Central Islip Union Free School District

Board of Education & School District Policy Book
50 Wheeler Rd. | Central Islip | N.Y. | 11722
(631) 348-5000
https://www.centralislip.k12.ny.us

Section	Section Title	Type
8000	Support Services	Local
Policy	**Policy Title**	
8632	Financial/Human Resources Management System Computer Controls Policy	

The Central Islip Union Free School District's financial and human resources are used to support the educational, administrative and financial goals of the district. Activities involving these resources must be in accord with district policies and regulations, including but not limited to the computer network and internet use policies, codes of conduct, and relevant local, state, federal laws and regulations.

For data 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 a 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 of others or themselves. It must only be shared with employees within their own department who need the information to perform their job responsibilities.

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 and internet user policies. Violators, when warranted, may be reported to the appropriate law enforcement officials.

SEGREGATION OF DUTIES/PERMISSIONS:

1. **Assistant Superintendent for Business:** Responsibilities include district oversight of the Financial/Human Resources Management System's segregation of duties.
2. **System Manager:** The Assistant Superintendent for Business will designate the individual(s) that is/are authorized as System Manager(s) to add data users to the district's financial /human resources system and define their rights as users.

The Senior Accountant has been designated to serve as System Manager. Responsibilities will 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 users' 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 function 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;
d. The specific reports the data user is able to generate in that functional area.

3. **Building-Based Data Users:** Job duties must be determined by the Building Principals, Department Heads; and authorized by the Assistant Superintendent for Business to gain access to the data on the financial/human resources management system. Only individuals who need direct access to financial and/or personal data in order to perform specific job responsibilities will be designated "building- based data users" and given this authorization. Access will only be limited to the departmental data and information required to perform the duties of the job.
4. **Central Office Business and Human Resource Data Users:** The Assistant Superintendent for Business will review and identify duties and user access permissions for the positions indicated:

Superintendent of Schools, Assistant Superintendent for Curriculum and Instruction, Assistant Superintendent for Personnel;

Secretaries to: The Superintendent of Schools, Assistant Superintendent for Business, Assistant Superintendent for Curriculum and Instruction, Assistant Superintendent for Personnel;

Business Manager, Senior Accountant, Payroll Clerks, Employee Benefits Clerk, Accounts Payable Clerks, Principal Account Clerks, Senior Account Clerks, Account Clerks, Purchasing Agent and District Treasurer.

5. **Representative Data Access:** Representatives whose official function 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 for Business and limited to a defined scope of time.

REPORT GENERATION AND APPROVAL: PASSWORD SECURITY:

1. The System Manager will generate, monitor, approve and log bi-annually 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 permission and restrictions;
    c. Data user security change report to track user id's that have been added or inactivated (deleted); password changes, and any other specific changes that have been made "specific rights" for individuals through the user profile maintenance;
    d. Data user log-in history.
2. The Assistant Superintendent for Business will generate, monitor, approve and log bi-annually the following reports:

    a. User security profile change report;
    b. Vendor record change report;
    c. Employee/vendor match report.

Passwords are a critically important component of the district financial/human resources management system's security. Passwords that are easily guessed, written down, or shared can put the district at risk for a security breach. Passwords are a significant portion of the data user's electronic identity and should remain confidential at all times.

The Assistant Superintendent for Personnel will notify the 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:

1. Password changes must be forced by the system automatically every 180 days;
2. Passwords must not be written down;
3. Passwords cannot be re-used;
4. All data users must not permit other users to access their computer, network or financial computer application under their personal passwords protected log-in accounts;
5. All data users must exit from the application when not in use and log-off their computers upon leaving their desks and at the end of the workday. An open computer that is left logged on presents a substantial security risk to the user and to sensitive district information.

REMOTE ACCESS:

The Assistant Superintendent for Business, Business Manager, and Senior Accountant will be permitted remote access to the district's financial/ human resource management system.

DATA BACKUPS:

See policy # 8630.1, section #7, "Offsite Backup of Critical Data".

1st Reading: December 11, 2017
2nd Reading: January 8, 2018
Adoption: January 8, 2018

Cross Reference:
8630.1, Disaster Recovery and Business Continuity Policy