



BEAUMONT-CHERRY VALLEY WATER DISTRICT
560 Magnolia Avenue, Beaumont, CA 92223

**NOTICE AND AGENDA
MEETING OF THE PERSONNEL COMMITTEE**

*This meeting is hereby noticed pursuant to
California Government Code Section 54950 et. seq.*

Tuesday, January 21, 2025 - 5:30 p.m.
560 Magnolia Avenue, Beaumont, CA 92223

TELECONFERENCE NOTICE

*The BCVWD Personnel Committee members will attend in person at the
BCVWD Administrative Office*

*This meeting is available to the public via Zoom teleconference
To access the Zoom conference, use the link below:*

<https://us02web.zoom.us/j/85792068838?pwd=cFArZHZ4aHRSUmJLeTBCZVpnUGRmdz09>

To telephone in, please dial: (669) 900-9128
Enter Meeting ID: 857 9206 8838 • Enter Passcode: 457586

*For Public Comment, use the “**Raise Hand**” feature if on
the video call when prompted. If dialing in, please **dial *9 to**
“Raise Hand” when prompted*

*Meeting materials will be available on the BCVWD’s website:
<https://bcvwd.org/document-category/personnel-committee-agendas/>*

PERSONNEL COMMITTEE MEETING – JANUARY 21, 2025

Call to Order: Chair Covington

Roll Call

	John Covington, Chair
	Lona Williams

	Andy Ramirez (alternate)
--	---------------------------------

PERSONNEL COMMITTEE MEETING – JANUARY 21, 2025 - *continued*

Public Comment

PUBLIC COMMENT: RAISE HAND OR PRESS *9 to request to speak when prompted. If you are present in the Conference Room, please fill out a Request to Speak card and deliver it to the Recording Secretary.

At this time, any person may address the Committee on matters within its jurisdiction. However, state law prohibits the Committee from discussing or taking action on any item not listed on the agenda. Any non-agenda matters that require action will be referred to Staff for a report and possible action at a subsequent meeting.

Please limit your comments to three minutes. Sharing or passing time to another speaker is not permitted.

1. Adjustments to the Agenda: In accordance with Government Code Section 54954.2, additions to the agenda require a unanimous vote of the legislative body members present, which makes the determination that there is a need to take action, and the need to take action arose after the posting of the agenda.

- a. Item(s) to be removed or continued from the Agenda
- b. Emergency Item(s) to be added to the Agenda
- c. Changes to the order of the Agenda

2. Acceptance of Personnel Committee Meeting minutes

Minutes may be accepted by consensus

- a. November 19, 2024 Regular Meeting (pages 4 - 8)

ACTION ITEMS

3. Report / Update from BCVWD Employees Association (no staff report)

Association Representatives		
Andrew Becerra	Luis Lomeli	Ericka Enriquez

4. Report / Update from BCVWD Exempt Employees (no staff report)

5. Human Resources Department Report (pages 9 - 11)

6. Policies and Procedures Manual Updates / Revisions

a.	Policy 3145	Driver Training and Record Review	Pages 12 - 22
b.	Policy 7004	Email and Communication	Pages 23 - 38
c.	Policy 7006	Password	Pages 39 - 52
d.	Policy 7011	Cellular Telephone Usage	Pages 53 - 71

PERSONNEL COMMITTEE MEETING – JANUARY 21, 2025 - *continued*

7. **Update on Policy Tracking Matrix** (pages 72 - 76)
 - a. Status of Policy Revisions / Updates
8. **Receipt of Association of California Water Agencies / Joint Powers Insurance Authority Award** (pages 77 - 78)
9. **Action List for Future Meetings**
10. **Adjournment**

NOTICES

AVAILABILITY OF AGENDA MATERIALS - Agenda exhibits and other writings that are disclosable public records distributed to all or a majority of the members of the Beaumont-Cherry Valley Water District Personnel Committee in connection with a matter subject to discussion or consideration at an open meeting of the Committee are available for public inspection in the District's office, at 560 Magnolia Avenue, Beaumont, California ("District Office") during business hours, Monday through Thursday from 7:30 a.m. to 5 p.m. If such writings are distributed to members of the Board less than 72 hours prior to the meeting, they will be available from the District Office at the same time or within 24 hours' time as they are distributed to Board Members, except that if such writings are distributed one hour prior to, or during the meeting, they can be made available in the Board Room at the District Office. Materials may also be available on the District's website: <https://bcvwd.gov/>. (GC 54957.5)

REVISIONS TO THE AGENDA - In accordance with §54954.2(a) of the Government Code (Brown Act), revisions to this Agenda may be made up to 72 hours before the Meeting, if necessary, after mailings are completed. Interested persons wishing to receive a copy of the set Agenda may pick one up at the District's Main Office, located at 560 Magnolia Avenue, Beaumont, California, up to 72 hours prior to the Committee Meeting.

REQUIREMENTS RE: DISABLED ACCESS - In accordance with Government Code §54954.2(a), and the Americans with Disabilities Act (ADA), requests for a disability related modification or accommodation, including auxiliary aids or services, in order to attend or participate in a meeting, should be made to the District Office. Notification of at least 48 hours in advance of the meeting will generally enable staff to make reasonable arrangements to ensure accessibility. The Office may be contacted by telephone at (951) 845-9581, email at info@bcvwd.gov or in writing at the Beaumont-Cherry Valley Water District, 560 Magnolia Avenue, Beaumont, California 92223.

CERTIFICATION OF POSTING

A copy of the foregoing notice was posted near the regular meeting place of the Personnel Committee of Beaumont-Cherry Valley Water District and to its website at least 72 hours in advance of the meeting (Government Code §54954.2(a)).



BEAUMONT-CHERRY VALLEY WATER DISTRICT AGENDA
560 Magnolia Avenue, Beaumont, CA 92223

MINUTES OF THE PERSONNEL COMMITTEE MEETING
Tuesday, November 19, 2024, at 5:30 p.m.

CALL TO ORDER

Chair Covington called the meeting to order at 5:40 p.m.

ROLL CALL

<i>Directors present:</i>	<i>John Covington, Lona Williams (alternate)</i>
<i>Directors absent:</i>	<i>None</i>
<i>Staff present:</i>	<i>General Manager Dan Jagers Assistant Director of Finance and Administration Sylvia Molina Director of Information Technology Robert Rasha Director of Operations James Bean Human Resources Manager Ren Berioso Management Analyst II Erica Gonzales Senior Water Utility Worker Jon Medina Field Superintendent Julian Herrera Water Utility Worker II Joshua Rogers Maintenance Technician I Jaden Schuler Maintenance Technician II Tommy LaMont Executive Assistant Lynda Kerney</i>
<i>BCVWD Employee Association reps:</i>	<i>Luis Lomeli, Andrew Becerra, Ericka Enriquez</i>
<i>Members of the Public:</i>	<i>None</i>

PUBLIC COMMENT: None.

ACTION ITEMS

- 1. Adjustments to the Agenda:** Ms. Molina identified a handout and a typo on the General Manager' salary of \$275,663.

- 2. Acceptance of the Personnel Committee Meeting minutes**
The October 15, 2024 meeting was canceled
 - a. September 17, 2024 Regular Meeting

The Committee accepted the minutes of the Personnel Committee meeting by the following vote:

MOVED: Covington	SECONDED: Williams	APPROVED
AYES:	Covington, Williams	
NOES:	None.	
ABSTAIN:	None.	
ABSENT:	None.	

3. Report / Update from BCVWD Employees Association: None

4. Report / Update from BCVWD Exempt Employees: None.

5. Report from Human Resources Department

Human Resources Manager Ren Berioso presented highlights of the report:

- Currently 46 employees
- No new hires and no recruitments, one separation
- Notable anniversaries and promotions

6. Policies and Procedures Manual Updates / Revisions

Human Resources Manager Ren Berioso noted that all polices were vetted by legal counsel and were prepared in tandem with the MOU group. He presented the proposed revisions to the following policies:

a. Policy 3090 Family and Medical Leave

Mr. Berioso explained that the Family and Medical Leave Act (FMLA) provisions had been eliminated from the policy in the last revision, perhaps under the assumption that FMLA did not apply to employers with fewer than 50 employees; however legal sources confirmed it applies to all government agencies. AB 1041 has added “designated persons” he noted. Legal counsel provided language for the document, he stated.

Chair Covington noted that these provisions look bad for any employer and asked for confirmation that all changes were in conformity with the law. Mr. Berioso assured that nothing was added.

The Committee recommended this policy revision for consideration by the Board of Directors by the following vote:

MOVED: Williams	SECONDED: Covington	APPROVED
AYES:	Covington, Williams	
NOES:	None.	
ABSTAIN:	None.	
ABSENT:	None.	

b. Policy 3145 Driver Training and Record Review

Mr. Berioso noted that driving is an essential function of many positions at the District. He worked with the Director of Operations and legal counsel to make clarifications in the policy and ensure the language is applicable with Labor Law.

On the draft, a distinction was made between the term “department head” and “director” so as not to confuse with Board members. Staff will change this nomenclature.

Chair Covington asked questions about the costs borne the District related to defensive driving classes and Mr. Berioso advised that legal counsel had provided those requirements for the District to pay. Chair Covington requested that this be confirmed with legal. He opined that the District should not be responsible for the cost if the employee is the violator.

Chair Covington requested better clarification of “driving probation.”

The Committee continued this item.

c. Policy 3045 Executive Officer

Mr. Berioso drew attention to the handout and reminded that this item had been tabled at the August meeting to assure no conflict with Part II Section 19, the Director, GM, and Financial Officer Relationship. He noted differences in the policy sections.

The District’s Executive Officer is the general manager, Berioso clarified. The purpose of this policy is to ensure alignment with the general manager’s job description.

Berioso asked the Committee about retention of language regarding the EO as the key point of contact for media relations and the 2019 resolution designating the President of the Board as the main District spokesperson, and the GM’s job description. General Manager Jaggars indicated there may be some overlap. Chair Covington indicated there was no crossover.

The GM’s job description was attached to the staff report but is not intended to be part of the policy, Mr. Jaggars confirmed. A job description should not be adopted by resolution as it should be flexible and able to be brought current as a working document, he noted. The draft was created during the Classification and Compensation study and was aligned with the thoughts of the current Board, he advised. Director Covington pointed out the job description was not agendized, and the Personnel Committee does not generally approve job descriptions. He requested the GM job description be brought to the full Board.

The Committee recommended this policy revision for consideration by the Board of Directors by the following vote:

MOVED: Williams	SECONDED: Covington	APPROVED
AYES:	Covington, Williams	
NOES:	None.	
ABSTAIN:	None.	
ABSENT:	None.	

7. Update on Policy Tracking Matrix

Mr. Berioso reviewed the dashboard and pointed out only three personnel policies remain for review. Progress had been made to 95.59 percent completeness for HR

policies. IT Department policies have been added. The Driver Training and Records Review will come back in January.

8. Initial Presentation and Acknowledgement of 2024 Great Place To Work Certification

Mr. Berioso presented the results of the 2024 survey and noted the District received the certification for the fourth straight year.

Mr. Berioso emphasized the following key points:

- For the fourth consecutive year, the district achieved Great Place to Work certification, effective from August 2023 to August 2024.
- Conducted in August over a month, involving 45 employees with a 91% response rate (up from 81% the previous year).
- Engagement score improved to 82% (up from 81% the previous year).
- Two key categories: overall Great Place to Work statement and employee engagement, both showed incremental improvements.
- Strengths included camaraderie, stability, gender equality, social responsibility, and time-off flexibility.
- Growth opportunities were identified in pride, fairness, transparency, benefits, and compensation.
- Items to address were identified: fairness and equality, compensation, and promoting transparency and communication.
- The benefit of the survey is it acts as a recruitment tool and boosts employee morale.
- The survey also provides actionable insights for management and the board on areas needing improvement.

Chair Covington highlighted the survey's role in shifting the District's focus toward valuing employee feedback since 2017. He commented on its effectiveness in measuring the district's health and supporting continuous improvement. Covington expressed hope that employees value the process and engage honestly.

