

Internal Control Policy

Considerations

Internal controls are critical to the District's program, administrative and fiscal operations. Properly utilized, documented, and updated internal controls protect District's assets, maintain public trust, and ensure compliance with legal and regulatory requirements. Departments that do not comply with internal control requirements are subject to corrective actions and potential penalties.

Policy

An internal control guide has been developed to assist department directors and staff in creating and maintaining internal controls and internal control plans. All District employees share responsibility for safeguarding resources, adhering to policy, and reporting suspected misuse of funds or assets.

The Internal Control Plan

An effective Internal Control Plan is a department-wide summary of risks and controls for all business processes. It is supported by detailed procedures, communicated to staff, and continuously monitored and updated.

Internal Controls

1. Internal control refers to the processes and procedures used to provide reasonable assurance regarding the achievement of objectives in the following categories:
 - a. Safeguarding assets
 - b. Ensuring validity of financial records and reports
 - c. Promoting adherence to policies, procedures, regulations and laws
 - d. Promoting effectiveness and efficiency of operations
 - e. Facilitating accomplishment of established goals for operations and programs.
2. Internal controls include but are not limited to:
 - a. Segregation of duties
 - i. Financial responsibilities are divided between different people to ensure a single person does not perform every aspect of a financial transaction. Segregating responsibilities can reduce errors and prevent or detect inappropriate transactions.
 - b. Authorization and Approval
 - i. Transactions should be authorized by a delegated official who verifies, prior to approving the transaction, that:
 1. They have approval authority
 2. Sufficient funds are available
 3. The transaction is:
 - a. Consistent with policy (and benefits the fund source(s) being charged), and
 - b. Allowable (meets the stipulations of the fund(s) as well as that of the Board),
 - c. Accurate, and

- d. Reasonable.
3. Review and Reconciliation
 - a. Routine examination and reconciliation of transaction records to official District records is required to verify the accuracy of the records, the appropriateness of the transactions, and their compliance with policy.
4. Physical and Cybersecurity
 - a. Equipment, inventories, cash and other property shall be physically secured, and periodically counted and reconciled to District records. Systems and data shall be secured against misuse and cyber threats.
5. Training and Supervision
 - a. Training is to be provided to ensure employees are equipped to fulfill their job duties. Employees are to be supervised to ensure they are appropriately directed and held accountable. Employees are to be informed of the process of reporting suspected improprieties.
6. Documentation of Policies and Procedures
 - a. District and department policies and operating procedures shall be written, communicated, promoted, accessible, and used to assure integrity and consistency in processes and transactions.

Accountability and Delegation of Authority

Accountability for financial control purposes is the delegation of authority to qualified persons to initiate, approve, process, and review business transactions. The delegated authority is responsible for assuring that each transaction is:

1. Within their delegation
2. Consistent with policy (and provides benefits to the fund source(s) being charged)
3. Allowable (meets the stipulations of the fund(s))
4. Accurate, and
5. Reasonable.

A delegation of authority entrusts a task, power, or responsibility to another. The purpose of a delegation is to empower an official(s) with designated responsibilities.

Conflict of Interest

A financial conflict of interest exists when an employee initiates, influences, authorizes, or approves a business decision that results in a financial benefit to the employee, a relative of the employee, a business associate or personal friend of the employee, or a business or investment in which the employee is associated.

Policy**A. General**

To foster the mission of the District and sustain the District's integrity as a custodian of public funds, every member of the District community is responsible for safeguarding the District's assets and reputation by following District policies, exercising sound business and financial practices, and ethically performing their responsibilities. Internal controls such as policies, practices, processes, systems, and delegated authorities are tools to accomplish these goals.

B. Accountability

1. Each department has the responsibility and is accountable for managing the resources it administers on behalf of the District.
2. The department head may delegate financial management responsibility to the business officer. Delegating authority and accountability does not relieve the department head of accountability for activities under their direction. The department head and or the business officer are responsible for developing an appropriate structure for handling the unit's financial resources, including the delegation of a variety of tasks to employees within the unit.
3. The department head must officially record in writing all delegations of authority as well as any cancellations or changes in delegations.
4. Accountability delegations are to be consistent with appropriate internal controls.

C. Internal Controls

1. Directors, principals, and coordinators at all levels are responsible for ensuring that an appropriate and effective internal control environment has been established within their areas of responsibility.
2. All District employees are responsible for:
 - a. Following District policy, procedures, and department internal control practices, and
 - b. Notifying their supervisor or an appropriate official if they observe or suspect fraud or misuse of District resources.

