Data Protection/Privacy Policy

Montezuma Valley Volunteer Community Service Organization (MVVCSO)

Effective Date: June 28, 2025

Purpose

The Montezuma Valley Volunteer Community Service Organization (MVVCSO) is committed to protecting the privacy of personal information collected from volunteers, members, and other individuals interacting with our food bank and community programs in Ranchita, CA. This Data Protection/Privacy Policy ensures compliance with the **California Consumer Privacy Act (CCPA)**, safeguards trust, and supports transparent governance. It secures data to meet grant requirements (e.g., USDA, HRSA), aligns with MVVCSO's mission to serve all residents, and rebuilds community confidence following past governance issues.

Authority

This policy is authorized by the **MVVCSO Bylaws (2025)**:

> **Article VII, Section 1**: Mandates accurate maintenance of records (e.g., membership, volunteer data), implying robust data security measures.
> **Article III, Section 2D**: Requires a public roster of Voting Members, with privacy measures to protect personal information.
> **Article XV**: Ensures accessibility of materials and processes, including data access requests, per ADA (28 CFR § 36).
> **Article XI**: Provides whistleblower protections for reporting data misuse.
> **Article VI, Section 1D**: Empowers the Ethics Committee to investigate data-related misconduct.

Scope

This policy applies to all **Personal Information** collected, stored, or processed by MVVCSO, including data from:

Voting Members: Names, addresses, contact details (e.g., membership applications, Article III, Section 3A).
Volunteers: Names, contact info, emergency contacts, skills, accessibility needs (e.g., Volunteer Sign-Up Forms, Article XIII).
Program Participants: Data from food bank clients or aid recipients (e.g., delivery recipients, Article XIV).
Other Individuals: Donors, community forum attendees, or website users (if applicable). It covers all MVVCSO personnel (Directors, officers, committee members, volunteers, contractors) handling data, ensuring compliance with legal and grant standards.

Definitions

Personal Information (PI): Information that identifies or relates to an individual, such as name, address, phone number, email, or accessibility needs, as defined by CCPA (§ 1798.140(o)).
Data Subject: An individual whose PI is collected by MVVCSO (e.g., member, volunteer).
Data Processing: Any operation performed on PI, including collection, storage, use, disclosure, or deletion.
Business Purpose: Activities related to MVVCSO's operations, such as membership management, volunteer coordination, program delivery, or grant reporting.

Policy Guidelines

1. Data Collection and Use

1.1 **Minimization**:

MVVCSO collects only the PI necessary for specific business purposes, including:

Membership: Name, address, contact details for Voting Member enrollment and roster (Article III, Sections 2D, 3A).

Volunteering: Name, contact, emergency contact, skills, accessibility needs for scheduling and safety (Article XIII).

Programs: Contact details for food bank delivery or aid recipients (Article XIV).

Grants: Aggregated data (e.g., volunteer hours, households served) for reporting to funders (e.g., USDA, HRSA).

Data Subjects are informed of collection purposes via forms (e.g., Volunteer Sign-Up Form) or notices (e.g., at community forums).

1.2 **Lawful Use**:

PI is used solely for disclosed business purposes, such as:

Managing membership and elections (Article III).

Coordinating volunteer activities (Article XIII).

Delivering programs (e.g., food distribution, Article XIV).

Complying with legal or grant obligations (e.g., IRS Form 990, USDA audits).

Use beyond these purposes requires explicit consent from the Data Subject, documented in writing.

1.3 **Non-Disclosure**:

PI is not sold, shared, or disclosed to third parties except:

With consent (e.g., sharing volunteer hours with grant funders).

For legal compliance (e.g., IRS audits).

To service providers (e.g., cloud storage vendors) under CCPA-compliant contracts ensuring confidentiality.

Public rosters (Article III, Section 2D) include only names and are redacted for sensitive details (e.g., addresses, phone numbers).