Mr. Jagers described the survey as a critical tool for identifying areas of improvement and reinforcing strengths. He emphasized its value in providing an independent perspective on culture and sentiment, serving as a reality check for management to stay aligned with staff needs. Jagers acknowledged the progress made in building a positive culture and underscored the importance of leveraging feedback for growth.

Director Williams praised the certification as a strong recruitment tool, helping to attract talent by showcasing the District's positive workplace culture. She appreciated the survey's anonymous nature and noted visible improvements in staff engagement and camaraderie during her tenure.

Other attendees highlighted the survey's impact on camaraderie and team building. Examples included public outreach successes and the use of the certification logo to enhance recruitment efforts at career fairs. Attendees commended the survey's detailed breakdown, which effectively identifies strengths and growth areas, fostering pride in the District's accomplishments.

9. BCVWD Fiscal Year 2025 Operating Budget: Proposed FY 2025 Salary Schedule and Organization Chart

The Personnel Committee reviewed key updates to the fiscal year 2025 operating budget, including the salary schedule and organizational chart. Personnel costs now account for 35.7% of the overall operating budget, a slight increase from the prior year. The budget schedule remains on track, with final approval planned for December 11, ensuring implementation by January 1.

The salary schedule was revised following an internal compensation study comparing salaries across ten agencies. Positions below market median were adjusted upward, while those above median received only a 2.5% cost-of-living adjustment (COLA). Notably, the Maintenance Technician I position was realigned to match the Water Utility Worker I entry-level range to address potential retention issues, at a cost of \$6,000 annually. The committee supported this change to maintain equity and competitiveness.

The organizational chart retains the same staffing levels as 2024 but was reformatted for clarity and professionalism. Maintenance Technicians were separated into their own category to reflect distinct responsibilities.

The Committee approved and recommended the salary schedule with the proposed change in Maintenance Technician range from 21 to 24, and the organization chart for consideration by the Board of Directors by the following vote:

MOVED: Williams	SECONDED: Covington	APPROVED
AYES:	Covington, Williams	
NOES:	None.	
ABSTAIN:	None.	
ABSENT:	None.	

10. Action List for Future Meetings

- Employee Association topics
- Policy manual updates (ongoing)
- Policy Updates related to travel and per diem (requested by Dir. Williams)
- General Manager’s job description (present to full Board)

11. Next Meeting Date:

Regular Meeting Tuesday, January 21, 2025, at 6 p.m.

ADJOURNMENT: 7:25 p.m.

Attest:

DRAFT UNTIL APPROVED

John Covington, Chairman
to the Personnel Committee of the Beaumont-Cherry Valley Water District



**Beaumont-Cherry Valley Water District
Personnel Committee Meeting
January 21, 2025**

Item 5

HUMAN RESOURCES REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: Human Resources Department Report for the Months of November and December 2024

Table 1: Personnel

The below table represents the District’s current Workforce.

As of November 30, 2024

Total Current Employees (Excluding Board Members)	45
Full-Time Employees	44
Part-Time	1
Temporary	0
Interns	0
Separations	1
Retired Employee(s)	0

As of December 31, 2024

Total Current Employees (Excluding Board Members)	45
Full-Time Employees	43
Part-Time	1
Temporary	1
Interns	0
Separations	1
Retired Employee(s)	0

Table 2: New Hires

The below table represents new hires.

As of November 30, 2024

Employee Name	Job Title	Department
None		

As of December 31, 2024

Employee Name	Job Title	Department
Marlon Jones	Water Utility Worker I (Temp)	Operations



Table 3: Anniversaries*

The below table represents BCVWD employee anniversaries.

As of November 30, 2024

Employee Name	Department	Years of Service
Joe Reichenberger	Engineering	18 years
Edmund Clark	Operations	4 years
Jeremy McCarty	Operations	4 years
Thomas Lamont	Operations	3 years
Jordan Smith	Operations	3 years
Dontae Williams	Operations	2 years
Andrew Powell	Operations	1 year

As of December 31, 2024

Employee Name	Department	Years of Service
Lilian Tienda	Engineering	1 year

**Work Anniversaries for the purposes of this report are calculated from the hire date and do not determine employment conditions or terms. This report does not include elected officials.*

Table 4: Promotions or Division/Title Change

The below table represents promotions or Division/Title Changes.

As of November 30, 2024

Employee Name	Former Title	Changed to
None		

As of December 31, 2024

Employee Name	Former Title	Changed to
None		

Table 5: Recruitment

The below table represents active/closed recruitment(s).

As of November 30, 2024

Position	Department	Update
Temporary Water Utility Worker I	Operations	Posting Opened 11/01/2024 Posting Closed 11/22/2024



As of December 31, 2024

Position	Department	Update
Temporary Water Utility Worker I	Operations	Interviews on-going

Table 6: Separation/Retirement

The below table represents employees separating from BCVWD.

As of November 30, 2024

Employee Name	Position Held	Department	Last Day
Tyler O'Hara	Water Utility Worker I	Operations	11/14/2024

As of December 31, 2024

Employee Name	Position Held	Department	Last Day
Oliver Rocha	Water Utility Worker I	Operations	12/19/2024

Table 7: Communications

The below table represents HR communications to BCVWD employees.

As of November 30, 2024

Communication	Topic
HR Memo 24-020, Voting Leave Policy for 2024 US General Elections Day	Policy
HR Memo 24-022, Workplace Conduct During Election Season	Workplace Conduct
HR Memo 24-023, Thanksgiving Holiday Closure, Timesheet, and Holiday Pay Reminder	Policy

As of December 31, 2024

Communication	Topic
HR Memo 24-024, Christmas Day Holiday Closure, Timesheet, and Holiday Pay Reminder	Policy
HR Memo 24-025, New Year's Day Holiday Closure, Timesheet, and Holiday Pay Reminder	Policy

Staff Report Prepared by Ren Berioso, Human Resources Manager



**Beaumont-Cherry Valley Water District
Personnel Committee
January 21, 2025**

Item 6a

STAFF REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

**SUBJECT: Policies and Procedures Manual Updates/Revisions Amending Policy 3145
Driver Training and Record Review**

Staff Recommendation

Approve the revision of Policy 3145 Driver Training and Record Review to move forward to the next Board of Directors meeting with the recommendations stated in Table 1, Summary of Policy Changes, or direct staff as desired.

Executive Summary

At the November 19, 2024 Personnel Committee meeting, Human Resources (HR) staff proposed a revision of Policy 3145, *Driver Training and Record Review*, to modernize the language, clarify the time frame for determining the start date of infractions in accordance with California DMV regulations, and eliminate redundant language. The Personnel Committee approved the policy draft but directed staff to clarify the dynamics of a "12-month driving probation" and to seek further legal advice regarding whether the District is obligated to cover the costs of enrolling an employee in a defensive driving class as a form of disciplinary action.

Background

At the November 19, 2024 Personnel Committee meeting, HR staff proposed revisions to Policy 3145, Driver Training and Record Review, to modernize its language, clarify procedures for determining the start date of infractions in alignment with California DMV regulations, and eliminate redundant language. These updates aimed to streamline the policy, improve clarity, and ensure consistency with other District policies. In addition to refining existing content, HR staff proposed incorporating new sections to align with Policy 3150, District Vehicle Usage, and Policy 3175, Disciplinary Action and Termination, to provide clear guidelines for managing situations where employees incur driving infractions. The proposed revisions are intended to establish clearer expectations for employees, ensure consistent application of disciplinary actions, and reduce legal risks to the District. HR staff emphasized that these changes would improve efficiency, foster accountability, and support a fair and transparent approach to managing driving responsibilities, reflecting the District's commitment to continuous improvement and effective workforce management. The Personnel Committee initially approved the policy draft but instructed staff to clarify the implementation and expectations of a "12-month driving probation" and to seek legal guidance on whether the District is required to cover the cost of enrolling an employee in a defensive driving class as part of disciplinary action before approving the policy changes to advance to the Board of Directors.

As part of the ongoing review of District policies, HR staff conducted a thorough consultation with multiple legal sources to ensure the policy language aligns with current labor laws, particularly Labor Code Section 2802. Legal Counsel has advised that, in accordance with the law, if the District mandates an employee to complete training necessary for performing his/her essential



job functions, the District is responsible for covering the associated direct costs. Additionally, the ACWA JPIA has clarified that employees holding Safety-Sensitive positions are required to complete defensive driving courses, either online or in-person, if they accrue points on their driving record. This requirement ensures compliance with safety standards and mitigates risks associated with their roles. This comprehensive review process also helps safeguard the District against potential legal risks while providing clear and lawful guidelines for both employees and management.

Discussion

Table A, Summary of Policy Changes, outlines the proposed Driver Training and Record Review (policy) that are in reference to the redline draft version attached herewith.

Table A – Summary of Policy Changes

TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Option/s to Consider	Fiscal Impact of Option
1	Section 3145.2	None	This policy applies to all staff who drive the District vehicle.	3145.2 Change the word from “Directors” to “Department Heads “ to provide distinction.	No fiscal impact.
2	Section 3145.5.2	None	The policy places an employee with 3 earned points in his/her driver’s license in a 12-month driving probation.	3145.5.2 Revise the section by keeping the probation and add a corresponding disciplinary action. Also, add language that supervisor will monitor the staff during the probationary period and will assess the driving capability at the end of the time frame.	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Option/s to Consider	Fiscal Impact of Option
3	Section 3145.6	CA Labor Code § 2802	The District pays for the Defensive Driving and costs associated to it if the employee is required by the District.	<p>3145.7. Per Labor Code Section 2802 and Legal Counsel's advice, if required by the employer to attend a defensive driving class whether as part of the disciplinary action or training, the employee shall be indemnified of the costs.</p> <p>Also, ACWA JPIA requires that if an employee has earned points in his/her driver's license, he/she is required to complete the defensive driving class if driving the District vehicle is an essential part of his/her role.</p>	The cost of the Defensive Driving class plus other costs such as Over-Time rate and mileage reimbursement.

Fiscal Impact

The fiscal impact is the appropriate District funding for the Defensive Driving class, including associated overtime pay and mileage expenses if required under Section 3145.5 Disciplinary Procedures. These expenses are all accounted for in the annual operating budget.

Attachments

1. Redline draft version of Policy 3145 Driver Training and Record Review
2. Side-by-side version of Policy 3145 Driver Training and Record Review
3. Clean draft version of Policy 3145 Driver Training and Record Review
4. Labor Code Section 2802

Staff Report prepared by Ren Berioso, Human Resources Manager

6a - Attachment 1

BEAUMONT-CHERRY VALLEY WATER DISTRICT

POLICY TITLE: DRIVER TRAINING AND RECORD REVIEW
POLICY NUMBER: 3145

3145.1 **Purpose.** The purpose of this policy is to reduce the frequency and severity of vehicle-related accidents and losses by:

1. Applying uniform criteria in evaluating the acceptability of driver-record information of individuals driving District vehicles or while on District business; or
2. Establishing disciplinary procedures for different types of driving violations.

3145.2 **Scope.** This policy applies to all regular, part-time, and temporary District employees and volunteers who drive on behalf of the District, and while driving the District vehicle. ~~Directors~~ Department Heads are required to provide their license information if driving is part of their essential job function.

3145.3 **Implementation.** The District shall participate in the Department of Motor Vehicles (DMV) Employer Pull Notice Program ("Pull Program"). Records for anyone operating vehicles on District business shall be requested from DMV:

1. Every six (6) months; and
2. Immediately in the event of new activity (e.g. moving violation, accident, address change, etc.). Employees who have terminated employment will be deleted from the program.

3145.4 **Review Criteria.** Information that will be generated during the record review will include:

1. Type of license;
2. Expiration Date;
3. Endorsements;
4. DMV action suspensions, revocations, and penal code violations; and
5. Vehicle Code Violations.

3145.5 **Disciplinary Procedures:**

1. A driver employed by the District shall immediately attend a qualified defensive driver training course (State of California Defensive Driver Training, National Safety Council Defensive Driver Training, etc.) if:
 - a. He/she earns two points within thirty-six (36) months from the current date.
 - b. He/she receives any moving violation in a District vehicle within thirty-six (36) months from the current date
 - c. He/she is involved in an accident while using the District vehicle within thirty-six (36) months from the current date.

