SOLANO COUNTY

REGISTRAR OF VOTERS

Request for Information "Multipurpose Voter File"

PRINT

Application to Purchase/View Voter Registration Information

The Applicant hereby agrees that the aforementioned information set forth in Affidavits of Registration of voters and any information derived from said electronic data processing information (hereinafter collectively referred to as "registration information") will be used ONLY FOR ELECTION OR GOVERNMENTAL PURPOSES, or research as defined by Title 2, Division 7, Article 1, Section 19003 of the California Code of Regulations, and Elections Code Section 2194 and Governmental Code Section 6254.4.

The Applicant (as principal or agent) further agrees NOT to sell, lease, loan or deliver possession of the registration information, or a copy thereof, or any portion thereof, in any form or format, to any person, organization or agency without first submitting a new application and receiving written authorization from the Solano County Registrar of Voters to release such registration information. The applicant also agrees that the data will not be used to harass any voter or voter's household; will not use the data for commercial advertising or marketing; will not use the data for solicitation of contributions or services for any personal, private or commercial use; and will not leave the voter data unsecured and publicly available online or offline (CA CCR §19004).

WILLFUL VIOLATION OF THESE PROVISIONS IS A MISDEMEANOR (ELECTIONS CODE SECTION 18109). In addition, subject to provisions of Title 2, Division 7, Article 1, Sections 19001 through 19007 of the California Code of Regulations, the Applicant agrees to pay to the State of California, as compensation for any UNAUTHORIZED USE OF EACH INDIVIDUALS REGISTRATION INFORMATION, an amount equal to the sum of fifty cents ($.50) multiplied by the number of times each registration record is used by the Applicant in an unauthorized manner.

_____

*Full name of Applicant (the person, business, organization or committee for whom application is submitted)

_____

*Phone *E-mail Date

_____

*Residence Address City State Zip Code

_____

Business Address (if different than Residence Address) City State Zip Code

_____

Mailing address (if different from above)

_____

*Driver's License Number (including state if not CA) *Phone Number

_____

"I certify under penalty of perjury, under the laws of the State of California, that all of the above information provided by me is true and correct."

Executed at: _____

City County State

_____

*Signature of applicant or agent *Print name Date

Applicant must Initial Each Statement: (CA CCR §19008(a)(12).	
_____ Initial in pen	Applicant and beneficiary, if applicable, hereby agree that the information set forth in the voter registration information will be used for the approved purposes, consistent with state law, as defined by Elections Code section 2194, CA CCR §19008, and Government Code section 6254.4.
_____ Initial in pen	Applicant and beneficiary, if applicable, further agree not to sell, lease, loan, or deliver possession of the registration information, or a copy thereof, in any form or format, to any person, organization, or agency except as prescribed in CA CCR §19005.
_____ Initial in pen	Applicant and beneficiary, if applicable, agree to maintain information in a secure and confidential manner using the best practices identified in CA CCR §19010, and will notify the Secretary of State immediately of any violation, exposure, and/or breach of voter registration information or suspected violation, exposure, and/or breach of voter registration information and will cooperate with the Secretary of State's office or any investigative agency efforts related to any resulting investigation.
_____ Initial in pen	Applicant and beneficiary, if applicable, understand that it is a misdemeanor for a person in possession of voter registration information to use or permit the use of all or any part of the information for any purpose other than is permitted by law.
_____ Initial in pen	Applicant and beneficiary, if applicable, agree to pay the State of California, as compensation for any unauthorized use of each individual's registration information, a penalty as described in Section 19007 of this Article.

The Application must be submitted by mail or in-person. Electronic applications can no longer be received per CCR §19009.

This form will be considered incomplete if the following are not included:

Section 1. A Copy of a current Driver Licenses is required.

☐	I have included a clear copy of my current driver licenses or state identification card. (required)

Section 2. Representation – the applicant represents one of the following: (select one) (CA CCR §19008(a)(7))

◯ Political Organization or Current Candidate:	_____ (name or organization)	I have included documentation establishing affiliation with the political organization; proof of current candidacy, or release from candidate authorizing obtaining file on his or her behalf.
◯ Academic Organization:	_____ (name or organization)	I have included a letter from a representative of the institution (professor, administrator, etc.) on the institution's letterhead stating that the applicant is authorized to receive the data.
◯ Media Organization:	_____ (name or organization)	I have included a copy of my press pass.
◯ Government Organization:	_____ (name or organization)	I have included a letter from a representative of the government organization (department head, supervisor, administrator, etc.) on the organization's letterhead stating that the applicant is authorized to receive the data.

Section 3. Type of Research – Is this for a candidate or measure?

◯ Candidate: (list all candidates ad specific elections that apply):	
◯ Measure: (list any/all measures and for which election they will appear on the ballot)	

Section 4. Provide a detailed description of the intended use(s). Any reference to "any unlawful use" will be rejected. If more space is needed, please add a second sheet. See pages 4-5 for permissible use. (CA CCR §19008(a)(8))

Section 5. Requirements for Storage and Security of Voter Registration Information. See pages 5-6 for security and storage requirements. (CA CCR §19012(1) and (2))

By receiving vote registration information from the Solano County Registrar of Voters, I agree to the following security best practices:

☐ I agree to use a strong and unique password ("strong password hygiene") per account with access to the voter registration information or privileges to grant access.