2. Data Security

2.1 **Storage**:

Physical Records: Stored in a locked cabinet at the principal office (27527 Skyway Drive, Ranchita, CA 92066), accessible only to authorized personnel (e.g., Secretary, Volunteer Coordinator).
Digital Records: Stored in an encrypted cloud service (e.g., Google Drive, funded by a $200 budget, Article VII, Section 1), with two-factor authentication and restricted access.
Records are retained for three years or as required by law (e.g., IRS 501(c)(3) audit requirements), then securely destroyed (e.g., shredded for paper, deleted for digital).

2.2 **Access Controls**:

Only authorized personnel (e.g., Secretary for membership data, Volunteer Coordinator for volunteer records) access PI, trained annually on CCPA compliance. Access is logged, with logs reviewed quarterly by the Ethics Committee to detect unauthorized use (Article VI, Section 1D).

2.3 **Breach Response**:

In case of a data breach (e.g., unauthorized access), MVVCSO notifies affected Data Subjects within 72 hours, per CCPA (§ 1798.150), via mail, email, or public posting (Article VII, Section 1).
The Board investigates breaches, implements corrective measures (e.g., enhanced encryption), and reports findings publicly (redacted for privacy), per Article IV, Section 3D.

3. Data Subject Rights

3.1 **Right to Know**:

Data Subjects may request details of their PI collected, used, or disclosed, including categories (e.g., name, address) and purposes (e.g., membership management), per CCPA (§ 1798.110).
Requests are submitted in writing to the Secretary (27527 Skyway Drive, Ranchita, CA 92066) or via email [insert contact], with a response within 45 days.

3.2 **Right to Access**:

Data Subjects may request a copy of their PI, provided in print, digital, or large-print format (Article XV), per CCPA (§ 1798.100).
Access requests are free, limited to two per year, with identity verification (e.g., matching membership records).

3.3 **Right to Delete**:

Data Subjects may request deletion of their PI, except where required for legal or operational purposes (e.g., IRS retention, grant audits), per CCPA (§ 1798.105).
Deletion requests are processed within 45 days, with confirmation sent to the Data Subject.

3.4 **Right to Opt-Out**:

Data Subjects may opt out of non-essential PI uses (e.g., event reminders), indicated on forms (e.g., Volunteer Sign-Up Form) or by written request to the Secretary.
Opt-out does not affect essential uses (e.g., membership roster, Article III, Section 2D).

3.5 **Non-Discrimination**:

MVVCSO does not discriminate against Data Subjects exercising CCPA rights (e.g., denying volunteer opportunities), per CCPA (§ 1798.125) and California Civil Code § 51.

4. Accessibility

4.1 **Accessible Requests**:

Data access, deletion, or opt-out requests are supported with accommodations (e.g., large-print forms, Spanish translation, assistance for disabled individuals), per Article XV and ADA (28 CFR § 36).
The Secretary provides in-person support at the food bank or via phone, funded by a $500 accessibility budget (Article XV).

4.2 **Public Notices**:

This policy and data rights are posted at the food bank, community bulletins (e.g., post office, church), and online (if available), in large-print and Spanish, per Article VII, Section 1.
Notices inform Data Subjects of their rights and how to contact the Secretary.

5. Training and Oversight

5.1 **Training**:

All personnel handling PI (e.g., Secretary, Volunteer Coordinator) complete annual CCPA training, covering data minimization, security, and breach response, funded by a $200 budget (Article VII, Section 1).
Training records are maintained by the Secretary, included in the annual report (Article VII, Section 3).

5.2 **Oversight**:

The Board designates the Secretary as the Data Protection Officer, responsible for policy implementation, request processing, and compliance monitoring.
The Ethics Committee reviews data-related complaints or breaches, reporting findings to the Board (Article VI, Section 1D).

6. Enforcement and Reporting

6.1 **Violations**:

Suspected data misuse (e.g., unauthorized disclosure) is reported to the Ethics Committee via the Misconduct Report Form (Volunteer Management SOP, Appendix E), with whistleblower protections (Article XI).
The Ethics Committee investigates within 14 days, recommending actions (e.g., retraining, suspension) to the Board.

