New York State Comptroller
THOMAS P. DiNAPOLI

Sewanhaka Central High School District

Information Technology Contingency Planning

2023M-12 | June 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Sewanhaka Central High School District

Audit Objective

Determine whether Sewanhaka Central High School District (District) officials developed an information technology (IT) contingency plan to help secure and protect business office IT systems in the event of a disruption or disaster.

Key Findings

District officials did not develop an IT contingency plan to help them adequately secure and protect business office IT systems in the event of a disruption or disaster.

Without a comprehensive written IT contingency plan in place that is properly distributed to all business office staff and periodically tested for efficacy, District officials have less assurance that employees and other responsible parties will react quickly and effectively to maintain business continuity. As a result, important financial and other business office data could be lost or suffer a disruption to operations.

Additional sensitive IT control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Develop, adopt and test a written IT contingency plan and communicate it to appropriate officials and employees.

District officials agreed with our findings and have initiated or plan to initiate corrective action.

Background

The District is located in the Town of Hempstead in Nassau County and provides educational services to students in grades 7-12 from its four elementary school districts: Elmont Union Free School District (UFSD), Floral Park-Bellerose UFSD, Franklin Square UFSD and New Hyde Park-Garden City Park UFSD.

The District is governed by the Board of Education (Board), which is composed of eight appointed members. Each UFSD board annually appoints two of its elected members to serve on the District's Board for one year. The Board is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction. The Coordinator of Classroom Instructional Technology and Student Achievement (Coordinator) is responsible for oversight of the District's IT systems.

Quick Facts	
Student Enrollment	8,100
Employees	700
Business Office Computers	53

Audit Period

July 1, 2021 – December 7, 2022

IT Contingency Planning

How Does an IT Contingency Plan Help Secure and Protect Business Office IT Systems?

To help minimize the risk of data loss or suffering a serious interruption of services in the event of an unexpected IT disruption or disaster, a board and school district officials should develop and adopt a comprehensive written IT contingency plan. An IT contingency plan is a school district's recovery strategy, composed of the procedures and technical measures that help enable the recovery of business office operations after an unexpected IT disruption or disaster. The plan should address the potential for sudden, unplanned disruptions (e.g., system failure caused by an inadvertent employee action, power outage, ransomware or other type of malware infection or a natural disaster such as a flood or fire) that could compromise the IT systems within the business office and the availability or integrity of the school district's business office IT systems and the data contained therein, including any personal, private and sensitive information (PPSI).[1] This is particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks.

The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the school district's computerized operations and IT environment. Proactively anticipating and planning for IT disruptions helps prepare personnel for the actions they must take in the event of an incident. The goal of an IT contingency plan is to help enable the recovery of an IT system and/or the electronic data contained therein as quickly and effectively as possible following an unplanned disruption.

The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of business office IT system hardware, applications, data and connectivity. Backup policies and procedures are also critical components and help ensure that information is routinely backed up and available in the event of a disruption.

The IT contingency plan can also include, among other items deemed necessary by school district officials, the following:

- Roles and responsibilities of key personnel,
- Periodic training regarding the key personnel's responsibilities,
- Identifying and prioritizing critical business office processes and services,
- Communication protocols with outside parties,

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or use - or disruption of access or use – could have a severe impact on critical functions, employees, students, third parties or other individuals or entities.

- Technical details concerning how business office IT systems and data will be restored,
- Resource requirements necessary to implement the plan,
- Backup procedures and storage policies,
- Details concerning how the plan will be periodically tested, and
- Reviewing and revising the plan to ensure that it meets the school district's needs.

