FINDINGS AND RECOMMENDATIONS

FINDING	**CORRECTIVE ACTION**	**RESPONSIBLE PARTIES**
Active Directory passwords for authenticating network and e-mail users are not required to be periodically changed. This leaves user accounts on all systems utilizing *Active Directory* for authentication vulnerable to unauthorized access. It is recommended that the District develop and adopt a password policy to strengthen computer security controls and reduce the risk of unauthorized access. A password policy should include criteria for password length, formation and duration as well as proper password management such as advising network users to never communicate their password by telephone, e-mail or instant messaging.	Adoption of a password policy will be evaluated by the Assistant Superintendent for Instruction and Administration and the Administrator of Technology during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology
The District is not currently utilizing the account lockout feature of *Windows* password security to prevent attackers from brute-force attempts to guess a user's password. It is recommended that the District consider implementing the *Windows* password security account lockout feature to help deter malicious users and certain types of automated attacks from discovering user passwords. A medium security lockout policy would include an account lockout duration of thirty minutes, an account threshold of three to seven invalid logon attempts, and	Implementation of *Windows* password security will be reviewed by the Assistant Superintendent for Instruction and Administration and the Administrator of Technology during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology

an automatic account lockout reset of thirty minutes.		
The District has not enabled the feature within *Windows* that causes a user's workstation to automatically lock out after a specified period of inactivity. If a user does not manually lock their computers before walking away, individuals passing by can have access to files, e-mails or other data that they are not authorized to see. It is recommended that the District implement a security lockout policy and configure the computers to have a password-enabled screen saver initiate after the computer remains idle for a specified amount of time. By requiring a user to enter their password when they return, it minimizes the risk of an unauthorized individual using an active session while the authorized user is away.	Implementation of a security lockout policy will be reviewed by the Assistant Superintendent for Instruction and Administration and the Administrator of Technology during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology
The backup tapes are maintained in the NOC located in the administration building. It is recommended that the District evaluate the available options for the off-site storage of back-up tapes to determine the optimal storage location for ensuring the safety of data.	The Assistant Superintendent for Instruction and Administration and the Administrator of Technology will evaluate available options for off-site storage of back-up tapes during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology
Although the assistant superintendent for business periodically reviews audit trail reports within *Finance Manager* for user activity to identify any activity that appears to be unusual, the review is not documented. The District does not review	The Assistant Superintendent for Business has begun to document audit trail and login/logout reports. Audit trail reports are generated to review the transactions of a particular employee. The final page of the audit trail report is printed, the review is	Assistant Superintendent for Business

the login/logout report within *Finance Manager* to identify users who may be logging into the financial software at unusual times. It is recommended that the District implement procedures whereby the review of audit trails be documented and maintained on file. It is recommended that the District periodically review and document the review of the login/logout report.	documented and the report page is maintained on file. The login/logout report is reviewed to determine if any staff member has logged into the *Finance Manager* system during off-hours. The final page of the report is printed, the review is documented and the report page is maintained on file.	
The District does not require the passwords to *eSchoolData* be changed periodically, which over time increases the risk that an individual's account can be compromised by an unauthorized user. It is recommended that the District require users of *eSchoolData* to periodically change their password to prevent unauthorized access and to reduce the vulnerability of an account being compromised.	Periodic *eSchoolData* password changes will be considered by the Assistant Superintendent for Instruction and Administration and the Administrator of Technology during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology
Although the District performs daily backups, a system restore has not been performed for all applications and backup information is not periodically tested to verify that the information is restorable. It is recommended that the District perform a restore for all applications to verify that information is complete and restorable. If this is not cost effective, the District should implement procedures to periodically test backups to verify that information is restorable in case of a network or application failure.	The Assistant Superintendent for Instruction and Administration and the Administrator of Technology will review the option of a system restore or periodic system backup tests during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting. Last year, the Assistant Superintendent performed a Data Verification Test with Eastern Suffolk BOCES. This test verified that the District's *Finance Manager* data was backed up accurately off-site. The	Assistant Superintendent for Instruction and Administration Administrator of Technology Assistant Superintendent for Business

