

SUBJECT: **Financial/Human Resources Management System Computer Controls Policy**

Plainview-Old Bethpage Central School District communication and computing resources are used to support the educational and administrative goals of the District. Activities involving these resources must be in accord with District Policies and regulations, including but not limited to Computer Network/Internet Use Policy, codes of conduct, and relevant local, state, federal laws and regulations.

For use to be acceptable it must demonstrate consideration for:

- the rights of others to privacy;
- ownership of data;
- system mechanisms designed to limit access;
- intellectual property rights (e.g., as reflected in licenses and copyrights)

Data Users are defined as individuals who have need for District data in order to perform their assigned duties and therefore have need for authorized access. Data Users having access to financial and human resource data must only use this information for job-related purposes - not for the personal use by others or themselves. It must only be shared with employees within their own department who need the information to perform their job responsibilities. All data users must sign the District Computer Network/Internet User Policy indicating their understanding of appropriate District-wide network access procedures and accountability.

The District regards any violation of this policy as a serious offense and violators are subject to disciplinary action as prescribed in the Computer Network/Internet User Policy and maybe reported to appropriate law enforcement officials when warranted.

SEGREGATION OF DUTIES / PERMISSIONS:

1. Assistant Superintendent for Business:

Responsibilities include District oversight of District Financial/Human Resource Management System segregation of duties and permissions.

2. System Manager/s:

A Security Maintenance Authorization Form is required for the Assistant Superintendent of Business to designate the individual(s) that are authorized as System Managers to add Data Users to the District's financial system and define their rights as users.

SUBJECT: **Financial/Human Resources Management System Computer
Controls Policy, Cont'd**

The Director of Technology and the Assistant Business Manager have been designated to serve as the primary and secondary District Financial/Human Resource Management System Managers respectively. Responsibilities include the set-up of the system for the technical maintenance of internal controls and segregation of duties among users as authorized by the Assistant Superintendent for Business. Data User security shall be designed to assure the segregation of duties among District staff and to establish internal controls related to the handling of District resources. Data Users' permissions are assigned by specific functional area. No staff will have access or permission rights beyond the scope of their job duties.

Separate authorizations shall be designated as to:

- a) the Data User's ability to maintain or display data or perform specific tasks in the functional area;
- b) the records the Data User can maintain and/or display related to the functional area or that are to be included on reports they have access to (View);
- c) the specific table maintenance rights the Data User has in that functional area (Tables);
- d) the specific reports the user is able to generate in that functional area (Reports);

3. Building-Based Data Users

Job duties must be determined by the building principal, department head or designee and authorized by the Assistant Superintendent for Business to gain network access to the data on the District Financial/Human Resource Management System. Only individuals who need direct access to financial and/or personnel data in order to perform specific job responsibilities will be designated Building Based Data users and given this authorization. Access will be limited to only the departmental data and information required to perform the duties of the job.

SUBJECT: **Financial/Human Resources Management System Computer
Controls Policy, Cont'd**

4. Central Office Business and Human Resource Data Users:

The Assistant Superintendent for Business in consultation with the Assistant Superintendent for Personnel, will review and identify duties and user access permissions for the positions indicated below:

Assistant Business Manager, Business Office Payroll Clerk, Business Office Insurance Clerk, Business Office Accounts Payable Clerk, Business Office Account Clerk, Business Office Purchasing Clerk, Business Office Claims Auditor, Personnel Office Clerical, Aides, and Custodial Records Clerk, Personnel Office Administrators and Teachers Records Clerk, Personnel Office Admin. & Teachers' Interviews and Substitutes Info Clerk, Local District Computer Network Technician.

4. Representative Data Access:

Representatives whose official functions include audits or investigations may have inquiry access to records when access to data is needed for specific official investigations. Such access must be justified in writing to the Assistant Superintendent of Business and limited to a defined scope of time.

