COMPUTER CONTROL POLICY FOR FINANCIAL NETWORK AND SYSTEMS

The goal of the North Merrick School District is to ensure that the financial networks and systems are adequately secured. Accordingly, our policies to achieve that objective are outlined below.

Current Network Facilities

The financial systems of the District are installed on a secure server on the wide area network. This server is secured behind a firewall and on a separate secured area from other storage areas and network applications and management systems of the District. Access to the financial system is denied to all users except those given specific rights of access.

All user computer policies shall disallow the installing or downloading of any software. Software can be installed on local computers by IT staff of the System Administrator and BOCES.

All routers, switches, servers, and communications appliances within network will be loaded with up-to-date anti-hacking and anti-virus software to protect the network from Denial of Service Attacks, Trojan Horses, Viruses, and Worms. Inspection logs will be verified on a regular basis by the Network Administrator.

The System Administrator shall monitor the environmental protections including air conditioning, heat, ventilation, battery back-up and electric generator function. Warning notifications will be reported to the System Administrator and corrective action taken as soon as possible. Once a week, a powered generator test will be held.

Automated and manual software update procedures must be in place and monitored. The main MDF closet will be secured at all times and access to this area will be given only to the IT staff and System Administrator and those highest level District Administrators who have full District building access

The department will monitor theft and vandalism, and report losses immediately to the school principal or other senior administrator. Equipment replacement will not occur unless the proper loss form is completed and sent to the Assistant Superintendent for Business.

Student folders shall be locked down so that each has access to his/her folder only. Teachers shall have access to any student's folder.

Students, teachers and non administrative staff, with some special exceptions shall not have network browsing rights, "right click" or "wrong" capability.

Requests for network access and e-mail accounts by staff, requires the completion of a sign-up form which includes a signature of approval by the employee's immediate supervisor/administrator.

Passwords

Employees of the District must change their network passwords every 90 days. Each password is secured by the individual users and maintained by the Office of Technology or BOCES.

All system level passwords shall be changed whenever a member of the IT staff changes.

All user level passwords for network access will be changed with a compromise is suspected.

Passwords are not to be shared under any circumstances. If access is needed by a supervisor, the system administrator will change the user's passwords to permit access. When the user returns to work, the password can be reset by the user.

Backup and Disaster Recovery

An on-site incremental tape and a off-site full digital backup of the District's system data, including but not limited to financial and student management systems data shall be performed daily. The digital backups shall be maintained off-site by the Nassau BOCES. The District shall have a disaster recovery plan in the event of a catastrophic loss of the District's processing capabilities with Nassau BOCES.

System Administrator

The System Administrator for IT Services will ensure that the operation of IT Services is in full compliance with the District's policies, New York State Education Law and Regulations, privacy laws and practices, disclosures, regulations, etc.

The System Administrator of IT Services shall maintain and manage e-mail policies, spam and agreements.

The System Administrator of IT Services shall manage third-party contracts and agreements.

The System Administrator of IT Services shall determine when, where, and how to install wireless access points. These access points shall be configured to disallow random log-ins.

Financial Manager Permissions

Permissions for individuals in the financial system will be created and managed by the System Administrator. These permissions will be based on the organization chart and list of duties and designated job responsibilities outlined in the organizational chart. These permissions will be reviewed on a yearly basis by the Business Administrator. When special needs arise such as an extended absence by one of our employees designated for a specific job function in the financial system, the Business Office may request temporary changes to the permissions. Approval for all changes in these permissions must be in writing and signed by the Assistant Superintendent for Business.

Segregation of Duties

All duties in the financial system shall be based on the roles and responsibilities of the specific job function with the administrative offices of the District. A review of these
duties shall be done by the Assistant Superintendent for Business each year to maintain a strict policy of segregation of duties and assignment of rights and permissions necessary for each job function. The administration will implement appropriate compensating controls when adequate segregation of duties is not practical or possible.

Remote Access and Security

Remote access will be granted to the finance manager vendor for purposes of updating the system or software by the System Administrator. The time of this access will be limited to business hours only and require IT staff approval each time access is granted. Access logs shall be reviewed on a regular schedule by the Network Administrator assigned to manage the system firewall. Any abnormal access shall be reported immediately by the System Administrator and all remote access shall be terminated until permission to resume is granted. Reports requested from or programmed by IT Services shall be for appropriate personnel only, and if questionable, the need shall be confirmed by the appropriate senior administrator.

Reporting

Within the financial systems there are a number of useful reports that can be generated for review by the Board of Education, the District Superintendent, the Assistant Superintendent for Business, and the auditors. Access to view and print these reports will be given to the Assistant Superintendent for Business, the Treasurer and/or the District auditors. Such reports may be requested as needed by the Board of Education and the District Superintendent.

Date Adopted: July 1, 2008