6.2 **Consequences**:

Violations result in:

- Mandatory retraining.
- Suspension from data-handling roles (up to 30 days).

Removal from Board or committee positions (Article IV, Section 4).
Termination of volunteer or contractor status.

Decisions are documented confidentially, with public summaries (redacted) in meeting minutes (Article VII, Section 1).

6.3 **Reporting**:

Data protection metrics (e.g., requests processed, breaches) are reported in the annual report (Article VII, Section 3), ensuring transparency.
The Board reviews compliance quarterly, with findings posted publicly (Article IV, Section 3D).

7. Policy Review and Updates

7.1 **Annual Review**:

The Board reviews this policy annually by January 31, incorporating feedback from Voting Members and volunteers via the Community Engagement Committee (Article VI, Section 1C).
Updates require a majority Board vote and 30-day member notice, posted at the food bank, online, and via mail (Article IV, Section 2A).

7.2 **Public Access**:

The policy is available at the food bank (27527 Skyway Drive, Ranchita, CA 92066), online (if available), or upon request (7-day notice, Article VII, Section 2), in large-print or Spanish formats (Article XV).

Compliance with Legal and Bylaw Requirements

The policy meets all relevant standards:

Proposed 2025 Bylaws:

Article VII, Section 1: Ensures secure, accurate record maintenance (Section 2), with encrypted storage and access logs.

Article III, Section 2D: Protects public roster data by redacting sensitive details (Section 1.3).

Article XV: Provides accessible data request processes (Section 4), aligning with ADA.

Article XI: Supports whistleblower protections for data misuse reports (Section 6.1).

Article VI, Section 1D: Empowers Ethics Committee oversight (Sections 5.2, 6.1).

Article IV, Section 3D: Ensures transparent reporting of data metrics (Section 6.3).

California Consumer Privacy Act (CCPA, Cal. Civ. Code § 1798):

Right to Know/Access: Sections 3.1-3.2 provide disclosure and copy rights within 45 days.

Right to Delete: Section 3.3 allows deletion with legal exemptions.

Right to Opt-Out: Section 3.4 permits opting out of non-essential uses.

Non-Discrimination: Section 3.5 ensures no penalties for exercising rights.

Security: Section 2 implements encryption, access controls, and breach notifications.

Training: Section 5.1 mandates annual CCPA training.

California Corporations Code (CCC):

§ 5231 (Duty of Care): Secure storage and oversight (Sections 2, 5) ensure responsible data management.

§ 5510 (Member Access): Data access aligns with bylaw record inspection rights (Section 3.2).

IRS 501(c)(3):

Prevents private benefit (IRC § 4958) by securing data to avoid misuse (Section 2).

Supports Form 990 transparency through public reporting of data practices (Section 6.3).

Americans with Disabilities Act (ADA, 28 CFR § 36):

Accessible data request processes (e.g., large-print, in-person support) comply with ADA (Section 4).

California Nonprofit Integrity Act (NIA, Government Code § 12586):

Transparent data practices and public access (Sections 6, 7) enhance governance integrity.

California Civil Code § 51 (Unruh Act):

Non-discriminatory data handling (Section 3.5) ensures inclusivity, aligning with serving-all North Star.

Grantor Expectations (USDA, HRSA):

Secure data practices (Section 2) meet USDA audit requirements for volunteer and program data.

Inclusivity and accessibility (Section 4) strengthen HRSA applications for underserved populations.

Transparent reporting (Section 6) supports grant compliance and accountability.

This **Data Protection/Privacy Policy** secures volunteer and member data in full compliance with the CCPA, ensuring privacy, trust, and grant readiness for MVVCSO. It aligns with **Article VII, Section 1** and **Article III, Section 2D** of the 2025 bylaws, implementing robust security, access rights, and transparency measures. By addressing data minimization, secure storage, breach response, and accessible processes, the policy supports MVVCSO's transparency North Star, complies with CCC, IRS, ADA, NIA, and grantor standards, and rebuilds community confidence. The policy's structure allows flexibility for future data needs (e.g., expanded programs) while maintaining legal and ethical standards.