STATE OF ALASKA DEPARTMENT OF MILITARY AND VETERANS' AFFAIRS STANDARD OPERATING PROCEDURES	REVISION NO. 1.0	PAGE 1 of 8
	ISSUED March 4, 2025	EFFECTIVE Upon Issuance
SUBJECT: DMVA One Card Standard Operating Procedures / Internal Controls	**APPROVED BY:** DMVA Finance Officer	

PURPOSE:

This SOP establishes the procedures for managing, issuing, using, reconciling, and securing the One Card Alaska program within DMVA. It ensures compliance with AAM policies and defines department-specific responsibilities.

SCOPE:

This SOP applies to all DMVA employees issued a One Card for procurement or travel, as well as supervisors, program administrators, and financial personnel responsible for oversight.

AUTHORITY:

AAM 38.300 – 360
AAM 60.070

DEFINITIONS:

Approving Officer: Individuals who are delegated the authority to approve invoices, adjusting journal entries, reimbursable service agreements, Travel Authorization forms, and personnel documents on behalf of their division.

Cardholder: A state employee authorized to use the One Card for state-approved purchases, responsible for card security and appropriate use.

Central Travel System (CTS) Account: A card-not-present account used by state agencies for booking air travel, lodging, and car rentals primarily through E-Travel Online.

Corporate Travel Management (CTM): The travel management provider contracted by the state which provides travel booking services.

Department Program Administrator (DPA): The individual designated within a state department to oversee the One Card Alaska program, enforce policies, and manage account activities.

Merchant Category Code (MCC): A four-digit code assigned by credit card networks to categorize a business based on the types of goods or services it provides. Used to enforce spending restrictions.

One Card: A Visa corporate charge card (the card) that may be used by a state employee with any merchant who accepts Visa. The card may be used for in-store, mail, phone, fax, or internet purchases.

ROLES & RESPONSIBILITIES:

The full list of responsibilities can be found in AAM 38 with an abbreviated version below:

Department Finance Officer

- Ensures compliance with AAM 38, as well as all applicable state procurement policies and financial regulations.
- Conducts periodic audits to identify policy violations, unauthorized purchases, or potential fraud.
- Provides guidance on proper financial coding and allocation of transactions.
- Assists in resolving financial discrepancies related to card transactions.
- Works with the DPA, issuing bank, and Division of Finance PCard Support Team to investigate and resolve fraudulent or disputed charges.
- If the Finance Officer vacates their role or is unable to perform their duties, a replacement must be designated, trained, and granted system access to ensure program continuity. If no immediate replacement is available, the DAS Division Operations Manager assumes oversight until a new Finance Officer is assigned.

Department Program Administrator (DPA)

- Acts as the primary liaison between DMVA and the issuing bank.
- Ensures proper issuance, maintenance, and cancellation of cards.
- Oversees the online card management system.
- Delegates access and responsibilities to Program Administrator Delegates as needed.
- Ensures compliance with PCI Data Security Standards.
- Reviews and approves requests for spending limit adjustments and policy exceptions.
- Monitors One Card transactions for adherence to spending limits, purchase restrictions, and reconciliation deadlines.
- Works with the Department Finance Officer, issuing bank, and Division of Finance PCard Support Team to investigate and resolve fraudulent or disputed charges.
- If the DPA vacates their role or is unable to perform their duties, a replacement must be designated, trained, and granted system access to ensure program continuity. If no immediate replacement is available, the Finance Officer assumes oversight until a new DPA is assigned.

Program Administrator Delegates

- Assists the DPA with card management in the online system.
- Sets up, modifies, or deletes cardholder accounts as authorized.
- Ensures card issuance and maintenance comply with DMVA policies.

Supervisors

- Request One Cards for eligible staff who have procurement authority or travel responsibilities.
- Ensure proper use of the card in accordance with DMVA and state policies.
- Ensure card destruction upon employee separation and document on the Employee Clearance Form.
- Notify the DPA of cardholder separations, transfers, or leaves of absence.

Cardholders

- Use the One Card only for authorized purchases or travel-related expenses.
- Follow AAM 38.310 for purchase documentation and reconciliation.

- Maintain the security of card data, such as the account number, the expiration date, and the card verification code (CVC).
- Report lost or stolen cards within 24 hours of discovery to the issuing bank, supervisor, and DPA.
- Submit invoices and supporting documentation to DAS payables section within two days of purchase.
- Submit a completed Travel Authorization form with all receipts within five days after trip completion.

CARD ISSUANCE & MAINTENANCE:

Requesting a One Card

- Supervisors or division administrative staff must submit a request to the MVA DAS Admin mailbox, providing the following:
    - One Card Cardholder Usage Agreement signed by the cardholder and either supervisor, manager, or Division Director signature.
    - DMVA Delegation of Purchasing Authority signed by the cardholder and Division Director.
    - Procurement Certification Level I, II, or III. The Request for Level I Procurement Certification found within the Alaska Public Procurement Academy Level I online manual is acceptable.
- DAS administrative staff will route the One Card Cardholder Usage Agreement and DMVA Delegation of Purchasing Authority forms for further approval.
- The DPA will review and approve requests in accordance with AAM guidelines. Once approved, the DPA will place an order for a physical One Card to be delivered to DAS for distribution.

