that workstation timeout settings were not enforced for District users at the time of our audit work. However, per discussion with District personnel, we noted that the new devices being deployed by the District have a timeout threshold of 45 minutes for teachers and 10 minutes for clerical.

ELWOOD UNION FREE SCHOOL DISTRICT
Report on Information Technology
For the Fiscal Year Ended June 30, 2025

Recommendation: We recommend that the District implement centrally managed timeout settings through tools such as Group Policy or Mobile Device Management (MDM) systems to ensure consistent enforcement across all user devices.

AREA: BACKUP AND DISASTER RECOVERY

Overview: Backup and disaster recovery are designed to ensure the availability and integrity of critical IT systems and data in the event of a cyberattack, system failure, or natural disaster. The District maintains regular data backups, stored in a secure cloud environment.

Procedures Performed:

- Reviewed published Board policies to ensure the District's data backup and disaster recovery process is documented, conforms with District policies as well as applicable regulatory requirements, and accurately reflects the current operations of the District.
- Verified the District conducts back-ups for critical systems and data.
- Verified backup information is stored in cloud-based software.
- Verified whether the District performs recovery tests periodically during the year.
- Verified that the disaster recovery plan is updated and reviewed to reflect current operations of the District.

Observation: We noted the District currently does not perform regular testing of its Disaster Recovery Plan or conduct system integrity tests to verify the effectiveness of IT system restoration in the event of a failure. We did note however that the District is in the process of implementing enhanced infrastructure designed to incorporate multiple layers of redundancy, high availability, and recovery capabilities. Additionally, disaster recovery testing is planned for later in the year.

Recommendation: We recommend the District implement a structured disaster recovery testing schedule that includes the following:

- Full-system recovery drills to validate the restoration process.
- Backup integrity testing to ensure data recovery procedures work correctly.
- Failover and redundancy tests to confirm that secondary systems (e.g., cloud backups) activate as intended.

AREA: IT ASSET MANAGEMENT

Overview: The District's IT department maintains an inventory of IT hardware assets that includes information regarding the asset type, asset tag number, and location to ensure the tracking and safeguarding of IT assets.

ELWOOD UNION FREE SCHOOL DISTRICT
Report on Information Technology
For the Fiscal Year Ended June 30, 2025

Procedures Performed:

- Reviewed the IT asset inventory listing as of January 25, 2025 to assess accuracy, completeness, and proper classification of assets.
- Obtained evidence of Board of Education approval as per District policy for IT assets deemed obsolete.

Observation: We noted that several items on the District's IT inventory listing did not include asset purchase dates. We did note however that the District transitioned to Incident IQ for tracking IT hardware recently and is currently in the process of reviewing and updating inventory accuracy as a continuation of the transition process.

Recommendation: We recommend the District continue to assess the accuracy of inventory listed in Incident IQ tracking software and update as needed.

AREA: INCIDENT RESPONSE AND CYBERSECURITY MONITORING

Overview: The District has procedures for identifying, containing, and mitigating cybersecurity incidents, such as data breaches, ransomware attacks, and unauthorized access. Automated cybersecurity monitoring tools, including intrusion detection systems (IDS), firewalls, and security logs, help detect and respond to threats in real time. IT staff receive alerts for suspicious activities.

Procedures Performed:

- Reviewed published Board policies to ensure the District's process is documented, conforms with District policies, as well as applicable regulatory requirements, and accurately reflects the current operations of the District.
- Verified the District has a written incident response plan.
- Verified whether the District retains a log of cybersecurity incidents and periodically reviews the log to identify potential trends.
- Verified the District has implemented endpoint detection and response software on the District's devices.
- Determined whether the District performs simulated phishing attacks to test employee awareness.

Observation: No exceptions noted.

Recommendation: No recommendations noted.

ELWOOD UNION FREE SCHOOL DISTRICT

**Report on Information Technology
For the Fiscal Year Ended June 30, 2025**

CORRECTIVE ACTION PLAN

The District is required to prepare a corrective action plan in response to any observations contained in the internal audit reports. As per Commissioner's Regulations §170.12, a corrective action plan, which has been approved by the Board, should be submitted to the State Education Department within 90 days of the receipt of a final internal audit report.

The approved corrective action plan and a copy of the respective internal audit report should be submitted using the NYSED Business Portal.