

SOUTHERN METHODIST UNIVERSITY
GUIDELINES and PROCEDURES for FINANCIAL TRANSACTIONS
BUSINESS AND FINANCE

Effective as of: 06/01/2001

Revised 6/01/2009

SCOPE

Many University departments are involved in handling financial transactions. It is these departments and personnel to which the *Guidelines and Procedures for Financial Transactions* (Guidelines) are directed. These Guidelines supercede any previous procedures and historical departmental practices regarding the handling of cash and should be followed in all circumstances, unless the department has requested an exception in writing from the Controller, and written permission has been granted.

GENERAL DEPARTMENTAL AND PERSONNEL RESPONSIBILITIES

Compliance

Full cooperation of all University personnel is necessary to safeguard University assets (see below the University Policies 3.1, *Expenditure Control for the University*) Financial Officers and other supervisors are responsible for ensuring adherence to policies and procedures. However, it is the responsibility of all University employees to be observant of these policies and report observed or suspected instances of malfeasance, including theft, negligence, misappropriations or carelessness. To the extent persons handling financial transactions do not comply with University cash handling policies and procedures, the Controller's Office is responsible for initiating further action, which may include termination from employment and prosecution.

All employees handling financial transactions must sign a statement indicating that they have read these Guidelines, that they will comply, and that they understand the ramifications of noncompliance **before** they are assigned responsibility for financial transactions. The signed statement will be placed in the employee's file in Human Resources.

Employment Practices

Permanent and temporary personnel who handle financial transactions are subject to criminal background and credit history checks **before** assuming their duties. New hires seeking positions that have financial responsibility will be required to authorize the University to perform these background and credit history checks prior to final consideration for the positions.

Student workers are subject to the same requirements as employees if they have unsupervised responsibility for financial activity. The accountability of student workers whose financial activities are supervised by University employees is the responsibility of those University employees and ultimately of the Vice President and/or his or her designee in charge of the area.

Employees who do not comply with these Guidelines will be subject to disciplinary action. Further, all University employees are bonded. The bond covers losses resulting from dishonesty in the handling of funds or property entrusted to employees. If the bonding company pays a loss, it has a legal right of action against the employee causing the loss. In addition, supervisors are subject to disciplinary action for failing to detect offenses (See University Policy 9.34, *Dishonest, Fraudulent or Illegal Practices*).

Roles and Responsibilities

The following is a brief description of various departments or individuals as they relate to financial transactions:

President - The responsibility and authority for the administration of all policies, personnel, and finances are vested in the President. The President fulfills his/her duties through a senior management team.

Vice President for Business and Finance - This vice president is responsible for all financial activity at the University. His or her staff is responsible for making any interpretation or clarification of financial transactions policies and procedures, including these Guidelines, as well as the implementation of personnel policies associated with individuals responsible for financial transactions.

Associate Vice President and Controller (Controller) - The Controller is responsible for ensuring that adequate controls exist to manage and account for all funds at the University, as well as administering and communicating financial transactions policies and procedures, including these Guidelines, to appropriate parties (Financial Officers, et al).

Associate Controller – The Associate Controller reports to the Controller and is responsible for implementing, maintaining, monitoring and enforcing a good control environment for financial activities at the University.

Financial Officers (FOs) – The FOs are responsible for financial activities within their schools and/or departments. FOs must be aware of the financial management environment that exists in their units and put procedures in place to safeguard the University's financial assets. Towards this end, FOs should ensure that their units have adequate systems, processes and written procedures in place for handling funds in their areas of responsibility and that

employees are aware of, understand, and are capable of complying with financial policies and procedures. The University Internal Auditor and Controller work with FOs on financial control and process issues, as necessary.

Cash Manager: The University's Cash Manager is responsible for managing the University's operating cash, including optimizing investment return and ensuring that funds are available to pay for goods and services, as needed.