REPORT GENERATION AND APPROVAL:

- The Primary District System Manager will generate, monitor, approve, and log quarterly summary reports consisting of:
 - a) Data User Listings showing a report of all active data users
 - b) Data User Security Report showing each user's actual permissions and restrictions
 - c) Data User Security Change Report to track user id's that have been added, inactivated or archived ("deleted"), any password changes, or any other specific changes that have been made to the specific rights for individual users through the user profile maintenance
 - d) Data User Login History

- The Assistant Superintendent for Business will generate, monitor, approve and log quarterly the following reports:
 - a) User Security Profile Change Report
 - b) Vendor Record Change Report
 - c) Employee/Vendor Match Report

SUBJECT: **Financial/Human Resources Management System Computer Controls Policy, Cont'd**

PASSWORD SECURITY:

Purpose

Passwords are a critically important component of the District Financial/Human Resources Management System security. Passwords that are easily guessed, written down or shared put the District at risk for a security breach. Passwords are a significant portion of a Data User's electronic identity and should remain confidential at all times.

Scope

This policy defines the parameters of the District's Financial/Human Resource Management System Security Policy and applies to all users personnel. Additionally, the Assistant Superintendent for Personnel will notify the District Financial/Human Resource Management System Manager when to remove a user from the system due to termination, retirement or change in job duties which leads to no longer needing access to the system.

Password Requirements

- Password changes **must** be automatically forced by the system every 180 days.
- Passwords **must** include a **minimum** of 6 characters and be alphanumeric - meaning it must contain at least one number and one letter.
- Passwords **must not** be written down.
- Passwords **can not** be re-used.
- All Data Users **must not** permit other users to access their computer, network or financial computer application under their personal password protected log-on accounts.
- All Data Users **must** exit from the application when not in use and log-off their computers upon leaving their desk and at the end of the work day. An open computer that is left logged-on presents a substantial security risk to the user and sensitive District information.

SUBJECT: **Financial/Human Resources Management System Computer Controls Policy, Cont'd**

DATA BACK-UP / DISASTER RECOVERY:

The application server is configured with a tape backup system that is monitored by the District's Financial/Human Resource Management software vendor, the System Manager, and a local District network technician. This protects against data corruption as well as system or network failures that prevent access to the "live" data stored on the server.

Tape backup procedures are utilized to assure that backups are performed routinely.

- A software program is run prior to each backup to log off all users on the system before the backup begins
- Another program is run after the backup has been successfully completed – it creates a file to let the District's Financial/Human Resource Management software vendor know that the backup was in fact completed. If this file does not exist, then the District's Financial/Human Resource Management software vendor provides a backup error message which is seen when each user logs into the system requesting that they have their System Manager be contacted.
- Utilizing the notification feature, a printed report indicating the status of the Server Backup (this goes to a defined "batch notifier" printer) is printed at the District Central Office of Technology and monitored by the network administrator and system manager.
- The System Manager verifies that backup tapes are switched each day and secured.
- On a rotating basis backup tapes are located in a secure off-site location.

Battery Backup Power Supply

The Application Server is equipped with an Uninterruptible Power Supply, which is essentially an intelligent battery backup system. It is designed to supply sufficient power to the server so as to allow time to log users off of the system and to power down the server in the event of a power failure. The UPS also provides power conditioning, by guarding against power "spikes" and brownouts.

SUBJECT: **Financial/Human Resources Management System Computer
Controls Policy, Cont'd**

Redundancy

- The District's Financial/Human Resource Management software has a minimum of three hard drives that act like one hard drive. Data is spread across the three hard drives, and a small segment of each drive contains parity. If one of the drives goes bad the other drives can keep the system going until a new drive is installed into the system.
- Dual Server Power Supplies
- Multiple Server Processors

Server Security

The District utilizes software for connectivity to the Financial/Human Resource Management Application Server. Only PC's with this software installed can connect to the Application Server. When Data Users are connected to the application server, they are logged directly to the Financial/Human Resource Management Software login screen, where they are required to enter a valid user name and password in order to gain access.

Administrative level access to the server is limited to technical staff, the District System Manager, and a designated District network technician.

The server is located at the District NOC (Network Operation Center) which is a secure environmentally controlled location to protect the server against vandalism, theft, heat and water damage, etc.

Anti-Virus Software

Anti-Virus software is installed on the District's Financial/Human Resource Management Application Server. System-wide virus updates and checks are performed regularly.