2. A driver employed by the District will be placed on a twelve (12) month driving probation with a corresponding corrective action (e.g. written warning or final written warning) if he/she earns three (3) points within thirty-six (36) months from the current date. The immediate supervisor, in collaboration with Human Resources, will actively monitor the employee's driving performance throughout the 12-month probationary period and evaluate their suitability for continued driving responsibilities at its conclusion.

BEAUMONT-CHERRY VALLEY WATER DISTRICT

- 3.2. A driver employed by the District will be suspended from District driving privileges for one hundred twenty (120) days or as determined by DMV whichever is longer if:
- He/she earns four (4) or more points within thirty-six (36) months other than DUI, reckless driving or speed contest of over 100mph from the current date.
 - He/she receives a citation for DUI, reckless driving, or speed contest over 100mph on personal time within thirty-six (36) months from the current date.
 - If he/she is involved in two chargeable (resulting in a point violation) accidents within twenty-four (24) months while using the District vehicle or during personal time.
- 4.3. A driver employed by the District will be permanently suspended of District driving privileges if:
- He/she receives a citation for DUI, reckless driving, or speed contest over 100mph while driving the District vehicle within thirty-six (36) months from the current date.
 - He/she receives another citation for DUI, reckless driving, or speed contest over 100mph on personal time resulting in DMV's suspension or revocation of the employee's driving privilege within thirty-six (36) months from the first citations listed herein.
- 5.4. Occasionally, it may be brought to the District's attention that an employee is exposing the District to undue liability through poor driving techniques and habits. All such complaints will be investigated and acted upon accordingly.
- 6.5. If an employee's job routinely involves driving the District vehicle and if having driving privileges suspended either temporarily or permanently would impose a hardship on normal District operations, the General Manager or his/her designee may review the employee's case for possible disciplinary action or termination of employment (see Policy 3150 District Vehicle Usage for more information). This includes situations where DMV suspends or revokes an employee's driving privilege for any reason and for any given time frame. The General Manager or his/her designee is not obligated to assign an employee with a suspended or revoked driving privilege to a temporary non-driving duty while the case is being litigated, investigated or reviewed.
- 7.6. For the purpose of counting the time frame of the infraction or violation, time is measured backwards from the date of the infraction or violation.
- 8.7. The employee is obligated to inform the District through its Human Resources of any infractions incurred resulting in a point violation against his/her driver's license, and any litigation updates as soon as possible.

3145.6 **General Manager.** If the General Manager operates a vehicle on District business or personal time, whether by assignment or through a contractual agreement, and commits any violations outlined in the preceding sections, the full Board may engage an external consultant to investigate the matter. Based on this policy, the Board shall determine and implement the appropriate corrective measures.

3145.7 **Defensive Driver Training:** All employees whose job routinely involves driving the District vehicle drivers shall attend an approved defensive driver training course at least once every four years, or more often as specified in Disciplinary Procedures, above. Department Heads Directors are required encouraged to attend courses if driving is part of their essential job function, but cannot be required to do so in accordance with State law. If required under Section 3145.5 Disciplinary Procedures, the District shall pay General Manager or his/her designee will determine the appropriate funding for the Defensive Driving class, including any overtime pay and mileage expenses incurred by the employee.

Commented [RTG1]: Do you mean compensation? Funding implies that the District may or may not be able to pay for the classes, but it would be required to pay for them under Labor Code section 2802.

6a - Attachment 2

CURRENT POLICY

POLICY TITLE: DRIVER TRAINING AND RECORD REVIEW
POLICY NUMBER: 3145

3145.1 **Purpose.** The purpose of this policy is to reduce the frequency and severity of vehicle-related accidents and losses by:

1. Applying uniform criteria in evaluating the acceptability of driver record information of individuals driving District vehicles or while on District business; or
2. Establishing disciplinary procedures for different types of driving violations.

3145.2 **Scope.** This policy applies to all regular, part-time, and temporary District employees and volunteers who drive on behalf of the District. Districts are encouraged to provide their license information, but cannot be required to do so in accordance with State law.

3145.3 **Implementation.** The District shall participate in the Department of Motor Vehicles (DMV) Employer Pull Notice Program ("Pull Program"). Records for anyone operating vehicles on District business shall be requested from DMV:

1. Every six (6) months; and
2. Immediately in the event of new activity (e.g. moving violation, accident, address change, etc.). Employees who have terminated employment will be deleted from the program.

3145.4 **Review Criteria.** Information that will be generated during the record review will include:

1. Type of license;
2. Expiration Date;
3. Endorsements;
4. DMV action suspensions, revocations, and penal code violations; and
5. Vehicle Code Violations.

3145.5 **Disciplinary Procedures:**

1. A driver will immediately attend a qualified defensive driver training course (State of California Defensive Driver Training, National Safety Council Defensive Driver Training, etc.) if:
 - a. They earn two points within thirty-six (36) months
 - b. They receive any moving violation in a District vehicle within thirty-six (36) months.
 - c. They are involved in an accident within thirty-six (36) months.
2. A driver will be placed on a twelve (12) month driving probation if they earn three (3) to five (5) points within thirty-six (36) months. Additional point violations within this probationary period will affect a one-hundred twenty (120) days suspension of District driving privileges. If their job routinely involves driving a vehicle and if having driving privileges suspended would impose a hardship on normal District operations, they will be terminated from employment.
3. A driver will be suspended from District driving privileges for one hundred twenty (120) days if:
 - a. They earn four (4) or more points within twenty-four (24) months.
 - b. They earn six (6) or more points within thirty-six (36) months.
 - c. They receive a citation for DUI, reckless driving, or speed contest on personal time within thirty-six (36) months.

PROPOSED POLICY

POLICY TITLE: DRIVER TRAINING AND RECORD REVIEW
POLICY NUMBER: 3145

3145.1 **Purpose.** The purpose of this policy is to reduce the frequency and severity of vehicle-related accidents and losses by:

1. Applying uniform criteria in evaluating the acceptability of driver record information of individuals driving District vehicles or while on District business; or
2. Establishing disciplinary procedures for different types of driving violations.

3145.2 **Scope.** This policy applies to all regular, part-time, and temporary District employees and volunteers who drive on behalf of the District, and while driving the District vehicle. ~~District~~ Department Heads are required to provide their license information if driving is part of their essential job function.

3145.3 **Implementation.** The District shall participate in the Department of Motor Vehicles (DMV) Employer Pull Notice Program ("Pull Program"). Records for anyone operating vehicles on District business shall be requested from DMV:

1. Every six (6) months; and
2. Immediately in the event of new activity (e.g. moving violation, accident, address change, etc.). Employees who have terminated employment will be deleted from the program.

3145.4 **Review Criteria.** Information that will be generated during the record review will include:

1. Type of license;
2. Expiration Date;
3. Endorsements;
4. DMV action suspensions, revocations, and penal code violations; and
5. Vehicle Code Violations.

3145.5 **Disciplinary Procedures:**

1. A driver employed by the District shall immediately attend a qualified defensive driver training course (State of California Defensive Driver Training, National Safety Council Defensive Driver Training, etc.) if:
 - a. He/she earns two points within thirty-six (36) months from the current date.
 - b. He/she receives any moving violation in a District vehicle within thirty-six (36) months from the current date
 - c. He/she is involved in an accident while using the District vehicle within thirty-six (36) months from the current date.
2. A driver employed by the District will be placed on a twelve (12) month driving probation with a corresponding corrective action (e.g. written warning or final written warning) if he/she earns three (3) points within thirty-six (36) months from the current date. The immediate supervisor, in collaboration with Human Resources, will actively monitor the employee's driving performance throughout the 12-month probationary period and evaluate their suitability for continued driving responsibilities at its conclusion.

- d. If they are involved in two chargeable (resulting in a point violation) accidents within twenty-four (24) months, if their job routinely involves driving a vehicle and if having driving privileges suspended would impose a hardship on normal District operations, permanent suspension of driving privileges will result in termination of employment.
4. A driver will be permanently suspended of District driving privileges if:
- a. They receive a citation for DUI, reckless driving, or speed contest during District business within thirty-six (36) months.
 - b. They receive two citations for DUI, two citations for reckless driving, or two citations for speed contest on personal time within twelve (12) months. If their job routinely involves driving a vehicle and if having driving privileges suspended would impose a hardship on normal District operations, permanent suspension of driving privileges will result in termination of employment.
5. Occasionally, it may be brought to the District's attention that an employee is exposing the District to undue liability through poor driving techniques and habits. All such complaints will be investigated and acted upon accordingly.

3145.6 Defensive Driver Training. All drivers shall attend an approved defensive driver training course at least once every four years or more often as specified in Disciplinary Procedures, above. Directors are encouraged to attend courses, but cannot be required to do so in accordance with State law.

- ~~3-2.~~ A driver employed by the District will be suspended from District driving privileges for one hundred twenty (120) days or as determined by DMV whichever is longer if:
- a. He/she earns four (4) or more points within thirty-six (36) months other than DUI, reckless driving or speed contest of over 100mph from the current date.
 - b. He/she receives a citation for DUI, reckless driving, or speed contest over 100mph on personal time within thirty-six (36) months from the current date.
 - c. If he/she is involved in two chargeable (resulting in a point violation) accidents within twenty-four (24) months while using the District vehicle or during personal time.

- ~~4-3.~~ A driver employed by the District will be permanently suspended of District driving privileges if:
- a. He/she receives a citation for DUI, reckless driving, or speed contest over 100mph while driving the District vehicle within thirty-six (36) months from the current date.
 - b. He/she receives another citation for DUI, reckless driving, or speed contest over 100mph on personal time resulting in DMV's suspension or revocation of the employee's driving privilege within thirty-six (36) months from the first citations listed herein.

~~5-4.~~ Occasionally, it may be brought to the District's attention that an employee is exposing the District to undue liability through poor driving techniques and habits. All such complaints will be investigated and acted upon accordingly.

~~6-5.~~ If an employee's job routinely involves driving the District vehicle and if having driving privileges suspended either temporarily or permanently would impose a hardship on normal District operations, the General Manager or his/her designee may review the employee's case for possible disciplinary action or termination of employment (see Policy 3150 District Vehicle Usage for more information). This includes situations where DMV suspends or revokes an employee's driving privilege for any reason and for any given time frame. The General Manager or his/her designee is not obligated to assign an employee with a suspended or revoked driving privilege to a temporary non-driving duty while the case is being litigated, investigated or reviewed.

~~7-6.~~ For the purpose of counting the time frame of the infraction or violation, time is measured backwards from the date of the infraction or violation.

~~8-7.~~ The employee is obligated to inform the District through its Human Resources of any infractions incurred resulting in a point violation against his/her driver's license, and any litigation updates as soon as possible.

3145.6 General Manager. If the General Manager operates a vehicle on District business or personal time, whether by assignment or through a contractual agreement, and commits any violations outlined in the preceding sections, the full Board may engage an external consultant to investigate the matter. Based on this policy, the Board shall determine and implement the appropriate corrective measures.

~~3145.76 Defensive Driver Training:~~ All employees whose job routinely involves driving the District vehicle shall attend an approved defensive driver training course at least once every four years. ~~or more often as specified in Disciplinary Procedures above.~~ Department Heads/Directors are required encouraged to attend courses if driving is part of their essential job function, but cannot be required to do so in accordance with State law. If required under Section 3145.5 Disciplinary Procedures, the District shall pay General Manager or his/her designee will determine the appropriate funding for the Defensive Driving class, including any overtime pay and mileage expenses incurred by the employee.

POLICY TITLE: DRIVER TRAINING AND RECORD REVIEW**POLICY NUMBER: 3145**

3145.1 **Purpose.** The purpose of this policy is to reduce the frequency and severity of vehicle-related accidents and losses by:

1. Applying uniform criteria in evaluating the acceptability of driver-record information of individuals driving District vehicles or while on District business; or
2. Establishing disciplinary procedures for different types of driving violations.

3145.2 **Scope.** This policy applies to all regular, part-time, and temporary District employees and volunteers who drive on behalf of the District, and while driving the District vehicle. Department Heads are required to provide their license information if driving is part of their essential job function.

