QUESTAR III
PUTTING STUDENTS FIRST

Hyde Park Central School District:

FY 2021/22 IT Data Security Audit - Final

www.questar.org

QUESTAR III
PUTTING STUDENTS FIRST

September 20, 2022

Board of Education
Hyde Park Central School District
11 Boice Road
Hyde Park, New York 12538

We have completed the annual testing of controls for the Hyde Park Central School District. One of the requirements of the 2005 School Financial Oversight and Accountability legislation is ongoing testing and evaluation of the district's internal controls. Our engagement was designed to evaluate the adequacy of internal controls over the IT Data Security processes to ensure they are appropriately designed and operating effectively and efficiently. And, to provide a report with recommended changes for strengthening controls and reducing identified risks.

The purpose of the audit was to review the internal controls that the district has in place to prevent errors, detect fraud and ensure that financial reporting is accurate and that the district assets are safeguarded.

RELIABILITY OF INFORMATION

In performing our engagement, we obtained a sample from the population of employee acceptable user agreement signoffs to test the accuracy and reliability of information provided by district personnel.

As noted, the purpose of our engagement was to assist you in improving the process by which you monitor and manage the risks that face the district. Any findings and recommendations in the attached report are the responsibility of the district to implement, accept the risk as identified, or implement alternative controls that will mitigate the risk to a level that is acceptable by the district. Ultimately, it is your responsibility to assess the adequacy of your risk management system.

DISTRIBUTION OF THE REPORT

This report is intended solely for the information and use of the Board of Education and management of the Hyde Park Central School District and should not be used for any other purpose.

We appreciate the opportunity to serve you and thank the individuals in your organization for their cooperation. Over time, it will be necessary to reassess your risks to ensure that they have not changed and to ensure that your risk management system is functioning properly. Through our ongoing involvement with you as a client and our knowledge of your district and its processes, we are in a unique position to assist you with that process. Please contact us at any time should you desire such services.

Sincerely,

Mark Beaudette

Mark Beaudette
Internal Audit Manager
Questar III

Executive Summary

Objectives and Scope

The Hyde Park Central School District asked us to examine the District's policies and procedures over IT Data Security. Key objectives included evaluating the internal controls established by the District and evaluating compliance with Data Security related Board policies.

The audit covered systems and controls in effect through March 18, 2022. Our fieldwork concluded on March 25, 2022.

Acknowledgements

We would like to thank the staff of the Hyde Park Central School District for their courteous and prompt assistance during our audit.

Conclusion

Eight observations were noted and are summarized below. Our recommendations are detailed in the report.

Reference	Observation	Risk
1	Inconsistent Acceptable Use Agreement Collection	🟡 Medium
2	Instances of eSchool Accounts not Deactivated	🟡 Medium
3	Instances of Frontline IEP Direct Accounts not Deactivated	🟡 Medium
4	No Annual Personally Identifiable Information Training	🟡 Medium
5	Instances of nVision Accounts not Deactivated	🟢 Low
6	Instances of Nutrikids Accounts not Deactivated	🟢 Low
7	Inconsistent Rules Over Password Changes, Complexity	🟡 Medium
8	Requirement to Publish Supplemental Information	🟢 Low

ENTITY NAME	**Hyde Park Central School District**
REPORT DATE	March 25, 2022
PROCESS REVIEWED	IT Data Security
PERSONNEL INTERVIEWED	Dr. Gregory Brown, Deputy Superintendent/Data Protection Officer Richard Wert, Director of Technology Services Therese McKenna, Network Support Specialist Michele Besnier; Secretary III IT Department Other District Staff, as Needed
SCOPE OF WORK	Reviewed the District's data security practices, policies and controls in place, conducted interviews with relevant staff members and performed the following testing procedures: • Selected a sample of 50 employees from a population of 907 with network system credentials for the purpose of evaluating whether staff sign-off on a hard copy Acceptable Use Agreement. • Reviewed the list of Incomplete Status' from the Global Compliance Network's compilation of employee sign-off of District policies. • Examined the entire population of 703 Frontline IEP Direct active user accounts to determine if they were associated with current employees or were from an outside provider that had a valid purpose for having an account. • Examined the entire population of 679 eSchool active user accounts to determine if they were associated with current employees. • Examined the entire population of seven Versatrans active user accounts to determine if they were associated with current employees. • Examined the entire population of 37 Nutrikids active user accounts to determine if they were associated with current employees. • Examined the entire population of 63 nVision system active user accounts to determine if they were associated with current employees. • Reviewed the District's requirements for changing system passwords as well as requirements for password complexity.
SCOPE RESTRICTIONS	None noted.
AUDIT OBJECTIVES	To evaluate the internal controls established by the District over data security to ensure they are operating effectively and efficiently.