	results of this test were positive. The Data Verification Test will be performed again this year. The District has recently received an e-mail from Eastern Suffolk BOCES requesting that we set up an appointment within the next few weeks. The night before the Data Verification Test (after all employees have terminated their *Finance Manager* sessions), the Assistant Superintendent for Business generates an Appropriation Status Report. The Assistant Superintendent for Business brings this report to Eastern Suffolk BOCES the next morning. At Eastern Suffolk BOCES, the Assistant Superintendent for Business signs on to the District's backed up *Finance Manager* data base, generates the Appropriation Status Report and verifies that the data is identical.	
The District has not restricted the ability to download or install software on District owned computers including ipads. It is recommended that the District restrict the rights to download or install software to as few individuals as practical. Software additions or changes should be made by the information technology department to ensure that the software works well with the network, it is safe to use and is for business use.	The Assistant Superintendent for Instruction and Administration and the Administrator of Technology will consider restricting the right to download or install software during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology

REQUIRED POLICIES

FINDING	**CORRECTIVE ACTION**	**RESPONSIBLE PARTIES**
Although the District has adopted policy No. 8635, *Information Security Breach and Notification*, the District has not established the appropriate regulations regarding the procedures that are to be followed in the event of a security breach. It is recommended that the District develop and adopt a formal *Information Security Breach and Notification* regulation to include, but not necessarily be limited to, identifying individual(s) responsible for checking for breaches, how often inspection is required to be performed, individuals required to be notified in the event of a breach and procedures currently in place. By having the Board formally adopt this regulation, the District will be in compliance with State Technology Law §208.	The District will consider adopting a formal *Information Security Breach and Notification* regulation during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology District Clerk Board of Education Policy Committee

RECOMMENDED POLICIES

FINDING	**CORRECTIVE ACTION**	**RESPONSIBLE PARTIES**
The District has not developed and adopted a computer controls policy as recommended by the State Comptroller's Office. It is recommended that the District develop and adopt a computer controls policy as recommended by the State	The District will develop and adopt a computer controls policy as recommended by the State Comptroller's Office during the 2012-2013 fiscal year. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology District Clerk Board of Education Policy Committee

Comptroller's Office. This policy should include: segregation of duties, report generation and approval, passwords and permissions, data input, remote access and data backups. The computer controls policy should also include the internal procedures currently in place. The District should review and update its policy on an annual basis to ensure that the District's electronic information integrity has not been compromised and to ensure that the District is in compliance with privacy laws and regulations.		

SERVER ROOMS

FINDING	**CORRECTIVE ACTION**	**RESPONSIBLE PARTIES**
The District has not implemented procedures for monitoring server room access to ensure that the network and its components have been protected at the physical level. It is recommended that the District perform a cost benefit analysis of installing a video surveillance camera. The camera should be placed in a location that makes it difficult to tamper with or disable but provides a view of individuals entering and leaving, and should be used to supplement an access log book or electronic access system. Surveillance cameras can monitor continuously, or use motion detection technology to record only when someone is moving about. Surveillance systems can also be	The Assistant Superintendent for Instruction and Administration, the Administrator of Technology and the Supervisor of Security will review server room access during the 2012-2013 fiscal year. The Audit Committee's recommendation to utilize an electronic ID access system in conjunction with a camera surveillance system will be reviewed by the responsible parties. The Audit Committee will be updated on this corrective action at its next meeting.	Assistant Superintendent for Instruction and Administration Administrator of Technology Supervisor of Security

configured to send e-mail or cell phone notification if motion is detected during non-business hours.		
The NOC does not have a fire suppression system such as a fire extinguisher. As per the National Fire Protection *Standard for the Protection of Information Technology Equipment* (NFPA 75) the server room at a minimum must have a fire detection and alarm, portable fire extinguisher and Emergency Power Off. It is recommended that the District place a fire extinguisher in the NOC, at a minimum, to be compliant with the National Fire Protection Association *Standard for the Protection of Information Technology Equipment* (NFPA 75).	At a minimum, the District will place a fire extinguisher in the NOC to be compliant with the National Fire Protection Association *Standard for the Protection of Information Technology Equipment.*	Assistant Superintendent for Instruction and Administration Administrator of Technology Superintendent of Buildings and Grounds

