Permitted Use Agreement for Digital Services and Social Media Management

Montezuma Valley Volunteer Community Service Organization (MVVCSO)

Effective Date: June 28, 2025

Purpose

This Permitted Use Agreement governs the access and management of MVVCSO's digital services and social media accounts, ensuring responsible use, transparency, and compliance with the Proposed Bylaws (revised April 27, 2025). It establishes protocols for authorized access, protects organizational assets, and enforces accountability for misuse.

Scope

This Agreement applies to all MVVCSO Board members, officers, and designated volunteers granted access to MVVCSO's digital services and social media accounts, including but not limited to email, Google Drive, website forms, calendars, and social media platforms.

Definitions

- **Digital Services**: MVVCSO's Gmail & Google Drive for institutional documentation and Board collaboration, website forms, and calendars.
- **Social Media Accounts**: MVVCSO's official accounts on platforms: Facebook, Twitter/X, Instagram.

- **Authorized User**: A Board member, officer, or designated volunteer in good standing, approved by the Board to access digital services or social media accounts.
- **RCO@Gmail (**ranchitacommunityorganization@gmail.com): The primary login account for all digital services and social media accounts, with the recovery email set to ranchita@mvvcso.org.

Agreement Terms

- **Primary Login and Recovery**
    - The primary login for all digital services and social media accounts shall be **RCO@Gmail**, with the recovery email set to **ranchita@mvvcso.org** (Article VII, Section 1, accurate records).
    - Authorized Users shall use RCO@Gmail for all official MVVCSO digital activities, ensuring centralized access and Board oversight.
    - The Secretary shall maintain a secure record of the RCO@Gmail password, updated after any changes, accessible to the Board at the principal office with 7 days' notice (Article VII, Section 2).
- **Permitted Uses**
    - Authorized Users may access digital services and social media accounts solely for:
        - Managing MVVCSO's email communications (ranchita@mvvcso.org) for official correspondence.
        - Storing and collaborating on institutional documentation via Google Drive, per Board-approved projects (Article IV, Section 2A).
        - Updating website forms and calendars to support community engagement (Article VI, Section 1C).
        - Posting content on social media accounts that aligns with MVVCSO's mission, approved by the Board or Community Engagement Committee (Article VI, Section 1C).

    - All actions must comply with MVVCSO's inclusivity goals (Article XII), accessibility requirements (Article XV), and California Consumer Privacy Act (CCPA) standards (Article III, Section 2C).
- **Prohibited Actions**
    - **Unauthorized Password Changes**: Changing the RCO@Gmail password or account settings without immediate notification to the Board and sharing the new password with the Secretary, except in emergency anti-compromise scenarios (e.g., suspected hacking), where the user must notify the Board within 24 hours and document the justification (Article IV, Section 6, transparency).
    - **Unapproved Actions**: Taking actions without Board approval, including posting unapproved content, altering account settings, or accessing restricted files, especially in cases of misconduct, rotation off the Board, or bad faith against the Board, community, or individuals.
    - **Personal Use**: Using digital services or social media accounts for personal purposes or non-MVVCSO activities.
    - **Confidentiality Breaches**: Sharing sensitive information (e.g., membership data, financial records) without Board authorization, violating CCPA or Article VII, Section 2.
- **Access and Authorization**
    - Access to digital services and social media accounts requires Board approval via majority vote, recorded in meeting minutes (Article IV, Section 2A).
    - The Community Engagement Committee shall recommend authorized users for social media management, subject to Board approval (Article VI, Section 1C).
    - The Secretary shall maintain a list of Authorized Users, updated annually, accessible to Voting Members with 7 days' notice in large-print and screen-reader-compatible formats (Article III, Section 2C, Article XV).
- **Password Management**
    - Password changes to RCO@Gmail or any linked account must be:
        - Approved by the Board in advance, except in emergency anti-compromise scenarios.

        - Immediately shared with the Secretary, who updates the secure record (Article V, Section 3).
        - Reported to the Board within 24 hours in emergency cases, with written justification (Article IV, Section 7A).
    - Unauthorized password changes are considered misconduct and subject to statutory penalties (see Section 7).
- **Accountability and Oversight**
    - The Ethics Committee shall investigate complaints of misuse, such as unapproved actions or bad faith conduct, with findings reported publicly (excluding confidential details) (Article VI, Section 1D).
    - Authorized Users must disclose conflicts of interest and recuse themselves from related digital actions, per the Conflict of Interest Policy (Article IV, Section 6).
    - The Board shall conduct semi-annual reviews of digital services and social media activity, overseen by the Community Engagement Committee, to ensure compliance (Article VI, Section 1C).
    - Misuse may result in immediate suspension of access, pending investigation, and potential removal from the Board per Article IV, Section 4, and California Corporations Code §§ 5221-5223.
- **Statutory Penalties for Non-Compliance**
    - **Unauthorized Password Changes**: Changing passwords without immediate sharing (except in emergency anti-compromise scenarios) violates this Agreement and may result in:
        - Suspension of access.
        - Board removal per Article IV, Section 4.
        - Civil penalties under California law for breach of fiduciary duty (California Corporations Code § 5231, duty of care).
        - Potential referral to legal authorities for intentional misuse.
    - **Unapproved Actions in Bad Faith**: Actions taken without Board approval, especially in cases of misconduct, rotation, or bad faith against the Board, community, or individuals, may result in:
        - Immediate access revocation.

        - Restitution for damages caused (e.g., recovery costs for compromised accounts).
        - Removal from the Board or volunteer roles (Article IV, Section 4).
        - Civil or criminal penalties for fraud, data breaches, or defamation, per California law (e.g., Penal Code § 502, unauthorized access; Civil Code § 1798.150, CCPA violations).
    - Whistleblower protections apply to reports of misuse, per Article XI.
- **Termination of Access**
    - Access is revoked upon:
        - Resignation, removal, or rotation off the Board (Article IV, Section 4).
        - Failure to remain in good standing (Article III, Section 3C).
        - Board resolution for misuse or non-compliance (Article IV, Section 2A).
    - Departing users must return or delete access credentials within 24 hours, coordinated with the Secretary (Article V, Section 3).
    - The Secretary shall update account settings to remove former users within 48 hours.
- **Emergency Protocols**
    - In emergencies (e.g., suspected hacking), Authorized Users may change passwords to protect accounts, provided they:
        - Notify the Board within 24 hours.
        - Document the justification, submitted to the Secretary (Article IV, Section 7A).
        - Share the new password with the Secretary for record-keeping.
    - If only one Director remains, they may access digital services to maintain operations, per Article IV, Section 7A, with actions reported within 14 days.
    - In a completely vacated Board, Emeritus Board Members may access accounts temporarily, limited to operational needs, per Article IV, Section 7B.
- **Transparency and Accessibility**
    - This Agreement and a summary of digital service usage shall be posted within 7 days at the food bank, community bulletins, and online (if available), in large-print and screen-reader-compatible formats, per Article XV.
    - Voting Members may inspect records of Authorized Users and account activity with 7 days' notice, ensuring CCPA compliance (Article VII, Section 2).

- The annual report shall include a summary of digital service and social media activity, certified by the President, Secretary, or a CPA (Article VII, Section 3).

Acknowledgment

I, the undersigned, acknowledge that I have read, understand, and agree to comply with the MVVCSO Permitted Use Agreement for Digital Services and Social Media Management. I understand that non-compliance may result in access revocation, Board removal, and statutory penalties under California law.

Name: _____ **Role**: _____

Signature: _____ **Date**: _____