Card Setup & Security

- All cards must be configured with appropriate spending limits and MCC restrictions per DMVA purchasing and travel policies.
- ATM cash advances for meals and incidental expenses (M&IE) are enabled by default. However, M&IE cash advances are only permitted under specific travel circumstances.

Employee Transfers or Separations

- Supervisors must ensure the One Card is destroyed and notify the DPA before the employee's last working day.
- The DPA must cancel or inactivate the account in the online management system.
- Cardholders going on seasonal leave must turn in their cards for secure storage by the agency until they return.

CARD USE & RESTRICTIONS:

General Guidelines

- Cardholders must use the card for official DMVA business only.
- Single transaction and monthly spending limits are based on the cardholder's procurement delegation and must be adhered to.
- Unauthorized personal purchases are strictly prohibited. Use of the card in any manner not in accordance with program policies may result in personal liability, revocation of the card, and all purchasing authority, and disciplinary action up to and including dismissal in accordance with applicable collective bargaining agreements. Instances of inappropriate

charge card use will be reviewed by the department finance officer and acted on depending on the seriousness of the offense and number of repeat violations.

Travel Guidelines

- Airline Tickets - Airfare should be charged to the traveler's card or a CTS account.
- Lodging – The cost of lodging expenses should be charged to the traveler's card, a CTS account, or should be direct billed.
- Rental Cars – All rental car expenses should be charged to the traveler's card, a CTS account, or should be direct billed.
- Meals and Incidental Expense Allowance – State travelers receive a per diem allowance to cover meals and incidental expenses, with any travel advances deducted accordingly. As such, the card should not be used for purchasing meals as these are not an authorized state expenditure.
- ATM cash advances for M&IE allowances are permitted under specific travel circumstances and generally limited to 80% of estimated M&IE.

Prohibited Transactions

- Personal use – If the amount of the personal use is over $500, the cardholder may be subject to felony prosecution.
- Splitting purchases to circumvent transaction limits (fragmentation).
- Circumventing procurement, travel, or payment procedures.
- Bypassing or replacing the contract award process.

PROGRAM CONTROLS & SECURITY:

Point-of-Sale Controls

- The issuing bank provides several controls, including:
    - Single transaction limits for procurement and travel.
    - Monthly spending limits per cycle.
    - Merchant category code (MCC) restrictions to limit purchases by vendor type.
    - ATM cash access restrictions set at a 20% limit by default.

CARD DATA SECURITY & STORAGE:

PCI Data Security Standards

- In compliance with AAM 38.335 and PCI Data Security Standards, the storage and handling of One Card Alaska account information must follow strict security protocols:
    - Permitted Storage: Card and account numbers may be stored in the state's contracted travel agency's reservation database for travel-related purchases, provided it meets PCI compliance. Secure access to full account details may also be available through the issuing bank's online card management system for authorized personnel.
    - Prohibited Storage: Full card numbers, expiration dates, and CVC codes must not be retained in spreadsheets, emails, hard copies, or non-secure digital locations. Cardholder data must never be stored on personal devices or in shared file systems unless explicitly approved and secured in compliance with PCI standards.
    - Access Controls: The DPA and other authorized personnel must access card details only through secure, approved systems and should ensure that access is limited to those with a business need.

Secure Transmission

- Cardholder data must only be transmitted through encrypted channels (e.g., encrypted email or secure file transfer systems). Card details must never be sent via unsecured email or messaging platforms.
- Authorized personnel may access full card details only through the issuing bank's online card management system or other approved encrypted systems.

GROUP, SHARED, AND UTILITY CARDS:

The Department of Military and Veterans Affairs (DMVA) may issue Group, Shared, or Utility Cards to facilitate purchases and travel-related expenses in scenarios where multiple authorized users need access. These cards must be administered and maintained securely under the guidelines established by the State of Alaska and the One Card Alaska program.

Administration & Access Controls

- Designated Administrator: Each shared card must have a primary Administrator responsible for oversight, security, and compliance. This individual must:
  - Maintain a list of all authorized users.
  - Ensures users acknowledge and comply with all card policies.
  - Monitor transactions for compliance with state policies.
  - Securely store and manage card details in compliance with AAM 38.335 and PCI standards.
  - Immediately report any unauthorized transactions, lost, or stolen cards.
- Authorized Users: Only pre-approved department personnel with individual purchasing delegation may use a group/shared card. A log of authorized users must be maintained, including usage justifications and access duration.
- Access Restrictions: Authorized users must not store or share full card details outside of secure systems. Access should be granted on a need-to-know basis and reviewed periodically.