KEY PROGRAM CONTROLS

The District has created the following key program controls designed to meet business obligations, provide accountability, and promote operational effectiveness and efficiencies:

- The District has established Board of Education policies 4526 Acceptable Use of Technology, 4526.1 Internet Safety, 5500 Student Records, 5550 Student Privacy, 5500-E Student Records Exhibit and Board Regulations 4526R Acceptable Use of Technology Regulation, 4526.1R Internet Safety Regulation and 5500R Student Records Regulation to provide guidance over the Data Security processes.
- The District utilizes an Acceptable Use of Technology Consent and Waiver for Staff from to document employee acceptance of the Hyde Park Central School District Acceptable Use Policy. The District collects a signed paper copy from employees at the start of employment. The District also asks employees to sign off electronically on a number of policies that include 4526 Acceptable Use of Technology as part of the Opening Day Packet.
- The District requires all vendors that have any contact with Personally Identifiable Information (PII) to sign a data sharing agreement, which includes all elements from the Parents' Bill of Rights.
- The District subscribes to a service provided by Dutchess BOCES that helps the District manage data privacy issues.
- The District uses the eSchoolData which is a student data management system to store student and parent contact information as well as attendance, grades and report card information. eSchool includes a parent portal that allows parents/guardians to access their child(ren)'s data online.
- The District utilizes Frontline IEP Direct which is a web-based software program designed to create and maintain the student's Individualized Education Program (IEP) and the provider's session notes.
- The District utilizes school bus routing software from Versatrans which contains student PII. The District plans to discontinue use of this later in the 2021-22 school year and move to the EZRouting system.
- The District utilizes the Nutrikids system from Heartland School Solutions which is an automated school meal account management system that contains student PII. The District plans to discontinue use of this later in the 2021-22 school year and move to the Titan system.
- The District utilizes the nVision system by Finance Manager to host the accounting system and process payroll and accounts payable. This system houses employee PII.

OBSERVATIONS AND RECOMMENDATIONS

Observation 1: From the sample of 50 active employee network accounts, we noted that for 35 accounts where the District could not provide a signed Acceptable Use Agreement in accordance with Board policy 4526 which reads in part, "The District also requires that every staff member sign an Acceptable User of Technology Policy form located on the website annually." It should be noted that the District also requires employees to read and sign off that they have read a group of District policies on an annual basis as part of the Global Compliance Network training modules. These policies include the Acceptable User of Technology Policy. As of the time of the audit there were listed 261 employees that had not yet completed the electronic sign-off. Most of these were still on the active employee list. The majority of these instances were substitutes.

Recommendation: The District should make a determination whether they require the paper document policy sign-off, the electronic version, or both. The District should then create a method to ensure that all staff members complete the necessary requirements. A staff person should be assigned to follow-up to ensure that all employees have complied with the District policy.

Observation 2: Of the 679 active accounts in eSchool, 58 were accounts that no longer had a valid reason to be open and should have been closed. Additionally, there were 74 accounts that were duplicates. Several District officials stated that the oversight to terminate accounts in a timely manner is often the result of inconsistent communication relating to on-boarding and off-boarding of employees.

Recommendation: The District should review the process to terminate system access to eSchool when employees leave the District. Additionally, a person should be assigned to review the access list periodically and make the appropriate edits. The need, if any, for duplicate accounts should be defined. Those duplicates deemed unnecessary should be deleted.

Observation 3: Of the 703 active accounts in Frontline IEP Direct, 37 were accounts that no longer had a valid reason to be open and should have been closed. Additionally, there were 46 accounts that were duplicates.