D. Conflict of Interest

1. All District employees shall refrain from participating in any activities which place them in a conflict of interest between their official activities and any other interest or obligation.
2. In addition, designated District officials are required to file conflict interest statements when they assume their designated position, annually, and when they leave the designated position.

Internal Control Guidelines**A. Payroll/Personnel****1. Separation of Duties**

- a. Duties related to payroll processing should be divided to ensure no single employee controls all aspects of the process.
- b. Different employees should be responsible for (1) entering and maintain payroll and personnel information into the finance software, (2) correcting, modifying and posting hourly and leave information, and (3) reviewing payroll reports and reconciliations and (4) issuing payroll checks and direct deposits.

2. Authorization and Approval

- a. Only persons with delegated authority may approve forms, workflows or requests for additional pay.
- b. Employees may not approve actions affecting their own pay.
- c. Supervisors should approve employee attendance records each pay period.
- d. Supervisors should approve any time recording or reporting alterations.

3. Custodial and Security Arrangements

- a. Payroll records must be filed and maintained in a secure location with access limited to authorized personnel. Records must be stored in compliance with retention and confidentiality requirements.
- b. Presentation of government-issued identification is required when releasing a manual check to employees not known to the person distributing. Employees picking up a manual check must sign for the check. Manual check issuance should be limited to necessary exceptions.
- c. Changes to employee direct deposit information must be verified in-person or through direct contact with the employee, not through email correspondence or other unverified electronic communication.

4. Review and Reconciliation

- a. Payroll expense reports should be reviewed and approved each pay period prior to processing.
- b. Any questionable or irregular entries must be immediately investigated, documented, and resolved.
- c. The person performing the review should sign and date reports to signify that the review has been satisfactorily completed and any discrepancies resolved.

B. Procurement of Materials and Services**1. Separation of Duties**

- a. Separation of purchasing related duties should be established so that no one employee has total control over any purchase transaction.
- b. Different individuals should be assigned responsibility for (1) approving requisition and purchase orders, (2) receiving ordered materials, (3) approving invoices for payment, and (4) reviewing and reconciling the monthly general ledger.

2. Authorization and Approval

- a. Only persons with delegated authority should approve purchases, invoices and check requests.
- b. The receipt of goods and services should be verified prior to approving invoices for payment.
- c. Verification should be made that invoiced amounts are correct, accounts charged are correct, object coding is correct, and payment has not already been made.
- d. Low value purchasing policy requirements should be observed.
- e. The splitting of purchases to bypass procurement thresholds is prohibited.

3. Custodial and Security Arrangements

- a. Changes to vendor direct deposit information and changes to vendor check remittance addresses must be verified through direct contact with the vendor, not through email correspondence.

C. Supply and Equipment Inventories

1. Separation of Duties

- a. Physical inventories must be performed by employees who are not responsible for maintaining custody of the items, nor subordinates of the custodian.
- b. Equipment and inventory changes must be approved by someone who is not directly responsible for the custody or disposal of equipment.

2. Authorization and Approval

- a. Purchase orders must be approved by a person with delegated approval authority.
- b. Adjustments to inventory records for returned, missing, damaged or stolen items must be approved by departmental management.

3. Custodial and Security Arrangements

- a. Security arrangements for safeguarding inventory must be proportional to the value of the inventory.
- b. Off-premises use of District equipment must be primarily for District business purposes, approved by the department head or higher authority, and documented in a maintained record.
- c. District equipment may not be used for personal purposes, except as permitted by policy for incidental use.
- d. Access to inventories must be limited to the minimum number of employees necessary.
- e. Locks must be re-keyed or changed when significant personnel turnover occurs. Keys must be collected from separating employees.

4. Review and Reconciliation

- a. Items must be inspected for condition prior to being included in inventory records.
- b. Obsolete, inactive or damaged items must be removed from inventory with approval from the Business Office.
- c. Physical counts of large supply inventories must be conducted annually. Equipment inventories must be conducted at least bi-annually.