☐ I agree to obtain training on security awareness to avoid social engineering and phishing attacks.

☐ I agree to practice the principles of "least privilege" By restricting user access to the minimum need based on users' job necessity.

☐ I agree to ensure user accounts are logged off or the session is locked after a period of inactivity, which shall be no more than 15 minutes.

☐ I agree to remove, deactivate, or disable accounts or default credentials.

☐ I agree to erase or wipe voter registration information that is no longer needed for its retention and sanitized following National Institute of Standards and Technology (NIST) 800-88 Guidelines for media sanitization.

☐ I agree to restrict physical access by not leaving your computer in places unlocked and unattended.

☐ I agree to limit the use of portable devices. If a portable device is used, strong storage encryption procedures must be applied utilizing Federal Information Processing Standards (FIPS) 197, commonly referred to as "Advanced Encryption Standard" or "AES."

☐ I agree to use wireless technology securely with Wi-Fi Protected Access 2 (WPA2) or better.

Section 5. Select the type of file:			
A. ◯	Standard Voter File - Countywide on CD (pre-made on Mondays)	Contains all Solano County voters and vote history for past 20 elections – tab delimited text file.	**Cost:** $10.00
B. ◯	Vote by Mail Subscription service	Cumulative VBM files that are emailed daily	**Cost:** $358.45
C. ◯	Custom Voter File (complete steps 1-6 below)	Mark desired options below.	**Cost:** Varies based on options. Charge for staff time is $48.15/quarter hour.

Step 1. Choose one:

◯ A secured, county provided flash drive (additional $10.00 for materials will be charged)	◯ Send to my E-Mail Address:_____

Step 2. Select File Format (choose only one):

Per CA CCR §19011 – the Registrar of Voters does not provide end-user technical support for opening/converting files.

◯ Comma Delimited	◯ Tab Delimited	◯ Excel File (requires additional staff time)

Step 3. Select Voter History (choose only one):

◯ None	◯ Last 20 Elections	◯ These Specific Elections _____ _____ _____

Step 4. District Information (choose only one):

◯ Countywide	◯ Only These Specific Precincts:

Step 5. Optional Information:

☐ Search only these dates:	From:	To:
◯ Include All Political Parties or --	◯ Specific Parties: _____	

Step 6. What voter data do you need (pick only one):

◯ Include All Eligible Voters	
◯ **ONLY INCLUDE** Perm Vote by Mail	
◯ **ONLY INCLUDE** these specific voters (must include full name, date of birth, county of residence, and residence address::	Provide a separate line for each individual voter: 1._____ 2._____ 3._____ 4._____ 5._____

19003. Permissible Uses.

1. Voter registration information obtained from a source agency shall be used solely for the following purposes:
    1. Election: for any person to communicate with voters in connection with an election by means that shall include, but shall not be limited to, the following:
        1. Communicating with voters for or against any candidate or ballot measure in any election;
        2. Communicating with voters regarding the circulation or support of, or opposition to, any recall, initiative, or referendum petition;
        3. Surveying voters in connection with any specific election campaign or specific potential election campaign in which any voter registered to vote may vote;
        4. Surveying voters in connection with an election-related exploratory committee;
        5. Soliciting contributions or services as part of any election campaign on behalf of any candidate for public office or any political party or in support of or opposition to any ballot measure, initiative, or referendum petition.
    2. Scholarly: students working on theses, professors researching voting patterns, and other academics involved in research related to political or election activities.
    3. Journalistic: members of the press for any purpose related to political or election activities.
    4. Political: for any person to communicate with voters to influence public opinion related to political or election activities. The content of such communications shall include, but shall not be limited to: news and opinions of candidates, elections, education related to political matters, political party developments, ballot measures, initiatives, referendum positions, and related political matters.
    5. Governmental: Any request from a governmental agency or for a use related to a governmental function by means including, but not limited to:
        1. Encouraging participation in the United States Census;
        2. Conducting any survey of opinions of voters by any government agency or its contractors;
        3. Any official use by any local, state, or federal governmental agency, which shall include use in connection with any judicial proceeding or investigation involving or being conducted by any local, state, or federal governmental agency.
    6. Record review: For any person to conduct an audit of voter registration lists for election, scholarly, journalistic, political, or governmental purposes. Record review includes, but is not limited to, detecting voter registration fraud, evaluating voter registration information accuracy, and evaluating compliance with applicable Federal and California laws.
    7. Vendor: By any vendor to compile and/or organize voter registration information for another person's use consistent with this Article.
2. Requests for voter registration information for a purpose not specifically listed in subdivision (a), and not prohibited by section 19004, shall be evaluated for compliance with the Elections Code by the source agency.
3. A source agency shall review each application for compliance with the Elections Code and this Article independent of decisions made on other applications.