3145.3 **Implementation.** The District shall participate in the Department of Motor Vehicles (DMV) Employer Pull Notice Program ("Pull Program"). Records for anyone operating vehicles on District business shall be requested from DMV:

1. Every six (6) months; and
2. Immediately in the event of new activity (e.g. moving violation, accident, address change, etc.). Employees who have terminated employment will be deleted from the program.

3145.4 **Review Criteria.** Information that will be generated during the record review will include:

1. Type of license;
2. Expiration Date;
3. Endorsements;
4. DMV action suspensions, revocations, and penal code violations; and
5. Vehicle Code Violations.

3145.5 **Disciplinary Procedures:**

1. A driver employed by the District shall immediately attend a qualified defensive driver training course (State of California Defensive Driver Training, National Safety Council Defensive Driver Training, etc.) if:
 - a. He/she earns two points within thirty-six (36) months from the current date.
 - b. He/she receives any moving violation in a District vehicle within thirty-six (36) months from the current date
 - c. He/she is involved in an accident while using the District vehicle within thirty-six (36) months from the current date.

A driver employed by the District will be placed on a twelve (12) month driving probation with a corresponding corrective action (e.g. written warning or final written warning) if he/she earns three (3) points within thirty-six (36) months from the current date. The immediate supervisor, in collaboration with Human Resources, will actively monitor the employee's driving performance throughout the 12-month probationary period and evaluate their suitability for continued driving responsibilities at its conclusion.

2. A driver employed by the District will be suspended from District driving privileges for one hundred twenty (120) days or as determined by DMV whichever is longer if:
 - a. He/she earns four (4) or more points within thirty-six (36) months other than DUI,

BEAUMONT-CHERRY VALLEY WATER DISTRICT

- reckless driving or speed contest of over 100mph from the current date.
- b. He/she receives a citation for DUI, reckless driving, or speed contest over 100mph on personal time within thirty-six (36) months from the current date.
 - c. If he/she is involved in two chargeable (resulting in a point violation) accidents within twenty-four (24) months while using the District vehicle or during personal time.
3. A driver employed by the District will be permanently suspended of District driving privileges if:
 - a. He/she receives a citation for DUI, reckless driving, or speed contest over 100mph while driving the District vehicle within thirty-six (36) months from the current date.
 - b. He/she receives another citation for DUI, reckless driving, or speed contest over 100mph on personal time resulting in DMV's suspension or revocation of the employee's driving privilege within thirty-six (36) months from the first citations listed herein.
 4. Occasionally, it may be brought to the District's attention that an employee is exposing the District to undue liability through poor driving techniques and habits. All such complaints will be investigated and acted upon accordingly.
 5. If an employee's job routinely involves driving the District vehicle and if having driving privileges suspended either temporarily or permanently would impose a hardship on normal District operations, the General Manager or his/her designee may review the employee's case for possible disciplinary action or termination of employment (see Policy 3150 District Vehicle Usage for more information). This includes situations where DMV suspends or revokes an employee's driving privilege for any reason and for any given time frame. The General Manager or his/her designee is not obligated to assign an employee with a suspended or revoked driving privilege to a temporary non-driving duty while the case is being litigated, investigated or reviewed.
 6. For the purpose of counting the time frame of the infraction or violation, time is measured backwards from the date of the infraction or violation.
 7. The employee is obligated to inform the District through its Human Resources of any infractions incurred resulting in a point violation against his/her driver's license, and any litigation updates as soon as possible.

3145.6 General Manager. If the General Manager operates a vehicle on District business or personal time, whether by assignment or through a contractual agreement, and commits any violations outlined in the preceding sections, the full Board may engage an external consultant to investigate the matter. Based on this policy, the Board shall determine and implement the appropriate corrective measures.

3145.7 Defensive Driver Training: All employees whose job routinely involves driving the District vehicle shall attend an approved defensive driver training course once every four years. Department Heads are required to attend courses if driving is part of their essential job function. If required under Section 3145.5 Disciplinary Procedures, the District shall pay for the Defensive Driving class, including any overtime pay and mileage expenses incurred by the employee.

KOKOZIAN LAW FIRM
A PROFESSIONAL LAW CORPORATION
LAWYERS FOR EMPLOYEE RIGHTS

Reimbursement of Work Expenses

Workers in California have a broad right to reimbursement for work expenses. Reimbursable expenses can include mileage for use of the worker's motor vehicle in the discharge of the employee's duties, as well as parking, hotel, restaurant, and airfare charges.

Originally enacted in 1937, California Labor Code section 2802 mandates that "An employer shall indemnify his or her employee for all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties, or of his or her obedience to the directions of the employer, even though unlawful, unless the employee, at the time of obeying the directions, believed them to be unlawful."

"[T]he broad purpose of Labor Code section 2802 is to require an employer to bear all of the costs inherent in conducting its business and to indemnify employees from costs incurred in the discharge of their duties for the employer's benefit." *In re Acknowledgment Cases* (2015) 239 Cal.App.4th 1498, 1506. The statute aims to protect California workers by preventing "employers from passing their operating expenses on to their employees." *Gattuso v. Harte-Hanks Shoppers, Inc.* (2007) 42 Cal.4th 554, 562. Any contract or agreement between an employer and employee waiving the employee's right to reimbursement for work expenses is invalid. California Labor Code section 2804.

There are two key elements to this statute. First, the employee shall be reimbursed only for "necessary expenditures." These shall include "all reasonable costs, including, but not limited to, attorney's fees incurred by the employee enforcing the rights granted by this section." California Labor Code section 2802(c). For instance, an employee is required to have a power drill to carry out the duties of his employment and the employer does not supply one. If the employee buys a set of power equipment that comes with other tools besides the drill, then the accompanying tools might not be recognized by a court as a reimbursable expense under the statute. However, the employee would still be entitled to reimbursement for the drill, because the job required use of a drill and the employer did not provide one.

Secondly, the expenditures must be in "direct consequence of the discharge of his or her duties." California Labor Code section 2802(a). A common example of a work expense in today's work environment is a phone bill. Some workers may be required to bring a cellular phone with them as they work in order to contact the business, clients, or other people associated with the performance of his or her job, when necessary. Often, an employee will not realize that these phone calls are inflating the rate of his or her phone bill. However, if the calls are necessary for the discharge of his or her duties and the calls affect the phone bill amount, then the employee is entitled under the law to reimbursement for each occasion where the employee used the employee's personal phone for work. See *Cochran v. Schwan's Home Service, Inc.* (2014) 228 Cal.App.4th 1137.

Similarly, an employee required to drive his vehicle in order to perform his work duties would also be entitled to reimbursement for fuel expenses directly attributable to his work-related travel.

Employer-Required Educational Program or Training

"Section 2802 applies to any expense or cost of any employer-provided or employer-required educational program or training for an employee providing direct patient care or an applicant for direct patient care employment. Those expenses or costs shall constitute a necessary expenditure or loss incurred by the employee in direct consequence of the discharge of the employee's duties, as that phrase is used in Section 2802." California Labor Code section 2802.1.

Claims for Failure to Reimburse Work Expenses

The elements of a failure to reimburse claim are:

- the worker made expenditures or incurred losses;
- the expenditures or losses were incurred as a direct consequence of the employee's job duties or in obedience to the directions of the employer;
- the expenditures or losses were necessary; and
- The employer did not exercise due diligence to reimburse the expenditures.

USS-POSCO Indus. v. Case (2016) 244 Cal.App.4th 197, 205; *Cochran v. Schwan's Home Service, Inc.* (2014) 228 Cal.App.4th 1137, 1140-1141.

An employee who successfully brings a claim for failure to reimburse work expenses is entitled to interest and costs, including attorney's fees under California Labor Code section 2802(c). The rationale for the entitlement to costs and attorney's fees is that without the right to recover attorney fees a California Labor Code section 2802 claim would essentially be useless to employees, as the cost of hiring a lawyer to enforce their rights could very well be greater than the unreimbursed expenses they are trying to recover. Thus, employers who did not wish to reimburse work expenses could simply refuse to reimburse those expenses, knowing employees were unlikely to take action given that it might cost the employee more to enforce his rights under the statute than the amount the employee could recover.

Note: An employer may not be vicariously liable or obligated to reimburse expenses if the conduct that gave rise to the expense substantially deviates from the employee's "course of duty so as to amount to a complete departure." *Jacobus v. Krambo Corp.* (2000) 78 Cal.App.4th 1096, 1101-1102.

Mileage Reimbursement

Employees are entitled to mileage reimbursement, even if the employer pays enhanced wages aimed at covering that expense. However, an enhanced wage scheme may be proper if the employer provides a means of distinguishing the amount being paid for labor performed from the amount being paid as reimbursement for work expenses. *Espejo v. The Copley Press, Inc.* (2017) 13 Cal.App.5th 329.

Traffic and Parking Tickets

Speeding and parking tickets are not reimbursable as work expenses under California Labor Code section 2802, as the statute does not entertain reimbursement for expenses arising from conduct that is unlawful and that the employee believes is unlawful. *Villalpando v. Exel Direct Inc.* (2016) 161 F.Supp.3d 873.

Independent Contractors

Independent contractors are generally engaged to do specific jobs and cannot be fired before the job is complete unless they violate the terms of the contract between the parties. Workers who under California law are independent contractors are not employees and thus they are not entitled to reimbursement of work expenses under California Labor Code section 2802. *Arnold v. Mutual of Omaha Ins. Co.* (2011) 202 Cal.App.4th 580.

Contact Us



**Beaumont-Cherry Valley Water District
Personnel Committee
January 21, 2025**

Item 6b

STAFF REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: Policies and Procedures Manual Updates/Revisions establishing Information Technology Policy Number 7004 Email and Communication

Staff Recommendation

Approve the establishment of Information Technology (IT) Policy Number 7004 Email and Communication to move forward to the next Board of Directors meeting, or direct staff as desired.

Executive Summary

Staff is proposing the establishment of IT Policy Number 7004 Email and Communication with sections that provide guidelines for authorized use, data protection, retention, and monitoring while prohibiting misuse, safeguarding sensitive communications, and promoting efficient, professional practices. The IT policy draft ensures the secure, responsible, and compliant use of District email systems, aligning with the standards of National Institute of Standards and Technology (NIST) and state regulations such as the California Public Records Act (CPRA) and California Consumer Privacy Act (CCPA).

Background

At the November 19, 2024 meeting, the Director of IT requested the Personnel Committee to review the Employee IT policy handbook to ensure they align with the district's strategic goals, legal requirements, and regulatory standards. This oversight fosters accountability, transparency, and overall guidance to personnel, reinforcing the District's commitment to effective IT governance and cybersecurity. With Human Resources (HR) as the custodian of the District's Policy Manual, HR staff partnered with the Director of IT in the review of the Employee IT policy handbook.

The Employee IT policy handbook is crucial for outlining policies, procedures, and expectations related to technology use, ensuring security compliance, and protecting both employees and the organization. The history of the Employee IT Policy Handbook and the IT and Cybersecurity Policy Manual reflects Beaumont-Cherry Valley Water District's (BCVWD) commitment to fostering a secure, compliant, and informed technology environment. First drafted in 2014, the Employee IT Policies Handbook is updated annually by the IT Department to align with evolving technology standards and is provided to all employees during new hire orientation to ensure consistent understanding of IT policies. Similarly, the IT and Cybersecurity Policy Manual, created in 2017, establishes administrative policies that align with the NIST framework and is updated annually to maintain compliance with laws, regulations, and industry best practices. Both documents underwent extensive review in their most recent updates, further strengthening their relevance and effectiveness. These efforts contributed to the district earning the prestigious Municipal Information Systems Association of California (MISAC) award for the last two (2) years, demonstrating leadership and excellence in IT governance and cybersecurity management.



As part of the ongoing review process of all District policies, HR staff, in partnership with IT Department presented the proposed policy draft to Legal Counsel to ensure compliance with applicable Federal, State and local labor laws.

Discussion

An Email and Communications IT policy is vital for the District to ensure secure, professional, and compliant use of communication systems, protecting sensitive information and maintaining operational integrity. Table A, Summary of Policy Sections, outlines the proposed Email and Communications (policy) that was drafted by HR and IT Departments.

