



The American Legion Department of Ohio

Unified Electronic Payment Handling & Financial Data Protection Policy

1. Purpose

This policy establishes mandatory procedures for securely handling, processing, documenting, and destroying all electronic payment information—including Automated Clearing House (ACH) transactions and credit card data—handled by the American Legion Department of Ohio. It ensures compliance with Generally Accepted Accounting Principles (GAAP), National Automated Clearing House Association rules (NACHA), Payment Card Industry Data Security Standard (PCI DSS), and Department fiscal governance while protecting the financial privacy of individuals, vendors, Posts, Districts, and programs.

2. Scope

This policy applies to:

- Department Officers
- Finance Committee members
- Employees, contractors, and volunteers handling financial data
- Vendors and service providers submitting ACH or credit card information
- Posts, Districts, and Programs transmitting payment information to the Department

3. Policy Statement

The American Legion Department of Ohio shall:

- Process all ACH payments and credit card transactions in a manner that protects financial data, maintains bank account privacy, and adheres to GAAP and Department fiscal controls.
- Prohibit the storage of full credit card numbers or sensitive authentication data under any circumstances.
- Require secure transmission, restricted access, and timely destruction of all sensitive financial information.

4. ACH Payment Handling Procedures

4.1 Authorization

- All outgoing ACH payments must be authorized in writing by the Department Finance Officer or an Executive Committee-approved signer.
- Incoming ACH information must be verified before acceptance or entry into Department systems.

4.2 Documentation Requirements

- Each ACH transaction must include supporting documentation such as invoices, vouchers, reimbursement forms, or program authorizations.
- Documentation must be retained for seven (7) years, or longer if required by audit or regulatory standards. However, destroy all sensitive financial data immediately, as outlined in section 5.2 below.

4.3 Reconciliation

- ACH transactions must be reconciled monthly by personnel independent of the initiator.
- Reconciliation must follow GAAP standards and Department accounting procedures.

5. Bank Account Privacy & Data Security

5.1 Confidentiality of Bank Information

- Bank account numbers, routing numbers, and other financial identifiers are classified as confidential financial data.
- Access is restricted to authorized personnel with a legitimate business need.

5.2 Secure Storage and Transmission

- ACH information must be stored only in encrypted, access-restricted systems approved by the Department Finance Officer.
- Electronic transmission of bank data must use secure, encrypted channels.
- In accordance with PCI DSS/National Institute of Standards and Technology (NIST) standards, ACH bank account information must be destroyed immediately after entry into Department systems.

5.3 Prohibited Actions

No Department Officer, employee, or volunteer may disclose bank account information to any external party except:

- The Department's financial institution
- Authorized auditors
- Entities legally entitled to the information

Unauthorized disclosure may result in disciplinary action or referral to appropriate authorities.

5.4 Third-Party Vendor Compliance

Vendors handling ACH data must comply with:

- GAAP
- NACHA rules
- Applicable federal and state privacy laws

Contracts must include mandatory data-protection clauses reviewed by the Department Judge Advocate.

6. *Credit Card Information Handling & Destruction*

6.1 Prohibited Storage of Credit Card Data

The Department shall not store or retain:

- Full credit card numbers
- CVV/CVC security codes
- Magnetic stripe data
- Chip data
- PINs
- Images or photocopies of credit cards

Retain only the last four digits for reconciliation or audit documentation.

6.2 Acceptable Use

Credit card information may only be used for:

- Processing authorized payments
- Validating payment details during a transaction
- Resolving immediate transaction errors

Destroy all sensitive data immediately after the transaction is completed and verified.

6.3 Required Destruction Procedures

The Office Manager is responsible for ensuring all sensitive data is destroyed immediately after the transaction is completed and verified.

Paper Records

Destroy immediately using:

- Cross-cut shredding
- Secure shredding service with documented chain of custody
- Locked destruction bins monitored by authorized personnel

Electronic Records

Destroy using:

- Secure deletion tools that overwrite data
- Permanent deletion from the POS systems
- Removal from email, attachments, scanned documents, or cloud storage
- Purging from temporary files, caches, or logs

Screenshots, photos, or digital images containing credit card data are strictly prohibited and must be deleted immediately if received.

6.4 Transmission Restrictions

Credit card information may not be transmitted via:

- Email
- Text message
- Social media
- Unencrypted digital forms
- Standard file attachments

If transmission is unavoidable, it must use a PCI-compliant encrypted payment portal approved by the Department Finance Officer.

6.5 Access Controls

Only authorized personnel can handle credit card information. Limit access to individuals with a legitimate business need. No credit card information may be shared with external parties except the Department's financial institution or authorized auditors.

7. Incident Reporting

Any suspected exposure, mishandling, or unauthorized access to ACH or credit card information must be reported immediately to:

- Department Finance Officer
- Department Commander
- Department Judge Advocate (if legal review is required)

Complete a written incident report within 24 hours.

8. Compliance & Enforcement

The Office Manager is responsible for ensuring all sensitive data is properly reviewed before destruction. Failure to comply with this policy may result in:

- Revocation of financial-handling privileges
- Disciplinary action under Department bylaws
- Referral to law enforcement or regulatory authorities when warranted

9. Effective Date

This unified policy becomes effective upon adoption by the Finance Committee and shall be incorporated into the Department Administrative Manual.

Appendix A — Vendor ACH Payment Authorization Form

(Included as an official attachment to this policy)



American Legion Department of Ohio

Vendor ACH Payment Authorization Form

Section 1 — Vendor Information

Vendor/Company Name: _____

Mailing Address: _____

City: _____ State: _____ ZIP: _____

Primary Contact Person: _____

Phone Number: _____

Email Address: _____

Section 2 — Banking Information (Confidential)

Protected under the Department's Financial Data Protection Policy.

Bank Name: _____

Bank Address: _____

Routing Number (9 digits): _____

Account Number: _____

Account Type: ☐ Checking ☐ Savings

Section 3 — Payment Details

Purpose of Payment: ☐ Goods ☐ Services ☐ Contracted Work ☐ Reimbursement

☐ Other: _____

Payment Frequency: ☐ One-time ☐ Recurring ☐ As invoiced

Section 4 — Authorization & Certification

By signing, the vendor certifies that:

1. The banking information provided is accurate and authorized for ACH deposits.
2. ACH payments may take 1–3 business days to process.
3. Changes to banking information require 10 business days' written notice.
4. Bank information will be handled in accordance with the Department's Financial Data Protection Policy.
5. The vendor releases the Department from liability for incorrect payments resulting from inaccurate information provided.

Authorized Representative Name: _____

Title: _____

Signature: _____

Date: _____

Section 5 — Department Use Only

Received By: _____ Date: _____

Verified By (Finance Officer): _____ Date: _____

Entered In System By: _____ Date: _____

Destructed By: _____ Date: _____

Notes: _____