Northport-East Northport UFSD
Annual Risk Assessment
For the period ending December 31st 2018
Corrective Action Plan

Risk Assessment Report
Nawrocki Smith LLP

Findings & Recommendations	**District's Response**	**Responsible Staff Member**	**Status**
<u>Observation #1</u> It was represented that the District has not established a formal review process of the invoices billed and status of accounts receivable for out of district tuition and COBRA insurance. **<u>Recommendation #1</u>** The District should assign a second individual to review the accuracy of out of district tuition and COBRA insurance bills. The review process should include a verification that the invoice amounts agree to the source documents. The individual responsible for reviewing the invoices should also ensure that gaps in invoice numbers are tracked and noted so as to prevent duplicate billings and lost invoices.	**Response:** The Senior account clerk in the business office will be the second individual reviewing out of district tuition and COBRA insurance bills.	Business Office	Completed
<u>Observation #2</u> The Payroll Office does not maintain annual salary notices supporting the rate of pay for each employee for each fiscal year.	**Response:** The Human Resources office currently has an initial salary letter in every employees file.	Human Resources Office	Completion target: December 31st 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
Recommendation #2 The District should explore the capabilities of the nVision application to issue an annual salary notice to all employees indicating their respective earnings for each current fiscal year. A copy of the employee salary notice should be provided to the employee to sign indicating his/her acknowledgment and a copy should be maintained in the employee's file. When a formal process exists to document authorized salaries and applicable changes, the opportunity for fraudulent or erroneous payroll changes to occur without detection decreases.	HR will print out and acquire signed salary letters on an annual basis and file.		
Observation #3 The District has established a process to evaluate instructional employees electronically through StaffTrack in accordance with APPR guidelines. It was presented that the District utilizes paper forms to document formal evaluations for non-instructional employees. It should be noted that formal annual evaluation results are reviewed and signed by each individual employee, as required by the employment agreements, and copies are maintained on file.	**Response:** The district will review the cost/benefit of electronic vs paper evaluations for non-instructional staff.	Human Resources Office	Completion target: September 1st 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
Recommendation #3 The District should explore the cost-benefit options of conducting evaluations for non-instructional staff on an electronic platform. This will assist the Human Resource Department in standardizing its employee evaluation process in identifying employees' strengths and weaknesses, documenting personnel decisions (including promotions, layoffs, and transfers), and meet legal requirements.			
Observation #4 The District has established a process whereby the request and approval for instructional employees leave days is electronically documented within AESOP. It was represented that the District utilizes paper forms to document the request and approval of leave days for non-instructional employees **Recommendation #4** The District should explore the full capabilities of the employee attendance software, AESOP, and implement a process whereby all employee	**Response:** The district will review the cost/benefit of implementing an electronic attendance and leave system.	Human Resources Office	Completion target: September 1st 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
leave requests and approvals are documented and processed through the existing application. As an alternative, the District should explore the cost-benefit options of implementing the "Employee Self Service Portal" from nVision that will directly communicate with the District's financial application. These controls will assist employees to obtain pre-approval from their building level supervisors for their vacation, personal business, maternity, military, jury duty, extended sick, and conference leave day requests in a consistent manner. These electronic platforms will also assist the District in detecting unapproved leave request and providing effective operating planning.			
<u>Observation #5</u> The District is in the process of developing a formal preventative maintenance schedule for the District's vehicles or equipment. **<u>Recommendation #5</u>** The Facilities Department should finalize its preventative maintenance program to improve the equipment useful life cycle and prevent excessive depreciation or impairments. The preventive maintenance schedule should include the manufacturer's recommended	**Response:** The district agrees with this recommendation and is in the implementation process.	Buildings & Grounds	Completion target: September 1st 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
maintenance for equipment, including any warranty documentation on breakdown or failures, owner's manuals, drawings and installation documents. The preventive maintenance should also include estimated costs for labor hours and applicable supplies to monitor against the actual activity. This will assist in increasing its controls over the timely completion of the scheduled routine service calls and ensure that preventative maintenance inspections are completed in a timely manner.			
<u>Observation #6</u> The District does not conduct physical inspections to verify the accuracy and the existence of assets listed on the property ledger. **<u>Recommendation #6</u>** The District should assign an employee separate from the Business Office and the Department Heads to conduct walk-through observations and verify whether the fixed asset tags are properly affixed to the equipment. The observation function should be conducted on an annual basis and the results should be documented and communicated to the Assistant Superintendent for Business. Any exceptions	**Response:** The district recently conducted a complete asset appraisal and physical inventory with CBIZ. We plan to continue to do a complete physical inventory every 3-5 years and perform periodic spot checks and inventories of larger assets on a yearly basis.	Business Office	Completed