Note: Authority cited: Section 2188.2, Elections Code; Sections 6254.4 and 12172.5, Government Code. Reference: Sections 2188 and 2194, Elections Code.

19004. Impermissible Uses.

1. Using voter registration information in a manner contrary to the authorized uses specified in Elections Code section 2194 is impermissible. Impermissible uses include, but shall not be limited to:
    1. Any communication for any personal, private, or commercial purpose other than for those purposes permitted by Section 19003.
    2. Solicitation of contributions or services for any personal, private, or commercial purpose.

3. Conducting any survey of opinions of voters other than for those purposes permitted by Section 19003, subdivision (a).
4. Using the voter registration information to harass any voter or the voter's household, including, but not limited to, any conduct prohibited by Elections Code sections 18540 and 18543.

2. Voter registration information shall not be sent outside of the United States, as specified in Elections Code section 2188.5.
3. Notwithstanding section 19003, a source agency may reject a request for voter registration information based on a reasonable belief or determination that it is being requested for use in a manner prohibited by law, including, but not limited to, uses contrary to the prohibitions or authorized uses specified in Elections Code sections 2188.5 and 2194 or that is contrary to Elections Code section 10. An impermissible purpose may include requests for voter registration information for an impermissible purpose submitted for fraudulent purposes or in bad faith or for the purpose of harassing or defrauding a person or entity. In such instances, the source agency shall provide the applicant its reasons for refusal. An applicant whose application is rejected shall not be prohibited from filing a new application.

Note: Authority cited: Sections 2188.2 and 2188.5, Elections Code; Sections 6254.4 and 12172.5, Government Code. Reference: Sections 2188 and 2194, Elections Code.

19012. Requirements for Storage and Security of Voter Registration Information

1. Any person who has directly or indirectly obtained voter registration information from a source agency must exercise due diligence in maintaining and securing the voter registration information in order to reduce the risk of information exposure and/or breach.
2. Any person who has directly or indirectly obtained voter registration information from a source agency shall:
    1. Use a strong and unique password ("strong password hygiene") per account with access to the voter registration information or privileges to grant access.
    2. Apply security best practices, which includes the following:
        1. Obtaining training on security awareness to avoid social engineering and phishing attacks.
        2. Practice the principles of "least privilege" By restricting user access to the minimum need based on users' job necessity.
        3. Ensure user accounts are logged off or the session is locked after a period of inactivity, which shall be no more than 15 minutes.
        4. Remove, deactivate, or disable accounts or default credentials.
        5. Erase or wipe voter registration information that is no longer needed for its retention and sanitized following National Institute of Standards and Technology (NIST) 800-88 Guidelines for media sanitization.
        6. Restrict physical access by not leaving your computer in places unlocked and unattended.
        7. Limit the use of portable devices. If a portable device is used, strong storage encryption procedures must be applied utilizing Federal Information Processing Standards (FIPS) 197, commonly referred to as "Advanced Encryption Standard" or "AES."
        8. Use wireless technology securely with Wi-Fi Protected Access 2 (WPA2) or better.
3. In addition to the requirements set forth in (b) above, any vendor shall:
    1. Apply additional security best practices, which include the following:
        1. Use strong identity and access management, preferring multi-factor authentication for any and all privilege accounts and/or accounts with access to voter registration data.
        2. Initiate an account lockout after a pre-defined number of failed attempts, no more than 10. Any automated account unlock actions must wait no less than 30 minutes from the lockout event.
        3. Force password changes on a pre-defined basis, but not less than 365 days.
        4. Backups of voter registration information shall be securely stored separately and utilizing FIPS 197 encryption at rest.
    2. Implement security log management, which includes the following:

1. Enable logging on all systems and network devices with sufficient information collection that answers the following:
    1. What activity was performed?
    2. Who or what performed the activity, including where or on what system the activity was performed?
    3. What activity was the action performed on?
    4. What tool(s) were used to perform or performed the activity?
    5. What was the status, outcome, or results of the activity?
2. Review log(s) regularly for any errors, abnormal activities and any system configuration changes.
3. Securely store log files separately from the systems monitored, archived, and protect from unauthorized modification, access, or destruction.
4. Use log monitoring tools to send real-time alerts and notifications.
5. Utilize multiple synchronized United States-based time sources.

3. Employ system hardening techniques, which include the following:
    1. Update and install all firmware and patches from a trusted and verifiable source.
    2. Use only the most up-to-date and certified version of vendor software.
    3. Install and maintain active malware and anti-virus software.
    4. Implement firewalls, also known as host-based firewalls, and/or port filtering tools with host-based intrusion protection services.
    5. Encrypt voter registration information using FIPS 197 at rest.
    6. Encrypt voter registration information in transit such as Transport Layer Security (TLS) 1.2 or better with a valid certificate and certificate chain.
    7. Do not use self-signed certificates.
    8. Conduct regular vulnerability scanning and testing for known or unknown weaknesses.
    9. Use application whitelisting on all endpoints and systems.

Note: Authority cited: Section 2188.2, Elections Code; Sections 6254.4 and12172.5, Government Code. Reference: Sections 2188 and 2194, Elections Code.