University Deposit Drop (Deposit Drop) – The Blanton Deposit Drop is the destination collection point for University cash receipts unless other arrangements have been made. Deposits are recorded at this central location and are forwarded to the University's depository bank(s) via armored transport. The cashier responsible for these deposits provides instructions for the proper transmittal of funds and works with General Accounting as well as interfacing with banks concerning delayed deposits or discrepancies. For purposes of these guidelines, note that not all deposits are forwarded to the University Deposit Drop for delivery to the bank. Deposits in Athletics and Development (Gift Processing) are handled separately with an armored transport to the bank, and deposits at Expressway Tower are made at the bank housed in the facility.

General Accounting - This office is responsible for reconciling bank accounts, investigating discrepancies, and making correcting entries as necessary.

Risk Management – The Risk Management Department assesses risks, ensures that University insurance coverage is adequate, verifies that appropriate loss control procedures are in place, and oversees employee bonding. All losses must be reported to this office when discovered.

Internal Audit - The Internal Auditor reviews University records to verify accuracy, adequacy of controls, and compliance with policy. Additionally, the Internal Auditors work with University officials to investigate allegations of financial misconduct.

University Police - This department investigates allegations of forgery, theft, other criminal violations, and violations of University policy. All losses must be reported to the Police Department when discovered. In addition, the Police Department will provide security guidance as needed.

Legal Affairs - This office is responsible for investigating and prosecuting fraudulent and criminal activities.

CASH COLLECTION AND DEPOSIT

Written internal control procedures must be in place at all locations handling cash (receipts) to ensure that the following objectives are met:

- Receipts are accurately and properly recorded;
- Receipts are properly safeguarded during the time between collection and deposit;
- Receipts are deposited on a timely basis (see below);
- Checks are restrictively endorsed immediately when received;
- Receipts are reconciled to accounts periodically, but no less frequently than monthly; and
- There is segregation of the collection, recording, and reconciliation functions at each location, to the extent practicable.

Deposits must be made in a timely manner, which is generally defined as the same or the next business day. Further, in no case should receipts totaling \$500 or more at any location be deposited later than the next business day. Receipts totaling less than \$500 must be deposited at least weekly. All receipts must be deposited at the end of the fiscal year regardless of amount.

Security

All receipts must be kept in a secure location. Receipts maintained during the day and receipts totaling less than \$500 held overnight may be kept in a locked desk, filing cabinet, safe or other secure location. Receipts totaling \$500 or more should be taken immediately to Secure Collection Stations if held overnight. The amount of receipts on hand will determine the level of security required.

Secure Collection Stations must have safes. Only personnel at Secure Collection Stations should know the combinations to safes and codes to alarms. Management should consider changing safe combinations and security codes when there is turnover in responsible persons or other individuals with knowledge of the combination. Access Control will conduct a regular accounting of all issued keys for offices with receipt handling responsibilities and address control issues associated with the lost keys with department management. Management should consider re-keying Secure Collection Station locks when keys are lost or misplaced and when employees with the keys leave or transfer.

Employees who handle cash receipts must take reasonable care to minimize loss. They should avoid counting receipts in open view of the public or of employees not having receipt handling responsibilities, whenever possible. Further, they must:

- Never leave cash or other negotiable instruments, unsecured and unattended.
- Transport all deposits in a secured manner, preferably in locked moneybags (Note that deposits over \$5,000 should be couriered to the Deposit Drop by two individuals when practicable. University police may be called to provide an armed officer at the discretion of the FO or their designee).
- Report any missing receipts to the Controller's Office immediately.

Points of Collection

The FOs or designees should be knowledgeable about the sources of receipts in their areas, the locations at which receipts are accepted, the estimated volume of receipts, and the detailed procedures for collecting and safeguarding receipts until transported. Requirements at points of collection, which are any and all locations where receipts enter the University, include the following:

- Departments that routinely process large volumes of financial transactions (e.g. ticket offices and shops) should have a cash register or a system that reconciles “sales” to receipts.
- Departments without a cash register or other reconciliation system must use a pre-numbered receipt system to record collections. Checks received by mail should be recorded on a log as soon as the mail is opened.
- Departments that process financial transactions for tuition (credit and non-credit) must have a system that reconciles the income to the registrations.
- Methods of recording receipts must include the information necessary to trace individual collections from the point of receipt, through aggregation, into daily or periodic entries into the accounting records.

Preparation of Deposits

Departments are responsible for completing deposit forms to accompany all deposits submitted to the Deposit Drop. Deposit forms must be used to record the deposit on the University’s accounting records in the appropriate departmental org and account. Currency and checks must be recorded in their respective spaces on the deposit form. Checks must be stamped with the departmental endorsement. Where practicable, deposits should be taken to the Secure Collection Station for proofing and transport.

Before transporting receipts to the Deposit Drop, a record such as a log must be made of all deposits. (See **Security** section above for transport detail.)

The cashier at the Deposit Drop will oversee the safe transport of deposits to the bank (except for departments that send their deposits directly to the bank via armored truck).

Reconciliation

Deposits must be reconciled periodically, but no less frequently than monthly. Reconciliation procedures should include the following:

- A staff accountant in General Accounting checks the processed deposit forms from the bank to ensure the amount shown thereon matches the record (log). Any discrepancies will be resolved by working with the originating office and the bank.
- The staff accountant will contact the originating office to resolve any issues associated with unprocessed deposits returned by the bank.
- Departments are responsible for reconciling their deposits on a monthly basis to their month-end reports. Any discrepancies must be reported promptly to their appropriate FO and, if not resolved, to General Accounting.
- The FOs or the Internal Auditors may conduct random audits of points of collection. The Internal Auditors may also audit an FO's records.

Internet Payment Sites

Internet payment sites are subject to some of the same control procedures as cash deposits. They need to be accurately and properly recorded and reconciled in a timely way and secured in a way that nonpublic financial information related to the payer is not available to those who should not have access rights to the information. In addition, Information Technology Services must approve the website, ensuring that the site is secure and meets University standards.

PETTY CASH

Petty Cash is a generic term for the use of cash to reimburse authorized small dollar purchases. Small dollar purchases can be reimbursed through a Petty Cash Fund, which is covered in detail in these Guidelines. The use of Petty Cash Funds at the University is restricted to select, approved areas due to additional risks associated with having cash on hand. Petty Cash Funds are held by departments to reimburse employees for authorized small dollar purchases or to be used as "change funds." The Petty Cash Fund is usually replenished with reimbursements processed on check requests.

The Controller's Office approves Petty Cash Funds for departmental use, when an appropriate justification can be made. Departments are responsible for providing adequate security and control of their petty cash. Any losses or theft of Petty Cash are the responsibility of the custodian and/or the department (see below).

Petty Cash may not be used for the following:

- Travel reimbursements requiring travel reports
- Payments for services which require a W-9

- Payments to employees for services, benefits, extra-compensation, awards, etc., which should be processed through Payroll
- Payment of invoices to the University, which should be processed through Accounts Payable
- Payment to University service centers, which can be processed on a journal entry or purchase requisition
- Personal loans or IOU's
- Check cashing

Petty Cash must be kept separate from all other receipts. Personal funds should not be commingled with Petty Cash.

Establishment and Management of a Petty Cash Fund

To establish or modify a Petty Cash Fund, an FO must send a written request to the Controller's Office. The request must detail the purpose and use of the fund, identify the custodian and his/her supervisor, the Petty Cash amount to be established or modified, and the proposed secure location. The Controller's Office will review each request and approve, decline, or return for more documentation.

The custodian will sign an agreement accepting responsibility for the Petty Cash, which General Accounting will keep on file. General Accounting must be notified if there is a change in a Petty Cash custodian. FOs will audit and document the fund at the time of the change, and a new custodian agreement will be made and signed. If there are any shortages, that amount will be deducted from the custodian's paycheck as referenced in the agreement.

The initial Petty Cash allocation will not appear as a charge to the department. Petty Cash is recorded as an asset on the University's books. Charges are not made to the department's budget or reflected as expenditures on the department's orgs until a check request is submitted to replenish the amount.

The custodian is responsible for ensuring that all reimbursement requests to replenish Petty Cash comply with University policies and that proper documentation for each expenditure is maintained. Petty Cash must be reconciled internally each time a replenishment is made to ensure that the cash balance and the paid receipts on hand equal the total authorized amount of the allocation. Petty Cash is subject to unannounced audits by any auditing entity (Internal Auditing, external auditors, General Accounting, FOs, and the Controller's Office), as appropriate. A confirmation of the Petty Cash balance is required by the Controller's Office at fiscal year-end.

To close a Petty Cash fund that is no longer needed, the cash must be deposited into the University's bank account (crediting the Petty Cash asset), and General Accounting must be notified. Closure will be noted on the original Custodian Agreement.

Security

Security of Petty Cash is the responsibility of the custodian. Petty Cash must be at least secured in a locked desk or cabinet, but Petty Cash over \$500 must be kept in a safe. It must be accessible only to the designated custodian, although the FO may also have combinations and spare keys, as necessary. Desk drawers or cabinets where Petty Cash is stored should be locked as often as practicable when the office is occupied; but they should always be locked whenever the custodian is out of the office.

Credit Card Services

Accepting credit cards can reduce administrative costs and improve funds access and customer convenience. Customers like using credit cards because they are simpler and safer methods of payment and offer benefits to card members. However, credit card processing can substantially reduce revenue if not processed wisely and according to the rules and guidelines prescribed in the credit card agreement.

These Guidelines are designed to delegate responsibility for facilitating proper credit card controls and procedures. Further, these Guidelines provide information to establish, maintain and discontinue the acceptance of credit card transactions in payment for University services

Establishing New Credit Card Services

To establish new Credit Card service (for Visa, MasterCard or Discover), a department must contact the Controller's Office. The Controller's Office will arrange for a unique "authorized merchant number" for the department to accept credit cards. The department or school is expected to obtain, budget and pay for any costs for the following items that might be necessary, depending on the type of location:

- Dedicated phone line for card processing
- Hardware/software from equipment provider
- A "Point-of-Sale Business Guide" from the credit card processor
- Proper training provided by the credit card processor
- Necessary forms and supplies, including deposit forms for credit cards only and credit card receipts or sales drafts
- A website for online sales

Internet credit card services must also be approved by Information Technology Services to ensure that the website on which payments are received is secure, is PCI compliant and meets University standards.

A discount fee is charged to departmental budgets for all credit card transactions. If expected revenue increases are not greater than the added cost, management should seriously consider whether credit cards are an acceptable form of payment. If a transaction is processed within the rules and guidelines of the credit card agreement, fees should be lower than if they are not followed. If the transaction is not processed according to the rules and guidelines of the credit card agreement, the total fees plus additional charges/penalties will increase costs significantly.

For more detailed information on procedures for establishing a credit card location, costs, including fees, or basic rules associated with maintaining the location, contact the Controller's Office or access the information on the Controller's website.

Security, Privacy, and Confidentiality

Sales receipts/document handling: Only authorized persons should see credit card numbers. Any imprint of a credit card number must be securely stored or shredded.

Record access: Current year receipts should be readily available. In addition, the prior three (3) years' receipts (except for international transactions described below) must be retrievable when requested. Each department must securely store all receipts and related records.

Record retention and storage: The credit card agreement with the University states that each department is responsible for retaining and providing copies of transactions for a minimum of three (3) years; seven (7) years are required for international transactions.

Transaction Processing

Credit card processing procedures should be followed to ensure that the transactions are legitimate. If a transaction is fraudulent, challenged by the cardholder, or disallowed for any other reason, the disallowed amount will be charged back to the department's org. In addition, the department will incur "surcharges" for any transactions not properly processed. Procedures for processing credit card transactions are not covered in detail in these Guidelines. For detailed instructions, contact the Controller's Office or access the instructions on the Controller's Office website.

Preparation of Deposits

Departments are responsible for processing deposit forms to record credit card transactions and maintaining records such as logs of all deposits, consistent with the requirements in the **Cash Collection and Deposit** section of these Guidelines.

Reconciliation

To the extent practicable, at each location there should be segregation responsibilities for collecting, recording and reconciling credit card receipts. No one person should be responsible for all these functions, since credit card transactions are highly negotiable. However, this basic control can be difficult to achieve in a small operation. If adequate separation of duties is not possible due to lack of sufficient staff, increased involvement or supervision by management, including review and reconciliation of the deposit activity, is critical. Departments are responsible for reconciling their deposits to their month-end reports on a monthly basis and reporting any discrepancies promptly to their FOs and, if not resolved, to General Accounting, consistent with the requirements in the **Cash Collection and Deposit** section of these Guidelines.

Discontinuing or Modifying Credit Card Services

A department choosing to discontinue or modify credit card services must advise the Controller's Office in writing.

Electronic Funds Transfer Policy

Authorization to Make Electronic Fund Transfers

The Board of Trustees has empowered certain officers and administrative staff with the authority to make electronic fund transfers. Changes in the authorized persons may be made only by Board resolution.

Internal Transfer of Funds

The University transfers funds from one University account to another for cash management and investment purposes. The request to establish these transfers must be made by one authorized person and approved by another, except when a repetitive wire template has been established. In this case the Cash Manager or other individual authorized to make a repetitive wire transfer may do so without additional approvals.

All transfers of University funds must be coordinated through the University's Cash Manager to ensure that funds are available for University business needs.

Electronic Fund Transfer Payments

Departmental requests for electronic fund transfers must be made on the University's Wire Transfer request form, with required documentation including original invoice or other appropriate support. The request must include transfer instructions, including the bank, ABA number (IBAN number, SWIFT code and BIC for international transfers) and the beneficiary's account number, and be approved by authorized departmental individual(s). Wire requests of \$1,000 or greater must also be approved by two accounting managers, neither of whom is the individual making the transfer. For non-repetitive wires in excess of \$10,000, and first time repetitive wires, the department requesting the transfer is responsible for having wire instructions sent directly to the transmitting agent by an agent or official of the company. Approved transfers may be made by either ACH or wire transfer, as is appropriate, based on the transfer requirements and the cost of the different options, as determined by the individual making the transfer. Secondary confirmation is required for all non-repetitive transfers. Confirmation is not required for repetitive transfers.

Electronic payments made will be added to the University's Accounts Payable system to further document the disbursement of University funds.

Student Refunds, Accounts Payable and Payroll Direct Deposits

Student refunds, employee reimbursements and employee compensation may be made by ACH, if requested by the payee. Signed ACH authorizations (or direct deposits authorizations, as they are more commonly known) must be on file in Enrollment Services, for student refunds; Accounts Payable, for employee reimbursement; and Payroll, for employee pay, to document bank information. ACH payment requests must be processed using the same controls as

payment requests that generate checks for refund or payment. Accordingly, ACH payments may be made only to individuals who are students or employees.

Only persons authorized by the Controller's Office may establish ACH payment authority for student refunds, employee reimbursements and employee compensation.

Electronic Funds Transferred to the University

University wire instructions are available from the University's Cash Manager. Departments that receive payments by electronic fund transfers must obtain wire instructions from the Cash Manager and advise him/her of the expected dollar amount and date of receipt. The Cash Manager will notify the department when funds are received, sending a copy of the notification of deposit to the beneficiary department.

It is the departments' responsibility to ensure that funds received for their operation are appropriately recorded into their departmental orgs. The accounting department will research unclaimed funds and record them in the appropriate department budget account when identifiable. Deposits not identified or claimed within three months following the fiscal year in which they were received will be written off or returned to payer, as determined by the University Controller.

There may be circumstances when it is in the best interest of the University to receive electronic funds in University bank accounts other than the deposit account typically used. Approval of deposits in other bank accounts not managed by the University's Cash Manager must be obtained from the University Controller prior to receipt. Approval will be based on a compelling business need, departmental funding of any additional costs to the University, as well as adequate policies and procedures to safeguard the receipt and recording of the deposited funds. Any new accounts established must be approved by the Controller, Vice President for Business and Finance, Treasurer, or President.

Glossary

ABA (American Bankers' Association) Number: Bank routing number that identifies the specific bank (electronic bank address).

ACH (Automated Clearing House): Electronic transfer made through the Automated Clearing House that takes funds out of one bank and moves them to another bank. Responsible parties of either the sending or receiving account may initiate an ACH. Funds transferred by ACH generally take 24 hours to settle.

