

SOPP #127	<u>Prepared By:</u> Department of Finance
<u>Effective Date:</u> 08/10/2026	<u>Approved By:</u>
Title	Credit Card Processing & Daily Settlement
Purpose	To mandate uniform processing, daily settlement, recording, safeguarding, and reconciliation of all credit card transactions processed by Departments and Agencies (D&As), ensuring timely revenue recognition, protection of public funds, and compliance with internal control, audit, and statutory requirements.
Policy	All Departments and Agencies that accept credit card payments shall: • Perform daily settlement of all credit card transactions on each business day activity occurs, without exception • Record all revenues in the Enterprise Resource Planning (ERP) system (e.g., Tyler Munis) within the required timeframe • Ensure timely deposit verification and reconciliation of funds • Maintain complete and auditable supporting documentation • Verify that all credit cards presented match a valid government-issued photo identification prior to processing the transaction Daily settlement is mandatory regardless of transaction volume. All Departments and Agencies must utilize only Department of Finance (DOF)-approved payment platforms, merchant accounts, and systems. Independent establishment of payment systems is strictly prohibited unless authorized by DOF. Failure to comply with this SOPP constitutes a violation of established financial controls and may result in corrective, administrative, or disciplinary action.
Accepted Credit Card Types (Mandatory)	• The GVI accepts Visa and Mastercard only • American Express and Discover are strictly prohibited • Departments and Agencies shall not process or attempt to process unauthorized card types • Non-compliance with accepted card standards will result in corrective action.

Responsibilities	Departments and Agencies • Perform daily settlements and ensure timely ERP recording • Maintain complete, accurate, and auditable documentation • Ensure identity verification is performed prior to processing transactions • Investigate and resolve discrepancies promptly Supervisors / Management • Ensure staff are trained and authorized • Ensure compliance with ID verification requirements • Perform and/or approve settlements (as required) • Enforce strict compliance with this SOPP • Review ERP entries and reconciliations Department of Finance – Treasury Division • Provide oversight, compliance monitoring, and enforcement • Verify deposits and perform reconciliations • Approve payment systems and merchant accounts • Escalate unresolved or repeat violations to leadership
Procedures	1. Daily Settlement • Credit card terminals and merchant systems shall not be settled prior to 3:00 PM • Settlements must occur once and only once per business day • Settlement must be performed by authorized supervisors or managers only • Multiple or unauthorized settlements are strictly prohibited 2. Credit Card Verification Requirement • Prior to processing any in-person credit card transaction, the cashier must: ○ Request a valid government-issued photo ID (e.g., driver's license, passport) ○ Verify that the name on the credit card matches the name on the ID ○ Confirm that the individual presenting the card is the authorized cardholder

- Transactions **must not be processed** if:
 - The names do not match
 - The individual refuses to provide identification
 - The authenticity of the card or ID is questionable
- Any suspicious activity must be reported immediately to a supervisor and documented

3. Prohibition of Manual Credit Card Processing

- All credit card transactions must be processed electronically through DOF-approved, secure payment systems at the time of the transaction.
- Manual processing of credit cards is strictly prohibited, including:
 - Keying in card numbers without the physical card present (unless explicitly authorized by the Department Head or Chief Financial Officer.
 - Use of paper imprints or manual slips;
 - Recording or storing cardholder information for later processing; and
 - Processing transactions outside of approved merchant platforms.
 - Under no circumstances shall cardholder data be written down, stored locally, or retained outside of PCI-compliant systems.

Limited Exception – Manual Credit Card Entries

- In the event a manual credit card transaction is deemed necessary due to terminal malfunction or the inability of an approved merchant terminal to read a physically present credit card, the transaction may only be processed upon prior approval from the Department Head or Chief Financial Officer.
- Prior to processing any manually entered credit card transaction, the following documentation is required:
 - A completed and signed Credit/Debit Card Authorization Form;
 - A signed certification and acknowledgment by the cardholder authorizing the transaction;
 - A copy of a valid government-issued photo identification (e.g., driver's license, passport, or state-issued identification card); and
- Verification that the name on the government-issued identification matches the name appearing on the credit card.
- All supporting documentation shall be maintained in accordance with applicable records retention requirements and made available upon request for audit or compliance review.

- Manual credit card transactions that are not accompanied by the required authorization form, signed acknowledgment, and valid government-issued identification are strictly prohibited and shall not be processed.

Manual Debit Card Transactions

- Manual entry of debit card information is strictly prohibited under all circumstances when the customer is not physically present.
- Departments and Agencies shall not process debit card transactions over the telephone or by any other means that do not allow the cardholder to personally enter their Personal Identification Number (PIN).
- Debit card transactions shall only be processed when:
 - The cardholder is physically present;
 - The debit card is inserted, tapped, or swiped through a DOF-approved merchant terminal; and
 - The cardholder personally enters their PIN, when required.
- Violations of this requirement will be treated as a serious breach of financial controls, PCI DSS standards, and Department of Finance policies and may result in:
 - Immediate suspension of merchant processing privileges;
 - Audit findings;
 - Corrective or disciplinary action; and
 - Referral to executive leadership for further review.

4. Revenue Recording

- All settled transactions must be recorded in the ERP as **cash receipts/payment entries**
- Recording must occur **within 24 hours of settlement**
- All entries must include proper coding (fund, org, object) and supporting documentation

5. Deposit Verification

- DOF Treasury shall verify that all settled funds are transmitted to designated bank accounts
- Any discrepancies between settlement totals and bank activity must be:
 - Identified immediately
 - Documented
 - Resolved without delay

	6. Reconciliation DOF shall perform daily reconciliation between: • Credit card settlement/batch reports • ERP cash receipt entries • Bank deposit confirmations All discrepancies must be investigated and resolved immediately. Unresolved issues shall be escalated. 7. Supporting Documentation (Mandatory) Departments and Agencies must maintain and upload to ERP: • Credit card settlement/batch reports • ERP cash receipt confirmations • Bank deposit confirmations/slips • Supporting documentation for adjustments or exceptions Failure to maintain or upload documentation constitutes non-compliance.
Internal Controls	Segregation of Duties • Collection, recording, reconciliation, and approval must be separated where feasible Access Controls • System access must be role-based and periodically reviewed • Unauthorized access is prohibited Security & Compliance • All entities must comply with PCI DSS standards • Cardholder data must not be stored locally unless explicitly authorized and secured • Manual handling, recording, or storage of cardholder data is strictly prohibited and constitutes a violation of PCI DSS compliance requirements.
Exception Handling (Mandatory Reporting)	• Failed settlements, processing errors, or suspicious transactions must be reported to DOF within one (1) business day

	• Corrective actions must be documented and tracked until resolved • Affected transactions must be corrected in the ERP
Compliance & Accountability	Failure to comply with this SOPP will result in corrective or enforcement action, including but not limited to: • Formal written notice of non-compliance • Increased monitoring or reporting requirements • Suspension of credit card processing privileges • Referral to executive leadership or oversight bodies • Inclusion in audit findings • Administrative or disciplinary action

Revision#	Date	Description of changes	Requested By
0	04/16/2026	Initial Release	BC,AH,RS
1	04/16/2026	Review	MW
2	05/06/2026	Final Review	KM
3	05/06/2026	Approval	KM
4	07/24/2026	Update Policies and Procedures	BC,AH,RS
5	08/05/2026	Review	MW
6	08/06/2026	Final Review	KM
7	08/07/2026	Approval	KM