***FINANCE MANAGER* PERMISSIONS**

FINDING	**CORRECTIVE ACTION**	**RESPONSIBLE PARTIES**
The District has not restricted the ability to delete or modify journal entries within *Finance Manager*. Deleting transactions will cause a break in the transaction sequence, and a partial deletion of the physical audit trail. It is recommended that the District disable the ability to delete or modify journal entries within *Finance Manager* for all users. If a transaction deletion occurs, the District should document the reasons in order to maintain a full audit trail.	The District has restricted the journal entry permissions for all employees that perform journal entry transactions. All employees with journal entry permissions are limited to adding, viewing and printing. Permissions to modify or delete have been removed from all users.	Assistant Superintendent for Business Administrator of Technology

The District is not periodically reviewing and documenting the review of user permissions. Reviews of user permissions within *Finance Manager* will assist the District in identifying potential incompatible duties, help verify that users are assigned to permissions that are within their job responsibility and ensure that only those new user permissions or changes to existing permissions that were approved were made. It is recommended that the District implement procedures whereby user permissions are reviewed periodically and the review be documented, perhaps on a test basis quarterly due to the volume of the reports that would need to be generated and reviewed. This additional control, which is considered a best practice, will serve to strengthen the control environment even further within the District's accounting information system.	The District continues to review and update user permissions. The Administrator of Technology functions as the *Finance Manager* Systems Administrator. This individual maintains a complete file on all updates to user permissions. The Assistant Superintendent for Business has begun to review user permissions by building and department. The review is documented and any updates to the permissions are forwarded to the Administrator of Technology.	Assistant Superintendent for Business Administrator of Technology
There are thirty individuals who have two active user accounts and two individuals with three active user accounts within *Finance Manager*. Additionally, the District has five active user accounts that appear to be generic templates such as supervisor user, purchasing clerical, system administrator and tech. It is recommended that the District ensure that each individual who has access to *Finance Manager* be given one active user account. Additionally, it is recommended that the District review and update its current user	Individuals have more than one user account for different *Finance Manager* approval pathways. Certain budget codes require one layer of approval (the building principal, for example) while other budget codes require two layers of approval (the principal and the Assistant Superintendent for Instruction and Administration, for example). The purchasing clerical user account has been disabled. The District is reviewing the need for the remaining generic templates and will disable if these accounts are deemed unnecessary.	Assistant Superintendent for Business Administrator of Technology

accounts within *Finance Manager* to ensure that only those authorized individuals have active user accounts to prevent unauthorized access to the District's financial information.		
It was noted that two retired employees had active user accounts in *Finance Manager*. It is recommended that the District disable the user accounts within *Finance Manager*. The District should implement procedures to ensure that only active employees in the business operations of the District have active user accounts in *Finance Manager*.	The District has disabled the user accounts of the two retired employees. To ensure that retired employees are disabled, the Assistant Superintendent for Business will review the agenda for retiring employees. The Administrator of Technology will be requested to disable the retiring employee's user account. On a quarterly basis, the Assistant Superintendent for Business will generate the *Finance Manager* user list report to ensure that employees who have retired or resigned from the District no longer have active user accounts in *Finance Manager*.	Assistant Superintendent for Business Administrator of Technology
The Assistant Superintendent for Business has the ability to override purchase orders, cash disbursements and the general ledger in an amount up to $250,000 and the accounting supervisor has the ability to override purchase orders, cash disbursements and the general ledger in an amount up to $50,000. It is recommended that the District establish a more reasonable limit for overriding purchase orders, cash disbursements and the general ledger to improve controls surrounding the District's budgetary management and reduce the risk that budget lines will be overextended.	The Supervisor of Finance and Accounting no longer has the ability to override purchase orders, cash disbursements or general ledger accounts. The Assistant Superintendent for Business can only override purchase orders in an amount up to $5,000. There is no override for cash disbursements and general ledger accounts.	Assistant Superintendent for Business Administrator of Technology