Findings & Recommendations	District's Response	Responsible Staff Member	Status
should be investigated, and corrective action should be implemented in a timely manner.			
Observation #7 The District has developed standardized forms to document the flow of information throughout the buildings, Central Registration Office, Human Resource Department, and the Office of Technology. These forms include but are not limited to the student registration packet, student physical/immunization forms, grade change forms, and new employee checklists. The narratives enclosed with the internal audit report describe the procedures carried out by the Central Registration Office and the Office of Technology regarding the processing and monitoring of student enrollment, student attendance, student performance, and granting user permissions and monitoring user access within the District's student data management system. **Recommendation #7** In addition to the existing forms, the Central Registration Office and Office of Technology should develop documented guidelines regarding the monitoring and auditing of student enrollment, student attendance, student	**Response:** The Office of Technology will add procedures and guidelines for monitoring and auditing of student enrollment, student attendance, student performance, and granting user permissions and monitoring user access within the District's student data management system to its existing Information Technology Guidelines and Procedures manual. The District's Information Technology Guidelines and Procedures manual is reviewed annually in January.	Office of Technology	Completion Target: August 31, 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
performance, and granting user permissions and monitoring user access within the District's student data management system. Procedures should be periodically reviewed to ensure that responsibilities are adequately performed at the District. The narratives and flowcharts attached to the internal audit report should serve as guidance to the District's documented procedures.			
<u>Observation #8</u> During the course of our audit, we noted an area for improvement in regard to the student registration, attendance, and performance of data entry and audit process. The District has not implemented a formal review process of the eSchool audit logs or exception reports in the District's student management database. The lack of review of audit logs is a risk as any unusual or unauthorized activity could become undetected. The District, with the assistance of its BOCES Support for eSchool, should develop a monitoring system including audit logs and exception reports to monitor student registration, attendance, and performance data. **<u>Recommendation #8</u>** Upon development of audit logs to monitor the	**Response:** The Office of Technology with the assistance of its BOCES Support for eSchool, will develop a monitoring system including audit logs and exception reports to monitor student registration, attendance, and performance data and document monitoring procedures in the existing Information Technology Guidelines and Procedures manual, including the designation of an individual, separate from the Central Registration Office, to periodically review the student registration, attendance, and performance information and determine appropriateness.	Office of Technology	Completion Target: August 31, 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
student registration, attendance, and performance information, the District should designate an individual separate from the Central Registration Office to periodically review the student registration, attendance, and performance information and determine appropriateness. Applications normally contain multiple audit logs or exception reports that can be reviewed to ensure individuals are making only authorized changes in the application. These audit logs and exception reports provide a mechanism for individual accountability and for management to reconstruct events, if necessary			
<u>Observation #9</u> We have examined the contents and the format of the "Grade Change Request Form" developed for the middle and high school levels and noted the following: • Teachers are not required to attach supporting documentation to the Grade Change Request Form. • The District does not have a Grade Change Request Form at the elementary level.	**Response:** Principals will require teachers to submit the standardized Change Request Form when requesting a student grade change. The principals will not accept any other forms of requests and will return incomplete forms to the applicable Teacher for re-submission. Principals will inform teachers of this procedural change in September when staff returns from summer recess. The principals or assistant principals will review and sign off on the Student Grade Change Forms and submit the approval to the	School Principals and Assistant Principals	Completion Target: September 30, 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
• We conducted key control testing in the area of student grade changes reported subsequent to closed marking periods at the elementary, middle, and high school levels and noted the following: • Certain student grade changes tested did not have documentation to support the purpose and circumstances of the reported grade changes. • Certain student grade changes tested were requested and processed based on emails or request forms other than the District's standardized "Change Request Form." • Certain grade values as reported on the student grade forms did not agree to the student grade changes entered into eSchool. • Certain student grades were changed subsequent to the marking period from no grade, incomplete, or fail to pass. **<u>Recommendation #9</u>** All Teachers should submit the standardized Change Request Form when requesting a	individuals who have access to eSchool to make changes subsequent to the close of marking periods. These approved Student Grade Change Forms will be retained in the school's main office.		