Table A – Summary of Policy Sections

TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	Section 7004.1	NIST, CPRA and CCPA	The District's IT policies are aligned with NIST, CPRA and CCPA.	Consider establishing Section 7004.1 Introduction	No fiscal impact.
2	Section 7004.2	NIST, CPRA and CCPA	The purpose of this policy is to secure the District's email and communication systems.	Consider establishing Section 7004.2 Purpose	No fiscal impact.
3	Section 7004.3	NIST, CPRA and CCPA	IT Email and Communication policies are applicable to all employees, contractors and third parties for District-related functions.	Consider establishing Section 7004.3 Scope.	No fiscal impact.
4	Sections 7004.4.1.1 to 7004.4.1.4	NIST, CPRA and CCPA	The District requires all the the users to use the email and communications systems strictly for business and to maintain professionalism. Personal accounts are also prohibited.	Consider establishing Sections 7004.4.1.1 to 7004.4.1.4 General Use and Ownership.	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
5	Sections 7004.4.2.1 to 7004.4.2.4	NIST, CPRA and CCPA	The District email use must follow strict security protocols, including encryption, multi-factor authentication, cautious handling of unknown emails, and compliance with the Mobile Device Management Policy.	Consider establishing Sections 7004.4.2.1 to 7004.4.2.4 Security Measures	No fiscal impact.
6	Sections 7004.4.3.1 to 7004.4.3.2	NIST, CPRA and CCPA	District maintains that business emails must be retained and archived per BCVWD's policy to comply with the CPRA, and deletion of critical records requires proper authorization.	Consider establishing Sections 7004.4.3.1 to 7004.4.3.2 Retention and Transparency	No fiscal impact.
7	Sections 7004.4.4.1 to 7004.4.4.3	NIST, CPRA and CCPA	BCVWD maintains that work email accounts must only be used for professional purposes, prohibiting inappropriate content, personal gain, and non-work-related activities.	Consider establishing Sections 7004.4.4.1 to 7004.4.4.3 Retention and Transparency	No fiscal impact.
8	Sections 7004.4.5.1 to 7004.4.5.2	NIST, CPRA and CCPA	The District highly encourage the use descriptive subject lines for clarity and limit "Reply All" to essential communications to maintain email efficiency.	Consider establishing Sections 7004.4.5.1 to 7004.4.5.2 Best Practices	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
9	Section 7004.4.6.1	NIST, CPRA and CCPA	The District if needed, may monitor email systems to ensure policy compliance while adhering to state laws and respecting employee privacy	Consider establishing Section 7004.4.6.1 Monitoring	No fiscal impact.
10	Sections 7004.4.7.1 to 7004.4.7.2	NIST, CPRA and CCPA	In practice, suspected email security incidents must be reported to IT immediately and will be handled per BCVWD's Incident Response Policy for prompt resolution and documentation.	Consider establishing Sections 7004.4.7.1 to 7004.4.7.2 Reporting Incidents	No fiscal impact.
11	Section 7004.4.8.1	NIST, CPRA and CCPA	The District email communications comply with the CPRA for transparency and the CCPA to protect sensitive data.	Consider establishing Section 7004.4.8.1 California Compliance	No fiscal impact.
12	Sections 7004.4.9.1 to 7004.4.9.2	NIST, CPRA and CCPA	At the District, employees are required to securely handle regulatory, disaster-related, and water sector communications while protecting confidential information in email exchanges.	Consider establishing Sections 7004.4.9.1 to 7004.4.9.2 Water Sector Guidelines	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
13	Section 7004.4.10.1	NIST, CPRA and CCPA	BCVWD maintains that email communications with third-party vendors must adhere to BCVWD's security standards, with vendors following secure practices per contractual agreements.	Consider establishing Section 7004.4.10.1 Third Party Communications	No fiscal impact.
14	Section 7004.5	NIST, CPRA and CCPA	The District through its IT and HR Departments will annually review the "Email and Communication" policy to ensure its effectiveness, compliance with regulations, alignment with NIST standards, and adherence to local and state laws, making necessary updates to support the District's mission.	Consider establishing Section 7004.5 Introduction	No fiscal impact.

Fiscal Impact: None.

Attachments

1. Draft and Clean version of Policy 7004: Email and Communication
2. National Institute of Standards and Technology (NIST) Fact Sheet
3. California Public Records Act (CPRA) FAQ
4. California Consumer Privacy Act (CCPA) Summary and Key Issues

Staff Report prepared by Ren Berioso, Human Resources Manager

6b - Attachment 1

Policy Title: Email and Communication
Policy Number: 7004

7004.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) relies on email and communication tools as essential methods for conducting business. This policy ensures these tools are used securely, responsibly, and in alignment with the National Institute of Standards and Technology (NIST) principles, which provide a framework for cybersecurity and data protection. As a California Special District, BCVWD adheres to state regulations, including compliance with the California Public Records Act (CPRA) and the California Consumer Privacy Act (CCPA), ensuring transparency, accountability, and data security in communications.

7004.2 Purpose. The purpose of this policy is to establish guidelines for the appropriate and secure use of BCVWD's email and communication systems, minimize risks such as data breaches and misuse, and ensure compliance with NIST standards and California laws.

7004.3 Scope. This policy applies to all employees, contractors, and third parties who use BCVWD's email and communication systems for business purposes.

7004.4 Policy Details

1. General Use and Ownership

- a. Employees must use BCVWD's email and communication systems for authorized business purposes only.
- b. All emails must use clear, friendly, and business-appropriate language to maintain professionalism.
- c. Personal email accounts are not permitted for District business use under any circumstances.
- d. Employees are discouraged from accessing personal email accounts while using District devices to maintain system integrity and focus on work-related activities.

2. Security Measures

- a. Emails containing sensitive, confidential, or personally identifiable information (PII) must be encrypted in accordance with NIST standards.
- b. Employees must exercise caution when handling emails from unknown sources to prevent phishing attacks. Avoid clicking on suspicious links or downloading untrusted attachments.
- c. Multi-factor authentication (MFA) is required to access District email accounts to prevent unauthorized access.
- d. Employees accessing District email via mobile devices must use District-approved applications and comply with the Mobile Device Management Policy to ensure secure communications.

3. Retention and Transparency

- a. Business-related emails are subject to retention and archiving per BCVWD's Electronic Data Retention and Records Management Policy to ensure compliance with the California Public Records Act (CPRA).
- b. Employees must not delete emails containing critical business information, compliance records, or other District-related documentation without proper authorization.

4. Prohibited Activities

- a. Sending, receiving, or forwarding inappropriate, offensive, or discriminatory content via email is strictly prohibited.
- b. Employees must not use BCVWD's email system for personal gain, solicitation, or non-work-related activities.
- c. District-issued email accounts must not be used for personal communications unrelated to District operations.

5. Best Practices

- a. Use descriptive subject lines to clarify the content of emails and facilitate easier management of email records.
- b. Limit the use of "Reply All" to essential communications to reduce unnecessary email traffic and maintain efficiency.
- c. Avoid sharing passwords or allowing unauthorized access to District email accounts.

6. Monitoring

- a. BCVWD reserves the right to monitor email and communication systems to ensure compliance with this policy. Monitoring will be conducted in accordance with state laws and District procedures to balance security with employee privacy.

7. Reporting Incidents

- a. Any suspected email-related security incidents, such as phishing attempts, unauthorized access, or email system breaches, must be reported immediately to the IT Department.
- b. Reported incidents will be addressed in accordance with BCVWD's Incident Response Policy, ensuring timely containment, mitigation, and documentation of any breaches.

8. California Compliance

- a. As a California Special District, BCVWD's email communications must comply with the California Public Records Act (CPRA) to ensure transparency and public access to records, and California Consumer Privacy Act (CCPA) to safeguard sensitive employee, customer, and stakeholder data.

9. Water Sector Guidelines

- a. Employees must handle regulatory notices, disaster-related communications, and other water sector specific matters securely, ensuring adherence to District policies and state requirements.
- b. Confidential information related to water infrastructure, vendor communications, customer specific data, or proprietary data must be protected in all email exchanges.

10. Third-Party Communications

- a. When engaging with third-party vendors or contractors via email, employees must ensure that communications adhere to BCVWD's security standards. Vendors are expected to follow secure communication practices as outlined in contractual agreements.

7004.5 Review and Revision Policy. The Information Technology Department will review the "Acceptable Use Policy" annually to ensure it remains current and effective in addressing the needs of the organization and any changes in regulatory or technological requirements. During the review process, the policy will be evaluated for its effectiveness, compliance with relevant regulations, alignment with the National Institute of Standards and Technology (NIST), and adherence to applicable local and state laws governing IT resource usage. Necessary updates or revisions will be made to ensure the policy continues to meet the district's requirements and supports its mission.

Understanding

THE NIST CYBERSECURITY FRAMEWORK

You may have heard about the NIST Cybersecurity Framework, but what exactly is it?

And does it apply to you?

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps

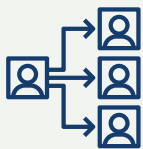
businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

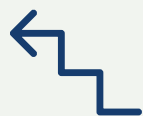
1. IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:



Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.



Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

LEARN MORE AT:
[FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness)



FEDERAL TRADE COMMISSION

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Homeland Security

3. DETECT



Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.



Check your network for unauthorized users or connections.



Investigate any unusual activities on your network or by your staff.

4. RESPOND

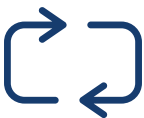
Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly.

5. RECOVER

After an attack:



Repair and restore the equipment and parts of your network that were affected.



Keep employees and customers informed of your response and recovery activities.

For more information on the NIST Cybersecurity Framework and resources for small businesses, go to NIST.gov/CyberFramework and NIST.gov/Programs-Projects/Small-Business-Corner-SBC.

LEARN MORE AT:



FEDERAL TRADE COMMISSION

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Homeland Security

6b Attachment 3

California Public Records Act FAQs

1. What is the California Public Records Act (CPRA)?

The California Public Records Act (CPRA) was passed by the California Legislature in 1968 for government agencies and requires that government records be disclosed to the public, upon request, unless there are privacy and/or public safety exemptions which would prevent doing so. Please see the California Attorney General's Office [Summary of the California Public Records Act](#) [↗](#) (pdf) for additional information.

2. What is a Public Record?

[Government Code §7920.530](#) [↗](#) defines a public record as "any writing containing information relating to the conduct of the public's business prepared, owned, used or retained by any state or local agency regardless of physical form or characteristics." The California Commission on Peace Officer Standards and Training (POST) respects the public's right to access records created and maintained by POST in the course of normal business.

Please ensure that you narrow your request to that which reasonably identifies the desired records that POST may have in its possession in order for staff to more efficiently search for and promptly provide responsive documents. Additionally, please ensure the records you are requesting are under POST's purview and what POST oversees as a state agency. For example, POST has no records related to 911 transcripts, accident/incident reports, warrants, county arrest records, and the like, unless they might be included in an officer's serious misconduct investigation.

The CPRA does not require creation/preparation of a record or document that does not exist at the time of the request. Additionally, certain categories of personal information and records are exempt from disclosure under the CPRA. Other laws also protect individual privacy interests and other propriety information from disclosure.