District Officials Did Not Develop an Adequate IT Contingency Plan

The District did not have a comprehensive IT contingency plan to describe how officials would respond to potential disruptions and disasters affecting the District's IT systems within the business office. Although the Board adopted a written disaster recovery plan (DRP) in October 2009, it did not address the range of threats to the District's business office IT systems. Also, the DRP does not focus on sustaining critical business functions during and after a disruption. While the DRP details the recovery steps to restore service to the network, it does not reflect the District's current IT environment. The DRP does not give specific details to restore operations, such as what resources are needed to recover its business office IT systems and the roles and responsibilities of key individuals in the event of an emergency. In addition, District officials and staff were not trained on what to do in the event of a potential disruption or disaster and did not test procedures to ensure that employees, IT vendors and all other responsible parties understood their roles and responsibilities if business office IT systems were compromised.

Consequently, in the event of a disruption or disaster, such as a ransomware attack (a type of malicious software designed to block access to a computer system until a sum of money is paid) or other malware infection, responsible parties have insufficient guidance to help resume, restore or repair and/or rebuild essential operations in a timely manner. Without an IT contingency plan, there is an increased risk that the District could lose important business office data and/or suffer a serious interruption to business office operations, such as not being able to process checks to pay vendors or employees.

The Coordinator said that the District has actively taken steps to ensure data continuity within its new IT environment, hardware redundancy efforts and backup procedures. However, the Coordinator acknowledged that these efforts were not adequately documented in a single IT contingency plan.

Without a comprehensive IT contingency plan in place that all responsible parties have been trained on and that is periodically tested for effectiveness, District officials have less assurance that employees and other responsible parties will react quickly and effectively to maintain business continuity. In addition, officials cannot ensure the recovery of necessary data to continue operations if a system malfunction or other disruption occurs. IT disruptions can occur unexpectedly. As a result, important financial and other data could be lost, or the District could suffer a disruption to operations that depend on its computerized environment.

What Do We Recommend?

The Board and District officials should:

1. Develop, adopt and test a written IT contingency plan that includes detailed guidance for continuing operations, key personnel and procedures for recovery of business office IT system operations.

Appendix A: Response From District Officials

S·C·H·S·D
SEWANHAKA
CENTRAL HIGH SCHOOL DISTRICT

Central Administrative Offices
77 Landau Avenue, Floral Park, NY 11001-3603

Unit Name: Sewanhaka Central High School District
Audit Report Title: Information Technology Contingency Planning
Audit Report Number: 2023M-12

Audit Response:

The Sewanhaka Central High School District agrees with the findings of the "Information Technology Contingency Planning" audit that we received on June 5, 2023. While we had internal knowledge, processes, and procedures in place to help us secure our systems in the event of disruption, our written IT contingency plan is deserving of attention and focus. This response is also serving as our Corrective Action Plan.

Corrective Action Plan:
For each recommendation included in the audit report, the following is our corrective action(s) taken and proposed.

Audit Recommendation:
Develop, adopt and test a written IT contingency plan and communicate it to appropriate officials and employees.

Implementation Plan of Action:
On March 28, 2023, the Board of Education adopted an amended Data Disaster Recovery Policy (3562) to enhance our information technology contingency planning. Moving forward, the Director of Classroom Instructional Technology will collaborate with his team and the school attorney to develop, adopt, and test an enhanced written IT contingency plan. The plan will include roles and responsibilities of key personnel, recommendations for periodic training, a focus on specific processes, and systems that need to be prioritized in the event of a service interruption. Details will include communication protocols and technical details on how systems will be restored.

Moving forward, after initial implementation the plan will be regularly reviewed and amended as needed.

Implementation Date:
It is our goal to have this process begin in July 2023 and a written plan completed ASAP and no later than October 2023.

Person Responsible for Implementation:
Director of Classroom Instructional Technology & Student Achievement

Signed:

Michael Jaime, Board of Education President

6/20/23
Date

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 the Coordinator and IT staff to gain an understanding of the District's IT environment.
- We inquired about and reviewed IT policies and procedures to determine whether the District had an adequate IT contingency plan and reviewed the District's existing DRP.
- We focused our audit work within the business office because the vast majority of business-related work (as opposed to instructional work) includes PPSI and other sensitive data that flowed through the District's business office.

Our audit also examined the adequacy of certain sensitive 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/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

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

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/files/local-government/publications/pdf/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

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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties