



SUPREME COURT OF APPEALS OF WEST VIRGINIA

General Accounting Policies and Procedures Finance Division

1. Scope.

The Supreme Court of Appeals of West Virginia (“the Court”) establishes this policy to prescribe the fiscal rules for general accounting processes relied upon the Court in conducting its business. Accordingly, this document establishes a distinct set of policies, procedures, and guidelines for general accounting processes for use by all employees of the Supreme Court of Appeals, including all Judicial Officers and Employees of Circuit Courts, Probation Officers, Family Courts, Magistrate Courts, the Administrative Office, Board of Law Examiners, Office of Disciplinary Counsel, the Supreme Court of Appeals’ Clerk’s Office, Circuit Clerks and their employees, and the Judicial Investigation Commission.

To the extent these rules fail to provide the adequate guidance in addressing or resolving a specific problem or question related to general accounting processes, the Administrative Director and Chief Financial Officer (“CFO”) shall address the matter and, with approval of the Court, establish the fiscal rules to be followed in these special situations.

Breaches of this policy may result in disciplinary or other corrective action. Address any questions regarding this policy to the CFO.

2. Cash Handling Procedures.

2.1 Definitions.

- (a) *Cash*. Money or its equivalent in the form of coins, currency, money orders and checks.
- (b) *Other*. For additional definitions of terms used in this policy, please refer to the ‘definitions’ section of the West Virginia State Treasurer’s Office (“STO”) Cash Receipts Handbook for West Virginia Spending Units. The Cash Receipts Handbook is available on the State Treasurer’s Office web site at <https://www.wvsto.com/>.

2.2 Overview.

- (a) Generally, the procedures detailed in this policy follow the West Virginia STO Cash Receipts Handbook for West Virginia Spending Units, as referenced above and found at <https://www.wvsto.com/>.
- (b) Cash must be handled with the highest security.
- (c) Each Court division/department with the authority to collect monies must have policies and procedures that detail all actions required at each step in the collection, handling, and depositing processes. These policies and procedures must give each employee a clear understanding of what is expected, what behavior is and is not

Effective Date:	2019 01-07
Revision Date:	2019 01-07
Review Date:	2019 01-07

acceptable, and how to accurately accept, handle, and safeguard cash. The policies and procedures must also be clear as to which employees have access and the ability to perform each task required in the entire process. Employees must understand their accountability for all cash which is due the State of West Virginia.

2.3 Safeguards.

- (a) Once cash is received, it must be protected immediately. It must be stored in a locked, fireproof cash drawer, safe, or other secure place until it is deposited.
- (b) Every division/department must provide a secure area for processing and safeguarding the cash and restrict the area to a minimum number of authorized employees only.
- (c) A limited number of people should have access to the secured receipts to prevent any mishandling.
- (d) Cash must be counted by two, authorized employees out of sight from the general public.

2.4 Segregation of Duties and Internal Controls. Following the standards outlined in this policy, each division/department must establish proper segregation of duties and checks and balances, which includes cash collecting, depositing, reconciling, and reporting.

- (a) Unless otherwise authorized by the CFO, an individual is not to have at any time the sole responsibility for more than one of the following cash handling components:
 - collecting
 - depositing
 - disbursing
 - reconciling
- (b) The employee taking a payment must not also prepare the deposit and/or make the deposit at the bank.
- (c) There must be dual signatures verifying any moneys transferred to the bank.
- (d) The bag holding such moneys must be sealed and/or locked before it leaves the division's/department's location.
- (e) The employee collecting the money or making the deposit must not also reconcile the funds.
- (f) Divisions/departments must use dual control when employees are authorized to accept cash and enter deposits into the Court's accounts receivable system.

2.5 Mail Payments.

- (a) Two employees should be present when opening the mail.
- (b) All checks received in the mail should be endorsed immediately. See Section 2.6 (a) below.
- (c) One of the employees present when the mail is opened shall date-stamp all enclosed documents.

2.6 General Requirements.

- (a) To decrease the risk of theft, all checks received must be endorsed immediately. The endorsement stamp must be restrictive and contain the words FOR DEPOSIT ONLY.
- (b) The Court has several outside bank accounts that are approved and monitored by the WV State Treasurer's Office as set forth in West Virginia Code §12-2-3. Any division/ department in need of an outside bank account must obtain approval from the Court's CFO before obtaining approval from the State Treasurer's Office.
- (c) All bank account information and activity must be recorded in the *wvOASIS* accounting system.
- (d) Under NO circumstances is an employee permitted to comingle Court received funds with his/her own personal funds, deposit the received funds in a personal bank account, or take the received funds home for safekeeping.
- (e) Cash received must not be used to establish an imprest fund or petty cash fund. Expenditures or refunds cannot be made from cash receipts. If an imprest fund is needed, please contact the Court's CFO for approval.
- (f) A check or money order received must be reviewed for completeness:
 - Verify that the accountholder's name, address and phone number are included on the check.
 - Verify that the check has a bank name listed, and that the routing number and customer's bank account number are encoded on the bottom edge of the check.
 - Note the date. Do not accept post-dated or stale dated checks and do not agree to hold a check for future deposit. Post-dated checks have a date in the future; stale dated checks have a date of six months ago or longer.
 - Verify that the amount written in numbers matches the amount written in words.
 - Verify that the check is signed and made payable to the appropriate department.

(g) Cash can be received via counter payments or by mail. A pre-numbered receipt must be issued for each counter payment at the time the funds are received. Receipts must be pre-numbered regardless of whether the department has computer generated or handwritten receipts.

(h) Receipts must be prepared in duplicate. The original must be given to the individual from whom the funds were received at the time the cash was remitted. The copy must be retained in numeric order, either in the receipt book or in a file established for this purpose. Every receipt issued must show the following information:

- amount received,
- date received,
- type of cash (coin, currency, money order, or check),
- check or money order number, if applicable,
- name of the individual/company from whom received,
- purpose of the collection for which the cash was received, and,
- division/department name and employee name that prepared the receipt.

(i) If an employee makes an error while preparing a receipt, the employee is to void the receipt and issue another one. To void a receipt, write the word "VOID" across the face of the receipt and retain the original along with the copy in the receipt file. DO NOT discard voided receipts. All receipt numbers must be tracked and accounted for within the division/department. The pre-numbered receipts help aid in the reconciliation process and theft prevention. Any missing receipts should be investigated.

(j) Each division/department must have a daily itemized record of the collections received. The daily itemized record should contain the following:

- name of person or entity,
- amount collected,
- date of collection,
- purpose of collection,
- type of cash (coin, currency, money order, or check),
- check or money order number, if applicable, and,
- name of employee who prepared the receipt.

(k) An employee other than the staff member that made the bank deposit must perform a reconciliation of the supporting documentation (itemized record) to the bank validated deposit tickets daily. The employee must sign and date the reconciliation to reflect who performed the reconciliation and when. Any differences that exist should be investigated.

(l) All cash receipts and related documents must be kept in accordance with the Court's record retention policy.

(m) West Virginia Code §12-2-2 requires that all cash collections must be deposited within one business day of receipt.

3. Credit Card Handling Procedures.

(a) Generally, these procedures follow the West Virginia STO's Credit Card Handling Handbook for West Virginia Spending Units, which provides guidance regarding the receiving, handling, and acceptance of electronic payments by spending units and their employees.

(b) Strong internal controls for electronic payments are designed to safeguard and protect consumer information as well as to protect employees from inappropriate charges of mishandling transactions.

(c) These procedures ensure the accurate and secure receiving and processing of electronic payments at various locations throughout the State.

3.1 Safeguards.

(a) **Payment Card Industry Data Security Standards ("PCI-DSS")** are security standards developed for organizations that handle branded credit cards to protect cardholder data. Court divisions/departments that accept credit card payments must do so in accordance with PCI-DSS.

(b) All technology and business processes implemented in association with transmitting, storing or processing credit cards must be in accordance with the PCI-DSS. The cost of equipment or other related business processes will be the responsibility of the divisions/departments.

(c) **Sensitive Card Data.** In accordance with PCI-DSS, divisions/departments are prohibited from storing sensitive cardholder data on any systems, databases, spreadsheets, email, or in paper files. PCI-DSS classifies the following as sensitive card data:

- Security codes (CVV2, CVC2, and CID)
- PIN/PIN block
- Full magnetic stripe data or equivalent data on a chip
- Full Personal Account Number ("PAN")

(d) **Personal Identifiable Information ("PII")** is data that can be used to recognize an individual's identity such as social security numbers, date of birth, email address, bank account number, etc. Divisions/departments are responsible to safeguard the customers' PII.

(e) Rules and regulations govern protection of PII. A Best Practice in the protection of PII is to routinely conduct an audit at the division/department level to ensure PII protection, as well as PCI-DSS compliance, in all aspects of the organization including

governance, procedural, and operational levels. Divisions/departments are responsible to protect all customer PII when processing payments.

3.2 General Requirements.

(a) **Swipe/insert or enter the card through the point of sale (“POS”) system.** Avoid manually keying card information whenever possible. This helps reduce the chance of errors. Cards swiped/inserted directly into the POS typically have lower interchange fees than those manually keyed.

(b) **Validate the card.** Check the expiration date, ensure the payment brand emblem is present, and ensure that the card is not altered.

(c) **Obtain a signature.** Obtain a signature on the receipt or invoice.

(d) **Prohibit storage of cardholder data.** The prohibition for divisions/departments to store cardholder data serves to protect the division/department, the Court, and the State of West Virginia against becoming targets of theft.

(e) **Properly authorize the transaction.** Confirm the authorization response provided and take the appropriate action. Responses to transactions include “Approved”, “Declined”, “Call Center”, or Pick Up”.

(f) **Settle the transactions daily.** Transactions not settled within a day are subject to higher interchange rates. Settling daily also helps to ensure that any issues are addressed more quickly.

(g) **Telephone Payments.** DO NOT accept credit card payments over the phone or if the card is not present.

(h) **Maintain records of supporting information to help complete research and disputes when needed.** Maintaining internal records of receipts and/or invoices (where applicable) can assist staff in investigating fraud if suspected and provides historical documentation in the event a chargeback occurs.

(i) **Confirm the purchase with the customer.** Especially on large ticket items, incorporate transaction confirmation into the customer service process to validate the transaction with the customer.

3.3 Credit Card Fraud.

(a) If fraud is suspected with the credit card terminal and/or the terminal has been tampered with, the division/department should contact the acquiring bank and local law enforcement immediately. The acquiring bank would notify its Loss Prevention department, and Loss Prevention would send a request to have the v# (terminal ID) closed and a replacement terminal sent out if desired

(b) If it is suspected that that merchant account or merchant terminal was compromised, the merchant account will be closed, a new merchant account (“MID”) will be opened and a replacement terminal will be sent.

(c) If a card is presented that has been coded as “fraudulent/lost/stolen,” the terminal will decline the transaction. In this instance, the division/department should ask the customer for another form of payment. If the customer has questions, they should be directed to call their bank

4. Form-1099 Standards.

(a) **1099 Requirement.** The Internal Revenue Service requires that recipients of certain financial transactions pay taxes on those transactions. The Court is required to notify recipients of such taxable transactions through the issuance of a Form 1099. The most common Form 1099 issued by the State of West Virginia, through the Department of Administration, is 1099-MISC for miscellaneous income received by a contract employee.

(b) **Issuance of 1099.** Original and duplicate Form-1099’s are issued by the WV Department of Administration during the month of January each year. Modifications to Form-1099’s can be completed by the Court’s Finance Office during a limited time frame. It is imperative that any changes to a Form-1099 be communicated immediately to the Finance Division.

5. Vendor/Customer Setup.

(a) **Requirement.** All Court vendors and service providers must be setup as a vendor/customer with the State of West Virginia, Department of Administration before the Court can provide payment to a vendor for providing goods or services to the Court.

(b) **W-9.** The Court Finance Division processes this setup in the wvOASIS accounting system once a W-9 is received from the vendor. Final approval of a vendor/customer rests with the WV Department of Administration.

(c) **Contract Requirement.** In order to effectuate payment through the Finance Division and State Auditor’s Office, all established vendors must have a contract with the Court in place. This requirement standardizes and defines the terms and conditions of the vendor relationship and is designed as a protection to all involved. Establishment of the contract must be facilitated through the Legal Division and Finance Division and should be completed prior to commencement of the vendor’s provision of goods and/or services.

(d) **Other Requirements.** There are other State requirements in establishment of the vendor relationship that will be reviewed with the Court division/department by the

Finance Division and Legal Division in the process of establishing the vendor relationship as outlined in this policy.

The details of this policy and all Court policies are subject to modification by the Court at any time as situations, standards, and legal requirements may change. The Court will ensure that all employees are notified of any such modification in a timely fashion.