3. Information to include with your request

Pursuant to [Government Code §7922.600](#), in order to make a focused and effective request for POST records, please include the following applicable information to ensure the scope of the request is narrow and clear enough for personnel to determine if POST has the records you are requesting:

- The subject of the record
- A clear, concise, and specific description of the record(s) being requested
- The date(s) of the record(s), or a time period for your request (e.g.: calendar year 2020)
- Full names for the individuals and/or agencies included in your request, including proper spelling
- POST ID(s) for the individual(s) included in your request if applicable, and/or current/former agency
- Any additional information that helps staff identify the record(s) being requested
- Your contact information for response to your request, preferably an email address

Please make every effort to research the POST records you are requesting, prior to submitting your request. A vast amount of information, resources, and records are already available on the [POST Website](#), by utilizing the search tool, or browsing the topics related to your request. Common questions for information might be found using the following resources:

- [SB978 and Presenter Course Content](#) 
- [SB978 Multimedia Products and Training Videos](#)
- [Certificates](#)
- [Basic Course Training Specifications](#) (by Learning Domain)
- [Basic Course Student Workbooks](#) (by Learning Domain)
- [POST Learning Portal questions](#) 
- [POST Commission Regulations, Procedures, and Authority](#)
- [Investigation Records Pertaining to Officer Misconduct/Decertification](#)  (Government Code section 7923.601)
- [POST Participating Agencies](#)

4. How to make a Public Records Act Request


[Submit Your Own Online Request for POST Records](#) 

(select "Submit Records Request")

Mail:

Attention: California Public Records Act Request
California Commission on Peace Officer Standards and
Training (POST)
860 Stillwater Road, Suite 100
West Sacramento, CA 95605-1630

For questions, email: CPRA@post.ca.gov

Please note: The 10-day period mentioned in the [Government Code §7922.535](#)  is not a deadline for producing records. Should the request be voluminous, or require research, or computer programming, POST may need a reasonable amount of time to research, review, and inspect records prior to release; therefore, it may take longer before the records can be made available. Upon receipt of your request, POST

6b Attachment 4

CCPA Summary and Key Issues
Consent
Enforcement
Financial Incentives
Jurisdictional Thresholds
Information Security
Marketing and Advertising
Notices to Consumers

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

Accept

Deny

Requests for Deletion
Service Providers
Sales of Minors' Information
Sales to Third Parties
Verification of Requestors

[View CCPA Act](#)

CCPA Summary and Key Issues

The California Consumer Privacy Act of 2018 ("CCPA" or "the Act") became effective on January 1, 2020, and is codified at §§1798.100–199 of the Civil Code. The Act offers new and wide-ranging privacy rights for California residents, including a right to be informed about personal data collected by a business and rights to access and delete that information, a right to prevent personal information from being sold to third parties, and a right to data portability. The law

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

Information that nominally falls under one or more of the categories of “personal information” cited in §140(o)(A)–(K) is only personal information if it “identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household”

The consumer private right of action only applies to violations of §150(a), which addresses security procedures and practices

The Act does not apply if it conflict to with the U.S. Constitution

Substantive changes include:

Allowing a business to disclose the consumer’s right to deletion of his/her personal information in a form that is “reasonably accessible to consumers”; previously, the Act required such information to be listed on a business’s website or in its privacy policy

Exempting personal information collected under the California Financial Information Privacy Act; this is in addition to personal information subject to the Gramm–Leach–Bliley Act, which was already exempt under the CCPA

Exempting health care providers and covered entities “to the extent the provider or covered entity maintains patient information in the same manner as medical

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

A.B. 1202. Data brokers. Data brokers must now register with the California Attorney General's office.

A.B. 25. CCPA amendment. One-year exemption for "employee" data.

A.B. 874. CCPA amendment. Adds "reasonably" to the definition of "personal information."

A.B. 1355. CCPA amendment. One-year exemption for "business-to-business" data; numerous drafting errors corrected.

A.B. 1146. CCPA amendment. Exemption for certain information related to motor vehicle repairs and recalls.

A.B. 1130. Breach notification. Adds new types of personal data subject to the state breach notification statute.

Go to an [unofficial version of the Act](#) that incorporates all previous amendments.



This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)



**Beaumont-Cherry Valley Water District
Personnel Committee
January 21, 2025**

Item 6c

STAFF REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: Policies and Procedures Manual Updates/Revisions establishing Information Technology Policy Number 7006 Password

Staff Recommendation

Approve the establishment of Information Technology (IT) Policy Number 7006 Password to move forward to the next Board of Directors meeting, or direct staff as desired.

Executive Summary

Staff is proposing the establishment of IT Policy Number 7006 Password with sections that provide guidelines to ensure that BCVWD's systems, networks, and sensitive data are protected through robust password management practices aligned with National Institute of Standards and Technology (NIST) standards and California cybersecurity regulations. By defining clear requirements for password creation, management, and enforcement, the policy minimizes risks of unauthorized access and data breaches while supporting the District's mission of operational integrity and regulatory compliance, and aligns with the standards of NIST.

Background

At the November 19, 2024 meeting, the Director of IT requested the Personnel Committee to review the Employee IT policy handbook to ensure they align with the district's strategic goals, legal requirements, and regulatory standards. This oversight fosters accountability, transparency, and overall guidance to personnel, reinforcing the District's commitment to effective IT governance and cybersecurity. With Human Resources (HR) as the custodian of the District's Policy Manual, HR staff partnered with the Director of IT in the review of the IT policy handbook.

The Employee IT policy handbook is crucial for outlining policies, procedures, and expectations related to technology use, ensuring security compliance, and protecting both employees and the organization. The history of the Employee IT Policy Handbook and the IT and Cybersecurity Policy Manual reflects Beaumont-Cherry Valley Water District's (BCVWD) commitment to fostering a secure, compliant, and informed technology environment.

First drafted in 2014, the Employee IT Policies Handbook is updated annually by the IT Department to align with evolving technology standards and is provided to all employees during new hire orientation to ensure consistent understanding of IT policies. Similarly, the IT and Cybersecurity Policy Manual, created in 2017, establishes administrative policies that align with the NIST framework and is updated annually to maintain compliance with laws, regulations, and industry best practices. Both documents underwent extensive review in their most recent updates, further strengthening their relevance and effectiveness. These efforts contributed to the district earning the prestigious Municipal Information Systems Association of California (MISAC) award for the last two (2) years, demonstrating leadership and excellence in IT governance and cybersecurity management.



As part of the ongoing review process of all District policies, HR staff, in partnership with IT Department presented the proposed policy draft to Legal Counsel to ensure compliance with applicable Federal, State and local labor laws.

Discussion

The Password policy is essential for safeguarding BCVWD's systems, data, and operations by ensuring secure password management practices that align with regulatory requirements and industry standards. Table A, Summary of Policy Sections, outlines the proposed Password (policy) that was drafted by HR and IT Departments.

Table A – Summary of Policy Sections

TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	Section 7006.1	NIST	At the District, the Password Policy ensures secure access to systems and data by enforcing NIST-aligned practices and complying with state cybersecurity regulations.	Consider establishing Section 7006.1 Introduction	No fiscal impact.
2	Section 7006.2	NIST	This policy defines password requirements to protect BCVWD's IT resources while aligning with NIST guidelines and California cybersecurity laws.	Consider establishing Section 7006.2 Purpose	No fiscal impact.
3	Section 7006.3	NIST	The Password policy is applicable to all individuals accessing BCVWD's IT systems, applications, devices, and password-protected resources, including employees, contractors, and third parties.	Consider establishing Section 7006.3 Scope.	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
4	Sections 7006.4.1.1 to 7006.4.1.4	NIST	The District requires passwords meet complexity standards, use passphrases for security, change default passwords immediately, and avoid generic or shared accounts unless authorized and monitored by IT.	Consider establishing Sections 7006.4.1.1 to 7006.4.1. Password Creation and Complexity	No fiscal impact.
5	Sections 7006.4.2.1 to 7006.4.2.5	NIST	The District requires employees not to reuse passwords, store them insecurely, or use previously used BCVWD passwords, while changes are required only for security concerns; IT evaluates policies periodically, and automated notifications ensure prompt reporting of unauthorized changes.	Consider establishing Sections 7006.4.2.1 to 7006.4.2.5 Password Management	No fiscal impact.
6	Sections 7006.4.3.1 to 7006.4.3.3	NIST	The District requires Multi-factor authentication (MFA) for accessing systems and remote tools, with employees promptly reporting lost secondary authentication methods to maintain security.	Consider establishing Sections 7006.4.3.1 to 7006.4.3.3 Multi-Factor Authentication (MFA)	No fiscal impact.
7	Sections 7006.4.4.1 to 7006.4.4.5	NIST	Practice is to ensure passwords and access codes must remain confidential, never be shared, and follow strict security standards, with all reset requests and suspected compromises promptly reported and handled through secure IT channels.	Consider establishing Sections 7006.4.4.1 to 7006.4.4.5 Password Protection	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
8	Sections 7006.4.5.1 to 7006.4.5.2	NIST	User accounts will lock after three failed login attempts and remain inaccessible for 30 minutes or until IT verifies the user's identity and unlocks the account.	Consider establishing Sections 7006.4.5.1 to 7006.4.5.2 Account Lockout	No fiscal impact.
9	Sections 7006.4.6.1 to 7006.4.6.3	NIST	The District requires administrative accounts use unique, complex passwords, shared accounts require IT approval and monitoring, and vendors must comply with BCVWD's password policies, including MFA and complexity standards.	Consider establishing Sections 7006.4.6.1 to 7006.4.6.3 Special Considerations for System Accounts	No fiscal impact.
10	Sections 7006.4.7.1 to 7006.4.7.3	NIST and CCPA	The IT Department audits password compliance, log failed login attempts to detect security threats, and enforce disciplinary actions for non-compliance, including account suspension.	Consider establishing Sections 7006.4.7.1 to 7006.4.7.3 Monitoring and Enforcement	No fiscal impact.
11	Section 7006.4.8.1	NIST and CCPA	The District password practices comply with CCPA to protect sensitive data.	Consider Section 7006.4.8.1 California Compliance	No fiscal impact.
12	Sections 7006.4.9.1 to 7006.4.9.4	NIST and CCPA	At the District, passwords for water sector-specific systems must follow enhanced security standards, undergo annual penetration testing, and include customized policies for critical systems, with periodic changes for high-risk accounts based on IT risk assessments.	Consider establishing Sections 7006.4.9.1 to 7006.4.9.4 Water Sector Guidelines	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
13	Section 7006.4.10.1	NIST	In emergencies like disaster recovery, the IT Department may implement temporary password overrides, ensuring all actions are logged, monitored, documented, and reviewed post-incident to restore compliance.	Consider establishing Section 7006.4.10.1 Emergency Situations	No fiscal impact.
14	Section 7004.5	NIST	The District requires employees undergo regular training on secure password practices, covering strong password creation, phishing prevention, and credential protection as part of BCVWD's Security Awareness Program.	Consider establishing Section 7006.4.11 Awareness and Training	No fiscal impact as training is done through Vector Solutions.
15	Section 7006.5	NIST	BCVWD will annually review the Password Policy to ensure its effectiveness, compliance with regulations, alignment with NIST standards, and adaptability to emerging technologies, updating it as needed to support the District's mission and security goals.	Consider establishing Section 7006.5 Maintenance	No fiscal impact.

Fiscal Impact: None.

Attachments

1. Draft and Clean version of Policy 7006: Password
2. National Institute of Standards and Technology (NIST) Fact Sheet
3. California Consumer Privacy Act (CCPA) Summary and Key Issues

Staff Report prepared by Ren Berioso, Human Resources Manager

6c Attachment 1

Policy Title: Password Policy

Policy Number: 7006

7006.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) recognizes that strong password practices are essential for protecting access to its systems, networks, and sensitive data. This policy establishes password management requirements aligned with the National Institute of Standards and Technology (NIST) standards, ensuring secure access while minimizing risks associated with unauthorized access or data breaches. As a California Special District, BCVWD ensures compliance with applicable state regulations and cybersecurity best practices.

7006.2 Purpose. The purpose of this policy is to define requirements for the creation, management, and use of passwords to safeguard BCVWD's IT resources, ensuring alignment with NIST guidelines and compliance with California's privacy and cybersecurity laws.

7006.3 Scope. This policy applies to all employees, contractors, and third parties who access BCVWD's IT systems, applications, devices, voicemail systems, physical security systems (e.g., gate codes, alarm codes), or other password-protected resources.

7006.4 Policy Details

1.1 Password Creation and Complexity

- a Passwords must meet complexity requirements, including a mix of uppercase and lowercase letters, numbers, and special characters.
- b Passphrases, such as a sequence of random words, are encouraged for greater memorability and security
- c Default passwords provided with devices, systems, or applications must be changed upon first use.
- d Generic passwords or shared accounts should not be used unless explicitly authorized by the IT Department for a specific operational purpose. These accounts must have passwords that change periodically and be closely monitored.

2.1 Password Management

- a Employees must not reuse passwords across multiple accounts or use passwords previously used for BCVWD systems.
- b Password changes are only required when there is evidence of compromise or as directed by the IT Department.
- c Passwords must not be written down or stored in plain text. Employees are encouraged to use a District-approved password manager for secure storage.
- d Employees will receive automated email notifications whenever a password change is made to their account. If a user does not recognize the change, they must report it immediately to the IT Department.
- e The IT Department will periodically evaluate the effectiveness of password policies, including lifecycle requirements, based on evolving threat landscapes and best practices, ensuring passwords meet security needs without imposing unnecessary user burden.