Recommendation: The District should review the process to terminate system access to Frontline IEP Direct when employees leave the District. Additionally, a person should be assigned to review the access list periodically and make the appropriate edits. The need, if any, for duplicate accounts should be defined. Those duplicates deemed unnecessary should be deleted.

Observation 4: The District does not currently have in place a program to annually train employees on data privacy and security awareness. New York Education Law 2d Part 121 reads, in part "Educational agencies shall annually provide data privacy and security awareness training to their officers and employees with access to personally identifiable information. Such training should include but not be limited to training on the state and federal laws that protect personally identifiable information, and how employees can comply with such laws. Such training may be delivered using online training tools and may be included as part of training the educational agency already offers to its workforce."

Recommendation: The District should develop a comprehensive cybersecurity training program that would be available to all instructional and non-instructional employees. The training should include but not be limited to training on the state and federal laws that protect personally identifiable information. The District should ensure all staff participate in the training, which can be tracked by user accounts. In addition, the District should consider adding this as part of professional development at the beginning of the school year.

Observation 5: Of the 63 active accounts in the nVision system, nine were accounts that no longer had a valid reason to be open and should have been closed. Users in nVision don't all have access to PII; however, the auditor noted some names that would have had access to employee payroll information. District officials stated that they believe they communicated a request to terminate some of these accounts to the Mid-Hudson Regional Information Center (MHRIC).

Recommendation: The District should review the process to terminate system access to nVision when employees leave the District. Additionally, a person should be assigned to review the access list periodically and follow up with the MHRIC when necessary.

Observation 6: Of the 37 active accounts in Nutrikids, two were accounts that no longer had a valid reason to be open and should have been closed.

Recommendation: The District should review the process to terminate system access to Nutrikids when employees leave the District. Additionally, a person should be assigned to review the access list periodically and make the appropriate edits.

Observation 7: Several of the systems that contain PII in the District do not have consistent practices in place over user passwords. The Nutrikids system does not require password changes, nor does it require the password to contain any particular complexity. The District plans to move the food service management system to Titan systems by year-end which will allow the District to choose how often passwords are

	changed and what their complexity should be. The Versatrans system also does not require password changes, nor does it require the password to contain any particular complexity. The District plans to move the transportation module to the EZRouting system by the end of the 2021-22 year. Frontline IEP Direct does not force users to change their password, although users can change the password voluntarily. The eSchool system does not currently require any password changes. The District's use of Google accounts for e-mail and other applications hasn't requested users to change passwords since 2020; prior to that an annual change was required. *Recommendation: The District should determine what the practice should be for changing system passwords and then design a program to enforce compliance. The District should also attempt to institute uniform rules governing password complexity. Any changes could be incorporated in the setup of the new EZRouting and Titan systems.* Observation 8: At the time of the audit the District was only partially compliant with the requirement to publish supplemental vendor information, as this was not currently available for every vendor the District utilizes that receive PII. Ed Law 2-d §121.3d reads, in part, "Each educational agency shall publish on its website the supplement to the Bill of Rights for any contract or other written agreement with a third-party contractor that will receive personally identifiable information." *Recommendation: The District should complete and update its website for all third-party contractors within the scope of Ed Law 2-d §121.*
SUBMITTED BY:	Mark Beaudette, Internal Auditor
DATED:	March 25, 2022

HYDE PARK CENTRAL SCHOOL DISTRICT
Administration Offices: P.O. Box 2033, Hyde Park, New York 12538-8033
Telephone: (845) 229-4000
www.hpcsd.org

Aviva Kafka
Superintendent of Schools

Gregory S. Brown, Ed.D. Deputy Superintendent Phone: 845-229-4008	***Linda Steinberg*** Assistant Superintendent for Finance & Operations Phone: 845-229-4009

MEMO

Technology Department

To: Board of Education

From: Richard Wert, Director of Technology

C: Aviva Kafka, Superintendent of Schools
Gregory Brown, Deputy Superintendent
Linda Steinberg, Assistant Superintendent for Finance & Operations
Mark Beaudette, Internal Auditor

Date: September 13, 2022

Re: Corrective Action Plan for the 2021-2022 Internal Audit

The following are our suggestions for corrective action based on recommendations in the internal auditors' 2021-2022 report.