Some District employees have been granted incompatible duties by having access to functions not pertaining to their job description. The result is a segregation of duties violation. It is recommended that the District review its current permissions in *Finance Manager* and create a system of controls that ensures the proper segregation of duties and restrict access where necessary. These deficiencies include: (1) the Assistant Superintendent for Business has full access to the *Payroll Manager* module; (2) the Assistant Superintendent for Business and two clerks within the accounting department have permissions to perform budget transfers and journal entries; (3) the Assistant Superintendent for Business and the part-time clerk within the accounting department have permissions to perform cash receipts; (4) three clerks within the payroll department have permissions to add, update and delete employee information for appointments and earnings in the *Payroll Manager* module; and (5) a clerk within the accounting department has the permission to post budgetary entries.	The following *Finance Manager* permissions have been revised: (1) The Assistant Superintendent for Business has permissions in the *Payroll Manager* module to view and print only. (2) The Assistant Superintendent for Business no longer has permission to perform budget transfers and journal entries. The titles of the two clerks that have permissions to perform budget transfers and journal entries in the accounting department are the Senior Account Clerk and the Accountant. These employees have been cross-trained to enter approved journal entry transactions in the absence of the Supervisor of Finance and Accounting. One of the responsibilities of the Senior Account Clerk is to enter approved budget transfer transactions in *Accounting Manager*. The Accountant has been cross-trained to enter approved budget transfer transactions in the absence of the Senior Account Clerk. (3) The Assistant Superintendent for Business and the account clerk in the Business Office no longer have permission to perform cash receipts. (4) The District is reviewing the permissions assigned to the payroll clerks to determine if these permissions are required. The payroll clerks have been assigned permissions in *Payroll Manager*; they have not been assigned permissions in *Human Resources Manager*.	Assistant Superintendent for Business Administrator of Technology

	(5) The accounting department clerk no longer has permission to post budgetary entries.	
VENDOR/EMPLOYEE MATCH		
FINDING	**CORRECTIVE ACTION**	**RESPONSIBLE PARTIES**
The District has not implemented procedures to identify potential conflicts of interest and ensure proper classification of vendor versus employee. It is recommended that the District develop and implement procedures to identify potential conflicts of interest, which should include but not necessarily be limited to, a periodic comparison of the master vendor file to the master employee file, identifying and addressing conflicts of interest, and reviewing IRS guidelines regarding employee versus independent contractor classification. The procedure should identify the individuals responsible for performing the comparison and establishing procedures to address conflicts of interest.	The Supervisor of Purchasing will implement a procedure whereby the master vendor file will be merged with the master employee file to identify potential conflicts of interest. A comparison of name, address and social security/federal identification number will be included as a means to identify employees and vendors included in both the master employee file and the master vendor file. All vendors are required to complete IRS Form W-9 (Request for Taxpayer Identification Number and Certification). The Supervisor of Purchasing will be provided with the IRS guidelines to distinguish an employee from an independent contractor.	Supervisor of Purchasing Purchasing Office Staff
VENDOR MASTER FILE		
FINDING	**CORRECTIVE ACTION**	**RESPONSIBLE PARTIES**
The District does have procedures in place to validate the master vendor file. However, there were 35 duplicate vendors and 10 instances in which individuals as well as the company they worked for were	The Supervisor of Purchasing has a procedure in place to inactivate vendors (initial action) and purge vendors (final action). Vendors are inactivated if there has been no activity during the year. If	Supervisor of Purchasing Purchasing Office Staff

set up as active vendors. It is recommended that the District review the vendor master file to ensure that only the appropriate vendors that the District does business with remain active. Inactive vendors whose services and/or goods are no longer required by the District should be inactivated.	those inactive vendors continue to remain inactive during the following year, the vendor is purged from the vendor file. The District requested the list of the duplicate vendors as well as the list of those individuals/companies that were set up as active vendors and have made the appropriate corrections. The Supervisor of Purchasing reviews requests for new vendors before authorizing the clerk in the Purchasing office to set up a new vendor in Finance Manager.	