Security & Data Storage Compliance

- Permitted Storage:
  - Card and account numbers may be stored in the state's contracted travel agency's reservation database for travel-related purchases, provided it meets PCI compliance.
  - Authorized personnel may access full account details through the issuing bank's online card management system.
- Prohibited Storage:
  - Card numbers, expiration dates, CVC codes, or other sensitive data must not be stored in non-secure formats, including spreadsheets, shared drives, emails, or hard copies (AAM 38.335).
  - If a cardholder is assigned a shared card, they may only access the last four digits when necessary to complete transactions.

Usage & Accountability

- Spending Limits & Restrictions:
  - Transactions must comply with AAM 38.340 (Program Controls), including single transaction limits, monthly spending caps, and Merchant Category Code (MCC) restrictions.

    - Utility cards must not be set up on any autopay system to ensure proper review and approval of all transactions before payment. All charges must be manually reconciled and approved per AAM 38.345.
    - Generally, credit limits for group, shared, and utility cards will default to $5,000 to safeguard against employees spending beyond their procurement limits. Requests for higher credit limits will be reviewed and approved on a case-by-case basis by the department Procurement Officer and Finance Officer.
- Periodic Access Review:
    - The Administrator must conduct a review of authorized users every six months to ensure that access is still required and to remove any inactive users from the authorized list.
- Audit Oversight:
    - The DPA must conduct quarterly audits of group/shared card transactions to verify compliance with state policies and to identify any irregularities.
- Cash withdrawals (ATMs) are generally prohibited unless pre-authorized for specific business purposes.

Reconciliation & Compliance

- Timely Review:
    - Purchases made with shared cards must be reviewed and submitted for reconciliation within two business days (AAM 38.345).
- Audit & Review:
    - The DPA is responsible for regular audits to ensure compliance with One Card policies.
    - Discrepancies or potential misuse must be reported immediately to the DMVA finance office and the issuing bank per AAM 38.350 (Dispute Resolution).

Card Cancellation & Inactivation

- If a shared card is no longer needed or if an authorized user transfers or separates from DMVA, the DPA must cancel or reassign the card in accordance with this SOP and AAM 38.355.
- Cards assigned for temporary projects must have an expiration date set at issuance to prevent unauthorized use.

RECONCILIATION & PAYMENT PROCESSING:

Transaction Review & Approval

- Cardholders must submit their invoices and other purchase support documentation to the DAS payables section within two days of purchase.
- Travelers or division administrative staff must submit completed Travel Authorizations and support documentation to the travel desk within five days after trip completion.
- Reconciliation must be performed by someone other than the cardholder.

AutoPay & Financial Coding

- Transactions post to the agency's default PCard suspense account via the AutoPay system until reconciled.
- Division administrative staff designated as an Approving Officer must ensure correct financial coding and submit to the DAS payables section for processing.

Annual Deadlines

- All transactions from the prior fiscal year must be reconciled by mid-to-late August.

- Travel-related One Card transactions from July–December should be cleared by December 31 as a deadline for taxable travel payments for the calendar year.

DISPUTES & FRAUD PREVENTION:

Disputing a Charge

- The state does not deduct disputed amounts from payments to the issuing bank. Instead, disputed amounts are initially paid and the state seeks credit for amounts overpaid.
- Cardholders, reconcilers, and/or the DPA should first attempt to resolve disputes with the vendor.
- If unresolved, transactions must be disputed with the issuing bank within 60 days of the statement date.
- The DPA must monitor disputes to ensure timely resolution.

Lost or Stolen Cards

- Cardholders must report lost/stolen cards within 24 hours of discovery to:
    - The issuing bank (contact info available on the Division of Finance website).
    - Their immediate supervisor.
    - The DPA for account cancellation or replacement.

Fraud Detection & Reporting

- Fraud is usually detected by one of two ways:
    - If the One Card holder discovers a fraudulent charge, it is the responsibility of the cardholder to contact the issuing bank as soon as possible to report the fraud.
    - The issuing bank monitors all DMVA One Card accounts for fraudulent activity and issues fraud referral notifications by email to the Division of Finance PCard Support Team. The fraud referral email is then forwarded to the One Card holder with a block placed on the account. It is the responsibility of the cardholder to contact the issuing bank's Fraud Assistance division to verify if there is fraud.
- Cardholders, supervisors, and the DPA must ensure timely action to protect the state's financial interests.

Recordkeeping

- Purchase documentation must be maintained per SOA and DMVA record retention policies.
- DMVA finance personnel must ensure compliance with reconciliation deadlines.
- The DPA must conduct annual audits to review card usage, approvals, and program compliance.

REVISION HISTORY AND REVIEW CYCLE:

Revision Date	Revision Number	Description of Changes	Reviewed By	Approved By
March 4, 2025	1.0	Initial Release	Pamela Wiederspohn	Pamela Wiederspohn

Review Cycle

- This SOP will be reviewed annually by the Department Program Administrator (DPA) and Department Finance Officer to ensure compliance with current AAM policies and DMVA requirements. Updates will be made as needed based on policy changes, operational adjustments, or audit findings.

CONCLUSION:

This SOP aligns DMVA's One Card administration with AAM policies, ensuring clear roles, accountability, and financial integrity. Compliance with these procedures protects DMVA against fraud, misuse, and financial liability.