Observation 1: *From the sample of 50 active employee network accounts, we noted that for 35 accounts where the District could not provide a signed Acceptable Use Agreement in accordance with Board policy 4526 which reads in part, "The District also requires that every staff member sign an Acceptable User of Technology Policy form located on the website annually." It should be noted that the District also requires employees to read and sign off that they have read a group of District policies on an annual basis as part of the Global Compliance Network training modules. These policies include the Acceptable User of Technology Policy. As of the time of the audit there were listed 261 employees that had not yet completed the electronic sign-off. Most of these were still on the active employee list. The majority of these instances were substitutes.*

<u>Internal Auditor Recommendation:</u>

The District should make a determination whether they require the paper document policy sign-off, the electronic version, or both. The District should then create a method to ensure that all staff members complete the necessary requirements. A staff person should be assigned to follow-up to ensure that all employees have complied with the District policy.

<u>Corrective Action Plan:</u>

All new hires of the Hyde Park Central School District will sign paper copies of the Acceptable Use Policy during their orientation with Human Resources. Each year, all employees will sign off on an electronic version of the Acceptable Use Policy as part of the district's annual mandatory training (Global Compliance Network Training). This process will be implemented by 7/1/22. The responsible administrator for new hires is Shelby Outwater, Director of Equity and Human Resources. Ms. Outwater will follow up with employees that have not complied with the District Policy and notify their supervisors of noncompliance. The responsible administrator for existing staff is Rick Wert, Director of Technology. Mr. Wert will inform supervisor if their staff have not completed the annual requirement by October each year. This process will be implemented by October 31, 2022.

<u>Observation 2</u>: Of the 679 active accounts in eSchool, 58 were accounts that no longer had a valid reason to be open and should have been closed. Additionally, there were 74 accounts that were duplicates. Several District officials stated that the oversight to terminate accounts in a timely manner is often the result of inconsistent communication relating to on-boarding and off-boarding of employees.

<u>Internal Auditor Recommendation</u>*:*

The District should review the process to terminate system access to eSchool when employees leave the District. Additionally, a person should be assigned to review the access list periodically and make the appropriate edits. The need, if any, for duplicate accounts should be defined. Those duplicates deemed unnecessary should be deleted.

<u>Corrective Action Plan:</u>

The Human Resources department will create an off-boarding work-order ticket for all employees that separate from the district. The Technology Department will remove access to E-School Data, effective the date of separation.

Duplicate accounts are necessary for teachers that are assigned to multiple buildings. The Technology Department will perform periodic audits of user access to determine if any duplicate accounts are unnecessary.

Director of Equity and Human Resources, Shelby Outwater will be responsible for reporting employee separations to the Technology Department. Director of Technology, Richard Wert, will be responsible for ensuring that access is removed from employees that should no longer have access and for removing unnecessary duplicate accounts. This process will be implemented by 7/1/2022.

Observation 3: Of the 703 active accounts in Frontline IEP Direct, 37 were accounts that no longer had a valid reason to be open and should have been closed. Additionally, there were 46 accounts that were duplicates.

Internal Auditor Recommendation:

The District should review the process to terminate system access to Frontline IEP Direct when employees leave the District. Additionally, a person should be assigned to review the access list periodically and make the appropriate edits. The need, if any, for duplicate accounts should be defined. Those duplicates deemed unnecessary should be deleted.

Corrective Action Plan:

The Human Resources department will create an off-boarding work-order ticket for all employees that separate from the district. The Special Education Department will remove access to IEP Direct, effective the date of separation.

The Special Education department will perform periodic audits of user access to determine if any accounts should be deactivated.

Director of Equity and Human Resources, Shelby Outwater will be responsible for reporting employee separations to the Technology Department. Assistant Superintendent, Melissa Lawson, will be responsible for ensuring that access is removed from employees that should no longer have access to Frontline IEP Direct. This process will be implemented by 7/1/2022.

Observation 4: The District does not currently have in place a program to annually train employees on data privacy and security awareness. New York Education Law 2d Part 121 reads, in part “Educational agencies shall annually provide data privacy and security awareness training to their officers and employees with access to personally identifiable information. Such training should include but not be limited to training on the state and federal laws that protect personally identifiable information, and how employees can comply with such laws. Such training may be delivered using online training tools and may be included as part of training the educational agency already offers to its workforce.”