Authorized Person: Individual who has certain rights defined by University or bank policies and procedures. For purposes of these Guidelines, a person may be authorized to make electronic transfers, approve wire transfers, establish banking relationships, handle cash or credit card transactions, or grant rights to others.

Cash: For purposes of these Guidelines, cash is defined as U.S. currency (dollars and cents); personal, business, bank, and cashiers' checks; money orders; credit cards; wire transfers; and foreign drafts. The University does not accept foreign currency in payment for goods and services purchased in the United States.

Confirmation: Secondary authorization for the bank to transfer funds, given by an individual other than the one who initiated the transfer. Confirmations are required for non-repetitive wire transfers.

EFT (Electronic Funds Transfer): Generic term for the electronic transfer of funds, including wire transfers and ACH, non-repetitive wire transfers and free-form wire transfers, generally to a non-University account for the payment of goods and services.

Funds: Purchasing power either in cash or rights to cash.

Petty Cash Fund: Currency advanced to an office, department, or University unit to be used to reimburse approved small-dollar/incidental University expenditures. Receipts and/or other documentation must be used to support replenishment of the petty cash imprest balance.

Repetitive Wires: Pre-approved wire transfer templates with debit and credit bank information. Individuals authorized to make repetitive transfers may make a wire transfer from one bank account to another by using an established transfer template, inserting only the appropriate dollar amount. Repetitive wire templates are generally set up for transfers to move funds between accounts at the same company or for frequent or regular payments.

Secure Collection Station: Locations designated by Financial Officers as capable of safely securing large amounts of cash until the next business day. Secure Collection Stations should have a safe. Those that routinely maintain over \$10,000 in receipts should also have a duress/intrusion alarm. If possible, safes should be in an area that is not visible to unauthorized persons and be kept in an office that is accessible to few employees.

Wire Transfer: Electronic transfers from one bank account to another. A wire transfer is made by the sending party, and funds are settled as specified in the wire instructions (generally the same day for domestic wires, but they may be future-dated – international wires settle in 2 to 3 days).

**SOUTHERN METHODIST UNIVERSITY
POLICIES AND PROCEDURES**

BUSINESS AND FINANCE

POLICY NUMBER: 3.1

REVISED AS OF: June 1, 1994

EXPENDITURE CONTROL FOR THE UNIVERSITY

A. It is the policy of the University that the primary responsibility for controlling University expenditures will be in the Office of the Vice President for Business and Finance/Treasurer.

B. The office of the Vice President for Business and Finance/Treasurer is responsible for all accounting, bookkeeping, and/or budget control functions of the University. University personnel, whether full-time or part-time, whose duties include fiscal management, must obtain assignment and approval of fiscal matters from the office of Vice President for Business and Finance/Treasurer. For those schools or departments not having any accounting personnel assigned to them, either on a part-time or full-time basis, accounting assistance will be provided from the Office of the Vice President for Business and Finance/Treasurer.

C. Full cooperation of all University personnel is necessary to administer funds fairly and to account accurately for University expenses. Any changes in the budget as adopted must be approved in advance by an officer of the University.



SMU

Office of Associate Vice President and Controller

PO BOX 750294 Dallas, TX 75275-0294 214-768-2800 www.smu.edu/controller

Southern Methodist University
Statement of Understanding
Financial Responsibilities

I understand that as an employee of SMU with financial responsibilities that I am held to a high standard of compliance with my fiduciary obligation in the performance of my duties. To comply with this high standard, I understand that I am responsible for fostering a good control environment and acting with the utmost of care and integrity to ensure business activities are transacted in compliance with legal and University requirements, as well as good business practices. I further understand that to comply with this high standard, I should be forthright in my business activities, not misrepresenting or concealing, or allowing to be misrepresented or concealed, any financial activities.

I have read and understand the Controller's Office's *Guidelines and Procedures for Financial Transactions* and agree to comply with these University requirements. I am accountable for compliance and understand that failure to comply subjects me to disciplinary action, including termination.

Signature

Date

Print Name

SMU ID #