Northport-East Northport UFSD
Information Technology Cycle

For the School Year Ending June 2018
Corrective Action Plan

Initial Risk Assessment Report
Nawrocki Smith LLP

Findings & Recommendations	District's Response	Responsible Staff Member	Status
Findings: Although the District is performing procedures as documented within our enclosed narratives (See Exhibits 1 through 12), the District has not developed documented formal guidelines regarding software and hardware acquisition, information technology inventory management, creating and modifying user accounts, data security, software security, network security, physical security, service continuity, social media accounts, and email security. Information Technology procedures are carried out based upon past practices and verbal guidelines provided by prior and current Administrators. Recommendations: The District should develop documented guidelines and procedures regarding software and hardware acquisition, information technology inventory management, creating and modifying user accounts, data security, software security, network security, physical security, service continuity, social media accounts, and email security. The documented procedures should be reviewed and updated annually to maintain relevance, and reflect regular changes in the information technology environment. The narratives attached to this report should serve	The Information Technology Department will develop the following document manual to support ongoing systems development, maintenance and acquisitions: Northport-East Northport Information Technology Guidelines and Procedures • Software and Hardware Acquisition • IT Inventory Management • Creating / Modifying User Accounts • Data, Email and Software Application Security • Network and Physical Security • Service Continuity / Disaster Recovery • Social Media Accounts	Administrator of Technology	Completion target: January 1, 2019

Findings & Recommendations	District's Response	Responsible Staff Member	Status
as supplemental enclosures to the District's documented procedures.			
Findings: We analyzed the user permission report from Nvision and noted that access to the financial application for one (1) former employee was not disabled. We also noted that one District cabinet member had access to perform data entry and setup parameters in the human resource module. Based on limited information provided to date, we were unable, at this time, to determine whether the District's cabinet members have utilized such permissions. Recommendations: The Information Technology Department should disable the former employee's access to Nvision. The Human Resource Department should notify the Information Technology Department of any employee position changes, including new hires, transfers, and terminations. The user permissions should be limited to each employee's job roles and duties. The Business Office and the Information Technology Department should limit the permissions for the Cabinet members to "view only" for their respective departments. This recommendation will assist the District in minimizing the access of Nvision to the individuals authorized by the Board of Education. The Business Office should periodically review the		Administrator of Technology	Completed

Findings & Recommendations	District's Response	Responsible Staff Member	Status
permissions user account report and verify the appropriateness of user accounts and permissions on an individual employee basis. This recommendation will assist the Business Office in increasing its oversight and controls over its access to the District's accounting system. ***Subsequent to our review, the Information Technology Department took immediate corrective action plan and implemented the above recommendations.***			
<u>Findings:</u> The Information Technology Department is in the process of developing controls to automatically lock the screens of the workstations when no activity has occurred. <u>Recommendations:</u> The Information Technology Department should finalize its logical security controls whereby workstations will automatically lock the screens after a period of inactivity. The Information Technology Department should also require users to log off their account before stepping away from their computers and before they leave for the day. This will ensure that unauthorized users will not access the District's systems and their information. ***Subsequent to our review, the Information Technology Department took immediate corrective action plan and implemented the above recommendations.***		Administrator of Technology	Completed

Findings & Recommendations	District's Response	Responsible Staff Member	Status
Findings: The District does not store backups of the Active Directory at a secured, off-site location. Recommendations: The District should consider the cost/benefits of maintaining off-site backup to allow for a restoration of data even if the original data within District premises is destroyed.	Every month the Information Technology Department will upload the previous month's Veeam backup files to G Suite for Education and/or Microsoft Azure utilizing Cloud storage to maintain limited backup for extreme disaster recovery.	Administrator of Technology	Completion target: October 1, 2018
Findings: The Information Technology Department has not conducted a full interruption test of its data backup and restoration procedures to ensure that the system will perform as intended and that users know how to carry out their duties in the event of a disaster. Recommendations: The Information Technology Department should conduct annual full interruption tests of its data backup and restoration procedures to ensure that the restoration process works as intended and that the Business Office is able to recover data, if needed. As an alternative to the above recommendation, the Information Technology Department should develop a testing schedule of restoration procedures for each critical application and perform such at various times on an annual basis to ensure that the restoration process works as intended and that the Business Office is able to recover data, if needed. District employees and Internal Auditors should	As part of the Service Continuity / Disaster Recovery section of the *Northport-East Northport Information Technology Guidelines and Procedures* document manual, the District will create a schedule for restoration tests of its data backup and systems, including: • Server Restoration (Physical) • Server Restoration (Virtual) • Data Restoration (Files) • Data Restoration (File Structure) • Active Directory Restoration • nVision Server and Data Restoration • SQL Server and Data Restoration • Nutrikids Server and Data Restoration • Transfinder Server and Data Restoration • Switching Config Files • Phone Call Server	Administrator of Technology	Completion target: January 1, 2019

Initial Risk Assessment Report Nawrocki Smith LLP			
Findings & Recommendations	**District's Response**	**Responsible Staff Member**	**Status**
participate during the restoration procedures. The testing results should be documented and communicated to the Assistant Superintendent for Business for review.			