D. Cash Receipts

1. Separation of Duties

- a. Responsibilities for cash handling must be separated so that no single individual has control over the entire process. At a minimum: (1) One person must receive and record cash collections, (2) A different person must balance daily cash receipts to related cash recordings, and (3) A third person must verify that deposit amounts recorded in the general ledger agree with departmental records.
2. **Cash Accountability**
 - a. Employees handling cash are individually accountable for their actions. Each employee is responsible for handling cash in accordance with District policies and guidelines.
 - b. Transfers of cash between two individuals must be jointly verified and documented.
 - c. Supervisors should review and verify cash deposits, voided transactions, and any cash overages or shortages.
3. **Recording and Depositing**
 - a. All cash receipts must be recorded at the time of receipt using a cash receipt form, cash register, or a properly controlled computer database.
 - b. Checks should be made payable to Fargo Public Schools and promptly endorsed for deposit upon receipt.
 - c. All collections (cash, checks, or cash equivalents) must be deposited weekly.
4. **Review and Reconciliation**
 - a. Cash receipts must be balanced to receipt records on the day they are received.
 - b. Deposit receipts must be verified to ensure the depositing location recorded the correct amount.
 - c. Deposit entries in the general ledger must be reviewed and verified.
- E. **Petty Cash**
 1. **Fund Establishment and Review**
 - a. Petty cash funds must be authorized by Business Office, maintained in a secure location, and accessible only to the petty cash custodian of record, and used only for appropriate District business purposes.
 - b. A supervisory employee who does not have custody of the petty cash fund must review expenditure documentation, verify that the total fund balance is accounted for, and approve requests for petty cash fund replenishment.
 2. **Custodial and Security Arrangements**
 - a. Cash and checks must be stored in a locked receptacle located in a secure area.
 - b. Custodial responsibility for a petty cash fund must be assigned to a single employee, with a designated alternate identified.
 3. **Review and Reconciliation**
 - a. All disbursements must be supported by a receipt documenting the expenditure.
 - b. The fund must be counted and balanced at least monthly by a supervisor who is not directly responsible for maintaining the fund.
- F. **Billing and Accounts Receivable**

The use of the District's Billing/Accounts Receivable Finance System is required for billings to external parties.

1. Separation of Duties

- a. Responsibilities must be separated so that: (1) One person is responsible for billing and maintaining accounts receivable records, (2) A different person is responsible for receiving or handling incoming payments, and (3) A third person is responsible for reconciling receivable records to the general ledger.

2. Custodial and Security Arrangements

- a. Invoices must be prepared for all charges and issued on a timely basis.
- b. Invoices must be issued in numerical sequence.
- c. Blank invoices, credit memos, and cancellation forms should not be used.

3. Review and Reconciliation

- a. Receivable reports must include aged listings of all amounts due, be reviewed at least monthly, and be reconciled to the related general ledger account.
- b. Delinquent account balances must be reviewed, and follow-up with customers must be initiated in a timely manner to facilitate collection.

G. Budgetary Control

- 1. Budgets should be prepared annually and based on realistic expectations of revenues and expenses.
- 2. General ledgers should be reviewed monthly to verify charges to expenditure accounts.
- 3. Actual expenditures should be compared to budgeted amounts, and variances identified monthly.
- 4. Financial and budgetary status reports should be reviewed regularly by directors, coordinators, principals, and other responsible managers.

H. Information Systems and Cybersecurity

- 1. New systems should be developed or acquired consistent with District policies, guidelines, and procedures.
 - a. New systems should be completely tested prior to putting them into operation.
 - b. Systems should be fully documented, including operations, program, and user instructions.
 - c. All changes to computer programs should be properly authorized and documented.
 - d. Systems should include audit trails and edit routines.
 - e. Systems, programs, databases, and data files should have logical access security and be physically secure.
 - f. Equipment should be properly safeguarded against theft, power fluctuations and application viruses.
 - g. Departments shall have backup and recovery processes to ensure continuity of operations. Backup media should be stored off-site, remote from the production files.
 - h. Employees should be properly trained and cross-trained to prevent an unduly high degree of reliance on one knowledgeable employee.
 - i. Employees should receive appropriate information on managing and protecting confidentiality of passwords.
 - j. Systems should include multi-factor authentication and password security.
 - k. Annual cybersecurity training, vulnerability scans and penetration should be conducted.

1. Software installed on District equipment should be authorized and used for District business purposes. Software use shall conform to copyright laws and licenses.

Adopted 1/11/11
Reviewed 7/23/13
Revised 7/2017
Revised 7/2022
Revised 6/2026