Findings & Recommendations	**District's Response**	**Responsible Staff Member**	**Status**
student grade change. The Principals should not accept any other forms of requests and should return incomplete forms to the applicable Teacher for re-submission. The Principals should review and sign off on the Student Grade Change Forms and submit the approval to the individuals who have access to eSchool to make changes subsequent to the close of marking periods. This will enhance the controls surrounding the review process of student grade changes.			
<u>Observation #10</u> Based upon the information gathered from the District and our analysis of the user permissions report applicable to the group access rights generated by eSchool, we made the following observations: • Student Registration - It was represented that the data entry and any applicable edits of student registration in eSchool are limited to select individuals and to BOCES Support. Our analysis of the user permissions report indicated that access to data entry and any applicable edits of student registration in eSchool is granted to	**Response:** The Office of Technology will add procedures and guidelines to its existing Information Technology Guidelines and Procedures manual to address the evaluation of user permissions currently assigned to user groups, the development of a process to verify that individual users' access needs are compatible with the rights of the assigned groups, and the revision of permissions or groups as needed.	Office of Technology	Completion Target: August 31, 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
fifty-four (54) groups. • Student Performance - We observed that eighteen (18) users have access to modify student grades in eSchool. However, we noted that ten (10) out of the eighteen (18) users actually made grade modifications during the period analyzed. **<u>Recommendation #10</u>** The Office of Technology should evaluate the user permissions currently assigned to each user group, develop a process to verify that individual users' access needs are compatible with the rights of the assigned groups, and update the permissions or groups as needed. This will ensure that individuals are assigned only those access rights needed to perform their job duties and will minimize the risk of unauthorized student enrollment or grade changes being made.			
<u>Observation #11</u> The District has not established a review process of the employees who have access to enter and exit the District's buildings to the	**Response:** Currently the district is deactivating employees upon separation from the district. As an added layer of security the Security	Human Resources Office / Security Office	Completion target: September 1st 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
employees listed as active in nVision. **<u>Recommendation #11</u>** The District should establish a process of reconciling the cardholder listing from the building access security software to the active employee listing from nVision at the end of each fiscal year and update the cardholder database by inactivating the employees who no longer are employed with the District. This will enhance the internal control over building access and will limit access during normal school operations and sessions to active employees only.	department will review the current access list on a yearly basis to verify all user access is accurate and up to date.		
<u>Observation #12</u> The District has not developed an incident response plan to address breach notification in the event there is a Personal Identifiable Information ("PII") compromise or breach. Without formal written procedures addressing notification of a breach of PII, there is an increased risk that the District may suffer a serious interruption in operations. **<u>Recommendation #12</u>**	**Response:** The District will include an incident response plan to address cybersecurity and breach notification within the Disaster Recovery section of its existing Information Technology Guidelines and Procedures manual. The incident response plan will include a crisis management and communication plan that involves employees/individuals who handle PII incident response and forensics.	Office of Technology	Completion Target: August 31, 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
The District should include within its Disaster Recovery Plan an incident response plan to address cybersecurity and breach notification. The incident response plan should include a crisis management and communication plan that involves employees/individuals who handle PII incident response and forensics, where warranted. This should enable sufficient business continuity in event of a cybersecurity breach.			
Observation #13 The District has not developed training workshops on cybersecurity or how to deal with related incidents. **Recommendation #13** The District should develop and provide periodic cybersecurity awareness training for all employees including new hires, Information Technology Department, and job positions that handle PII. The training should explain the proper rules of behavior for using information technology systems, the insider type of threats from a cybersecurity perspective, and the implications of a cybersecurity breach. The training should also include guidance on the	**Response:** Annually, the District will require all employees, including new hires, and information technology technical support staff to complete training, (for example, Global Compliance Network training module, "Digital Security & Protection") which includes the proper rules of behavior for using information technology systems, the insider type of threats from a cybersecurity perspective, and the implications of a cybersecurity breach, guidance on the use of online applications, mobile devices, and how to respond to phishing or ransomware attacks.	Human Resources	Completion Target: December 31, 2019

Risk Assessment Report Nawrocki Smith LLP			
Findings & Recommendations	**District's Response**	**Responsible Staff Member**	**Status**
use of social media, Bring Your Own Device ("BYOD"), and how to respond to a phishing or ransomware attacks.			