Internal Auditor Recommendation:

The District should develop a comprehensive cybersecurity training program that would be available to all instructional *and non-instructional employees. The training should include but not be limited to training on the state and federal laws that protect personally identifiable information. The District should ensure all staff participate in the training, which can be tracked by user accounts. In addition, the District should consider adding this as part of professional development at the beginning of the school year.*

Corrective Action Plan:

All staff will be trained in data privacy and protection by 6/30/2023 using the GCN portal module. The Director of Technology, Rick Wert, is the responsible administrator.

All staff will be subjected to the InfosecIQ phishing tests by 6/30/2023. Remediation lessons will be provided to those that fail. The Director of Technology, Rick Wert, is responsible for implementing this plan.

Observation 5: Of the 63 active accounts in the nVision system, nine were accounts that no longer had a valid reason to be open and should have been closed. Users in nVision don't all have access to PII; however, the auditor noted some names that would have had access to employee payroll information. District officials stated that they believe they communicated a request to terminate some of these accounts to the Mid-Hudson Regional Information Center (MHRIC).

Internal Auditor Recommendation:

The District should review the process to terminate system access to nVision when employees leave the District. Additionally, a person should be assigned to review the access list periodically and follow up with the MHRIC when necessary.

Corrective Action Plan:

The business office will submit requests to disable permissions to nVision to the Ulster BOCES Mid-Hudson Regional Information Center based on information provided in the personnel agendas. Additionally, a periodic review will be performed to determine if there are any active accounts for individuals that should no longer have access to nVision. The Assistant Superintendent for Finance & Operations is responsible for implementing this plan by 6/30/2022.

Observation 6: Of the 37 active accounts in Nutrikids, two were accounts that no longer had a valid reason to be open and should have been closed.

Internal Auditor Recommendation:

The District should review the process to terminate system access to Nutrikids when employees leave the District.

Additionally, a person should be assigned to review the access list periodically and make the appropriate edits.

Corrective Action Plan:

The food office will remove permissions to Nutrikids as food service employees leave the district. Additionally, a periodic review will be performed to determine if there are any active accounts for individuals that should no longer have access to Nutrikids. The Director of Nutrition Services is responsible for implementing this plan by 6/30/2022.

Observation 7: Several of the systems that contain PII in the District do not have consistent practices in place over user passwords. The Nutrikids system does not require password changes, nor does it require the password to contain any particular complexity. The District plans to move the food service management system to Titan systems by yearend which will allow the District to choose how often passwords are changed and what their complexity should be. The Versatrans system also does not require password changes, nor does it require the password to contain any particular complexity. The District plans to move the transportation module to the EZRouting system by the end of the 2021-22 year. Frontline IEP Direct does not force users to change their password, although users can change the password voluntarily. The eSchool system does not currently require any password changes. The District's use of Google accounts for e-mail and other applications hasn't requested users to change passwords since 2020; prior to that an annual change was required.

Internal Auditor Recommendation:

The District should determine what the practice should be for changing system passwords and then design a program to enforce compliance. The District should also attempt to institute uniform rules governing password complexity. Any changes could be incorporated in the setup of the new EZRouting and Titan systems.

Corrective Action Plan:

District administration will determine password characteristics for all district PII-sensitive programs and password reset timetables will be determined for all PII-sensitive titles. All programs that have reset/password complexity settings as part of the system will be enabled. This corrective action will be implemented by January 1, 2023 and the responsible administrator is Director of Technology, Rick Wert.

Observation 8: At the time of the audit the District was only partially compliant with the requirement to publish supplemental vendor information, as this was not currently available for every vendor the District utilizes that receive PII. Ed Law 2-d §121.3d reads, in part, "Each educational agency shall publish on its website the supplement to the Bill of Rights for any contract or other written agreement with a third-party contractor that will receive personally identifiable information."

Internal Auditor Recommendation:

The District should complete and update its website for all third-party contractors within the scope of Ed Law 2-d §121.

Corrective Action Plan:

All district software/subscriptions that collect PII will be listed on the district website and will include links to title privacy policies, and 2D compliance statements. This will be completed by December 31, 2022 and the responsible administrator is Director of Technology, Rick Wert.