3.1 Multi-Factor Authentication (MFA)

- a Multi-factor authentication (MFA) is required whenever possible for accessing BCVWD systems, email, and sensitive applications to enhance security.
- b Employees must promptly notify the IT Department if they lose access to their secondary authentication method (e.g., mobile device, hardware token).

- c Passwords for remote access tools, such as VPN or remote desktop applications, must meet
-

complexity requirements and be protected by multi-factor authentication (MFA) when possible, to ensure secure access from external networks.

4.1 Password Protection

- a Passwords must not be shared under any circumstances, including non-computer systems such as mobile devices, voicemail systems, gate codes, and alarm codes.
- b Any requests for passwords, regardless of the source, must be directed to the IT Department for verification and handling. Employees must report any suspected password compromises to the IT Department immediately.
- c Temporary or one-time passwords issued by the IT Department must be used only for their intended purpose and changed immediately upon first login.
- d Password reset requests must be submitted through secure channels, such as the IT helpdesk portal, and verified using identity confirmation methods (e.g., employee ID verification or multi-factor authentication).
- e Passwords and access codes for physical security systems (e.g., gate codes, alarm codes) must adhere to the same confidentiality and complexity standards as IT passwords. These codes must be updated periodically and immediately upon suspected compromise.

5.1 Account Lockout

- a User accounts will be locked after three (3) consecutive failed login attempts to prevent unauthorized access.
- b Locked accounts will remain inaccessible for 30 minutes or until unlocked by authorized IT personnel after verifying the user's identity.

6.1 Special Considerations for System Accounts

- a Administrative and system accounts must use unique, complex passwords that are different from user-level accounts.
- b Shared accounts (e.g., service accounts) must be approved by the IT Department, including enhanced logging and monitoring, and be limited to use cases where individual accounts are impractical. Each use of a shared account must be traceable to an individual user.
- c Vendors and contractors accessing BCVWD systems must adhere to the same password requirements, including complexity, change intervals, and MFA. Contractors requiring shared accounts must obtain written approval from the IT Department.

7.1 Monitoring and Enforcement

- a The IT Department will conduct periodic audits of password compliance and security practices.
- b Non-compliance with the Password Policy may result in disciplinary actions, including suspension of account access.
- c Failed login attempts will be logged and reviewed periodically by the IT Department to identify patterns of potential unauthorized access or brute-force attack attempts.

8.1 California Compliance

- a BCVWD's password practices comply with the California Consumer Privacy Act (CCPA) and other applicable state cybersecurity regulations to ensure data protection.

9.1 Water Sector Guidelines

- a Passwords used to access water sector-specific systems (e.g., SCADA or water quality monitoring systems) must adhere to enhanced security requirements as directed by NIST and industry best practices.
- b Periodic penetration testing will be conducted at least annually to evaluate the strength of

- password controls, identify vulnerabilities, and address risks to both IT and operational technology systems.
- c Critical systems such as SCADA must use customized password policies that address their unique security and operational requirements.
- d High-risk accounts, such as administrative or SCADA accounts, may require periodic password changes based on risk assessments conducted by the IT Department.

10.1 **Emergency Situations**

- a In emergency scenarios, such as disaster recovery or major system failures, the IT Department may implement temporary password overrides or bypass measures. These measures must be logged, monitored, and documented, with a full review conducted post-incident to ensure compliance is restored.

11.1 **Awareness and Training**

- a Employees will receive periodic training on secure password practices as part of BCVWD's Security Awareness and Training Program. Topics include creating strong passwords, avoiding phishing attempts, and protecting credentials.

7006.5 Review and Revision Policy. The Information Technology Department will review the "Acceptable Use Policy" annually to ensure it remains current and effective in addressing the needs of the organization and any changes in regulatory or technological requirements. During the review process, the policy will be evaluated for its effectiveness, compliance with relevant regulations, alignment with the National Institute of Standards and Technology (NIST), and adherence to applicable local and state laws governing IT resource usage. Necessary updates or revisions will be made to ensure the policy continues to meet the district's requirements and supports its mission

Understanding

THE NIST CYBERSECURITY FRAMEWORK

You may have heard about the NIST Cybersecurity Framework, but what exactly is it?

And does it apply to you?

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps

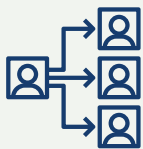
businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

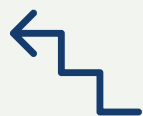
1. IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:



Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.



Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

LEARN MORE AT:
[FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness)



FEDERAL TRADE COMMISSION

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Homeland Security

3. DETECT



Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.



Check your network for unauthorized users or connections.



Investigate any unusual activities on your network or by your staff.

4. RESPOND

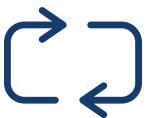
Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly.

5. RECOVER

After an attack:



Repair and restore the equipment and parts of your network that were affected.



Keep employees and customers informed of your response and recovery activities.

For more information on the NIST Cybersecurity Framework and resources for small businesses, go to [NIST.gov/CyberFramework](https://www.nist.gov/CyberFramework) and [NIST.gov/Programs-Projects/Small-Business-Corner-SBC](https://www.nist.gov/Programs-Projects/Small-Business-Corner-SBC).

LEARN MORE AT:



FEDERAL TRADE COMMISSION

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Homeland Security

06c Attachment 3

CCPA Summary and Key Issues
Consent
Enforcement
Financial Incentives
Jurisdictional Thresholds
Information Security
Marketing and Advertising
Notices to Consumers

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

Accept

Deny

Requests for Deletion
Service Providers
Sales of Minors' Information
Sales to Third Parties
Verification of Requestors

[View CCPA Act](#)

CCPA Summary and Key Issues

The California Consumer Privacy Act of 2018 ("CCPA" or "the Act") became effective on January 1, 2020, and is codified at §§1798.100–199 of the Civil Code. The Act offers new and wide-ranging privacy rights for California residents, including a right to be informed about personal data collected by a business and rights to access and delete that information, a right to prevent personal information from being sold to third parties, and a right to data portability. The law

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

Information that nominally falls under one or more of the categories of “personal information” cited in §140(o)(A)–(K) is only personal information if it “identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household”

The consumer private right of action only applies to violations of §150(a), which addresses security procedures and practices

The Act does not apply if it is conflict to with the U.S. Constitution

Substantive changes include:

Allowing a business to disclose the consumer’s right to deletion of his/her personal information in a form that is “reasonably accessible to consumers”; previously, the Act required such information to be listed on a business’s website or in its privacy policy

Exempting personal information collected under the California Financial Information Privacy Act; this is in addition to personal information subject to the Gramm–Leach–Bliley Act, which was already exempt under the CCPA

Exempting health care providers and covered entities “to the extent the provider or covered entity maintains patient information in the same manner as medical

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

A.B. 1202. Data brokers. Data brokers must now register with the California Attorney General's office.

A.B. 25. CCPA amendment. One-year exemption for "employee" data.

A.B. 874. CCPA amendment. Adds "reasonably" to the definition of "personal information."

A.B. 1355. CCPA amendment. One-year exemption for "business-to-business" data; numerous drafting errors corrected.

A.B. 1146. CCPA amendment. Exemption for certain information related to motor vehicle repairs and recalls.

A.B. 1130. Breach notification. Adds new types of personal data subject to the state breach notification statute.

Go to an [unofficial version of the Act](#) that incorporates all previous amendments.



This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)



**Beaumont-Cherry Valley Water District
Personnel Committee
January 21, 2025**

Item 6d

STAFF REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: Policies and Procedures Manual Updates/Revisions establishing Information Technology Policy Number 7011 Cellular Telephone Usage

Staff Recommendation

Approve the establishment of Information Technology (IT) Policy Number 7011 Cellular Telephone Usage to move forward to the next Board of Directors meeting, or direct staff as desired.

Executive Summary

Staff is proposing the establishment of IT Policy Number 7011 Cellular Telephone Usage with sections that establish clear guidelines for the secure and responsible use of District-issued and personal devices for work-related activities. By aligning with National Institute of Standards and Technology (NIST) standards, California laws, and water sector regulations, the policy safeguards sensitive data, ensures compliance, and supports operational efficiency while minimizing risks such as data breaches and misuse.

Background

At the November 19, 2024 meeting, the Director of IT requested the Personnel Committee to review the Employee IT policy handbook to ensure they align with the district's strategic goals, legal requirements, and regulatory standards. This oversight fosters accountability, transparency, and overall guidance to personnel, reinforcing the District's commitment to effective IT governance and cybersecurity. With Human Resources (HR) as the custodian of the District's Policy Manual, HR staff partnered with the Director of IT in the review of the IT policy handbook.

The Employee IT policy handbook is crucial for outlining policies, procedures, and expectations related to technology use, ensuring security compliance, and protecting both employees and the organization. The history of the Employee IT Policy Handbook and the IT and Cybersecurity Policy Manual reflects Beaumont-Cherry Valley Water District's (BCVWD) commitment to fostering a secure, compliant, and informed technology environment.

First drafted in 2014, the Employee IT Policies Handbook is updated annually by the IT Department to align with evolving technology standards and is provided to all employees during new hire orientation to ensure consistent understanding of IT policies. Similarly, the IT and Cybersecurity Policy Manual, created in 2017, establishes administrative policies that align with the NIST framework and is updated annually to maintain compliance with laws, regulations, and industry best practices. Both documents underwent extensive review in their most recent updates, further strengthening their relevance and effectiveness. These efforts contributed to the district earning the prestigious Municipal Information Systems Association of California (MISAC) award



for the last two (2) years, demonstrating leadership and excellence in IT governance and cybersecurity management.

As part of the ongoing review process of all District policies, HR staff, in partnership with IT Department presented the proposed policy draft to Legal Counsel to ensure compliance with applicable Federal, State and local labor laws.

Discussion

The Cellular Telephone Usage policy is crucial for ensuring the secure, compliant, and efficient use of cellular devices in conducting District business while protecting sensitive data and adhering to regulatory standards. Table A, Summary of Policy Sections, outlines the proposed Cellular Telephone Usage (policy) that was drafted by HR and IT Departments.

Table A – Summary of Policy Sections

TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	Section 7011.1	NIST	Cellular Telephone Usage policy ensures the secure and compliant use of cellular phones for District business, protecting sensitive data and maintaining operational integrity.	Consider establishing Section 7011.1 Introduction	No fiscal impact.
2	Section 7011.2	NIST	This policy defines the proper use, security requirements, and responsibilities for cellular telephones in District activities, aiming to prevent risks and ensure compliance with cybersecurity and legal standards.	Consider establishing Section 7011.2 Purpose	No fiscal impact.
3	Section 7011.3	NIST	The Password policy has been applicable to all employees using District-issued or personal cellular phones for work, including accessing District systems, data, or communications.	Consider establishing Section 7011.3 Scope.	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
4	Sections 7011.4.1.1 to 7011.4.1.3	NIST	The District requires that District-issued phones are for work purposes with limited personal use, personal phones require IT authorization for District activities, and all usage must follow professional standards and District policies.	Consider establishing Sections 7011.4.1.1 to 7011.4.1.3 General Use	No fiscal impact.
5	Sections 7011.4.2.1 to 7011.4.2.6	NIST	All District-issued and authorized personal phones meet NIST security standards, including encryption and strong authentication, while being enrolled in the Mobile Device Management program, with immediate reporting of lost devices and secure decommissioning processes.	Consider establishing Sections 7011.4.2.1 to 7011.4.2.6 Security Requirements	No fiscal impact.
6	Sections 7011.4.3.1 to 7011.4.3.4	NIST	The District requires sensitive District data only be stored or accessed on authorized and encrypted devices using District-approved applications, with all data on District-issued phones considered BCVWD property and subject to privacy laws.	Consider establishing Sections 7011.4.3.1 to 7011.4.3.4 Data Ownership and Protection	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
7	Sections 7011.4.4.1 to 7011.4.4.2	NIST and CA Vehicle Code § 23124	District-issued phones must not be used for unauthorized apps, non-work files, or policy-violating activities, and hands-free devices are required for phone use while driving on District business.	Consider establishing Sections 7011.4.4.1 to 7011.4.4.2 Prohibited Activities	No fiscal impact.
8	Sections 7011.4.5.1 to 7011.4.5.3	NIST and CPRA	BCVWD may monitor District-issued phones for compliance, with personal communications subject to CPRA disclosure, and tracking enabled for security and recovery purposes in line with privacy laws.	Consider establishing Sections 7011.4.5.1 to 7011.4.5.3 Monitoring and Privacy	No fiscal impact.
9	Sections 7011.4.6.1 to 7011.4.6.4	NIST	The District requires employees to safeguard District-issued phones, report security incidents promptly, maintain devices responsibly, and avoid tampering, while supervisors ensure compliance with the policy.	Consider establishing Sections 7011.4.6.1 to 7011.4.6.4 Responsibilities	No fiscal impact.
10	Sections 7011.4.7.1 to 7011.4.7.2	NIST, CPRA and CCPA	At the District, Cellular phone use comply with California laws, including the CCPA and CPRA, with District-related communications subject to CPRA disclosure.	Consider establishing Sections 7011.4.7.1 to 7011.4.7.2 California Compliance	No fiscal impact.



TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
11	Section 7006.4.8.1	NIST and CCPA	The District password practices comply with CCPA to protect sensitive data.	Consider establishing Section 7006.4.8.1 California Compliance	No fiscal impact.
15	Section 7006.5	NIST	BCVWD will annually review the Cellular Telephone Usage Policy to ensure its effectiveness, compliance with regulations, alignment with NIST standards, and adaptability to emerging technologies, updating it as needed to support the District's mission and security goals.	Consider establishing Section 7006.5 Maintenance	No fiscal impact.

Fiscal Impact

There is no fiscal impact in the establishment of this policy.

Attachments

1. Draft and Clean version of Policy 7011: Cellular Telephone Usage
2. National Institute of Standards and Technology (NIST) Fact Sheet
3. California Public Records Act (CPRA) FAQ
4. California Consumer Privacy Act (CCPA) Summary and Key Issues
5. California Vehicle Code § 23124 Summary

Staff Report prepared by Ren Berioso, Human Resources Manager

6d Attachment 1

Policy Title: Cellular Telephone Usage

Policy Number: 7011

7011.1 Introduction . Beaumont-Cherry Valley Water District (BCVWD) recognizes the importance of cellular telephones for conducting District business efficiently and securely. This policy establishes guidelines for the proper use and management of District-issued and personal cellular telephones to ensure compliance with National Institute of Standards and Technology (NIST) principles, California laws, and water sector regulations. By implementing these standards, BCVWD ensures the protection of sensitive data and operational integrity.

7011.2 Purpose. The purpose of this policy is to define the appropriate use, security requirements, and responsibilities related to cellular telephones used for District-related activities. The policy aims to minimize risks such as data breaches, unauthorized access, and misuse, while ensuring compliance with NIST cybersecurity standards, California laws, and public records regulations.

7011.3 Scope. This policy applies to all employees, contractors, and third parties who use District-issued or personal cellular telephones for work-related purposes, including access to District systems, data, or communications.

7011.4 Policy Details

1.1 General Use

- a District-issued cellular telephones are provided exclusively for work-related purposes. Personal use must be limited to incidental activities that do not interfere with work responsibilities or result in excessive costs to the district.
- b Personal cellular telephones must not be used for District-related activities unless explicitly authorized under the Bring Your Own Device (BYOD) Policy and approved by the Information Technology Department.
- c Cellular telephone usage must adhere to professional and ethical standards and comply with all applicable District policies, including the Acceptable Use Policy.

2.1 Security Requirements

- a District-issued cellular telephones must be configured to meet NIST security guidelines, including:
 - Full Device Encryption
 - Strong Authentication
 - Automatic Lockout after a maximum of 5 minutes of inactivity
 - b Employees must report lost, stolen, or compromised District-issued cellular telephones to the IT Department immediately. The IT Department will remotely lock or wipe the device to prevent unauthorized access.
 - c Personal cellular telephones authorized for District use must comply with security requirements outlined in the BYOD Policy and Mobile Device Management Policy, including encryption and password protection.
 - d Cellular telephones used to access District systems must be enrolled in the District's Mobile Device Management (MDM) program for enhanced monitoring and compliance.
 - e District-issued cellular telephones must maintain a separation between personal and work-related data through containerization or similar security methods, as specified by NIST guidelines.
 - f When a District-issued cellular telephone is decommissioned, it must be returned to the IT Department for secure wiping and reconfiguration to ensure no residual data remains on the device.
-

3.1 Data Ownership and Protection

- a Employees must not store sensitive District data, including personally identifiable information (PII), on personal cellular telephones unless explicitly authorized and encrypted.
- b Communications and data transmitted via cellular telephones are subject to applicable privacy laws, including the California Consumer Privacy Act (CCPA) and California Public Records Act (CPRA).
- c Employees must use District-approved applications to access email, documents, or other sensitive data on cellular telephones.
- d All data stored on District-issued cellular telephones, including work-related emails, documents, and communications, is the property of BCVWD. Employees must not delete, transfer, or share District data without prior authorization.

4.1 Prohibited Activities

- a District-issued cellular telephones must not be used for:
 - Downloading unauthorized applications or software.
 - Storing non-work-related files, media, or software.
 - Engaging in activities that violate District policies or local, state, or federal laws.
- b Using cellular telephones while driving on District business is prohibited unless using a hands-free device, in compliance with California Vehicle Code Section 23123.5.

5.1 Monitoring and Privacy

- a BCVWD reserves the right to monitor District-issued cellular telephones for compliance with this policy. Monitoring includes, but is not limited to, call logs, data usage, and installed applications. Monitoring will be conducted in accordance with applicable state and federal laws.
- b Personal communications made on District-issued cellular telephones are not private and may be subject to disclosure of public records under the CPRA.
- c District-issued cellular telephones are equipped with tracking capabilities for loss or theft prevention. Employees are required to consent to these measures as a condition of using District-issued devices. Tracking will be used solely for security and recovery purposes and will comply with applicable privacy laws.

6.1 Responsibilities

- a Employees are responsible for safeguarding District-issued cellular telephones from loss, theft, or damage.
- b Employees must immediately report any suspected or actual security incidents involving District-issued cellular telephones to the IT Department.
- c Supervisors/Department Heads must ensure employees using District-issued cellular telephones understand and comply with this policy.
- d Employees must take reasonable care of District-issued cellular telephones, ensuring the device is clean, not physically damaged, and free from unauthorized alterations or misuse. Employees are prohibited from jailbreaking, rooting, or otherwise tampering with device software or hardware, or removing protective equipment designed to protect the device from damage.

7.1 California Compliance

- a Cellular telephone use must comply with applicable California laws, including the California Consumer Privacy Act (CCPA), the California Public Records Act (CPRA), and state laws governing electronic communications.
- b Text messages and other communications related to District business are subject to disclosure under the CPRA.

7011.5 **Review and Revision Policy.** The Information Technology Department will review the "Acceptable Use Policy" annually to ensure it remains current and effective in addressing the needs of the organization and any changes in regulatory or technological requirements. During the review process, the policy will be evaluated for its effectiveness, compliance with relevant regulations, alignment with the National Institute of Standards and Technology (NIST), and adherence to applicable local and state laws governing IT resource usage. Necessary updates or revisions will be made to ensure the policy continues to meet the district's requirements and supports its mission.

DRAFT

Understanding

THE NIST CYBERSECURITY FRAMEWORK

You may have heard about the NIST Cybersecurity Framework, but what exactly is it?

And does it apply to you?

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps

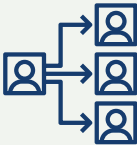
businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

1. IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:



Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.



Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

LEARN MORE AT:
[FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness)



3. DETECT



Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.



Check your network for unauthorized users or connections.



Investigate any unusual activities on your network or by your staff.

4. RESPOND

Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly.

5. RECOVER

After an attack:



Repair and restore the equipment and parts of your network that were affected.



Keep employees and customers informed of your response and recovery activities.

For more information on the NIST Cybersecurity Framework and resources for small businesses, go to NIST.gov/CyberFramework and NIST.gov/Programs-Projects/Small-Business-Corner-SBC.

LEARN MORE AT:



FEDERAL TRADE COMMISSION

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Homeland Security

6d Attachment 3

California Public Records Act FAQs

1. What is the California Public Records Act (CPRA)?

The California Public Records Act (CPRA) was passed by the California Legislature in 1968 for government agencies and requires that government records be disclosed to the public, upon request, unless there are privacy and/or public safety exemptions which would prevent doing so. Please see the California Attorney General's Office [Summary of the California Public Records Act](#) [🔗](#) (pdf) for additional information.

2. What is a Public Record?

[Government Code §7920.530](#) [🔗](#) defines a public record as "any writing containing information relating to the conduct of the public's business prepared, owned, used or retained by any state or local agency regardless of physical form or characteristics." The California Commission on Peace Officer Standards and Training (POST) respects the public's right to access records created and maintained by POST in the course of normal business.

Please ensure that you narrow your request to that which reasonably identifies the desired records that POST may have in its possession in order for staff to more efficiently search for and promptly provide responsive documents. Additionally, please ensure the records you are requesting are under POST's purview and what POST oversees as a state agency. For example, POST has no records related to 911 transcripts, accident/incident reports, warrants, county arrest records, and the like, unless they might be included in an officer's serious misconduct investigation.

The CPRA does not require creation/preparation of a record or document that does not exist at the time of the request. Additionally, certain categories of personal information and records are exempt from disclosure under the CPRA. Other laws also protect individual privacy interests and other propriety information from disclosure.

3. Information to include with your request

Pursuant to [Government Code §7922.600](#), in order to make a focused and effective request for POST records, please include the following applicable information to ensure the scope of the request is narrow and clear enough for personnel to determine if POST has the records you are requesting:

- The subject of the record
- A clear, concise, and specific description of the record(s) being requested
- The date(s) of the record(s), or a time period for your request (e.g.: calendar year 2020)
- Full names for the individuals and/or agencies included in your request, including proper spelling
- POST ID(s) for the individual(s) included in your request if applicable, and/or current/former agency
- Any additional information that helps staff identify the record(s) being requested
- Your contact information for response to your request, preferably an email address

Please make every effort to research the POST records you are requesting, prior to submitting your request. A vast amount of information, resources, and records are already available on the [POST Website](#), by utilizing the search tool, or browsing the topics related to your request. Common questions for information might be found using the following resources:

- [SB978 and Presenter Course Content](#) 
- [SB978 Multimedia Products and Training Videos](#)
- [Certificates](#)
- [Basic Course Training Specifications](#) (by Learning Domain)
- [Basic Course Student Workbooks](#) (by Learning Domain)
- [POST Learning Portal questions](#) 
- [POST Commission Regulations, Procedures, and Authority](#)
- [Investigation Records Pertaining to Officer Misconduct/Decertification](#)  (Government Code section 7923.601)
- [POST Participating Agencies](#)

4. How to make a Public Records Act Request


[Submit Your Own Online Request for POST Records](#) 

(select "Submit Records Request")

Mail:

Attention: California Public Records Act Request
California Commission on Peace Officer Standards and
Training (POST)
860 Stillwater Road, Suite 100
West Sacramento, CA 95605-1630

For questions, email: CPRA@post.ca.gov

Please note: The 10-day period mentioned in the [Government Code §7922.535](#)  is not a deadline for producing records. Should the request be voluminous, or require research, or computer programming, POST may need a reasonable amount of time to research, review, and inspect records prior to release; therefore, it may take longer before the records can be made available. Upon receipt of your request, POST

6d Attachment 4

CCPA Summary and Key Issues
Consent
Enforcement
Financial Incentives
Jurisdictional Thresholds
Information Security
Marketing and Advertising
Notices to Consumers

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

Accept

Deny

Requests for Deletion
Service Providers
Sales of Minors' Information
Sales to Third Parties
Verification of Requestors

[View CCPA Act](#)

CCPA Summary and Key Issues

The California Consumer Privacy Act of 2018 ("CCPA" or "the Act") became effective on January 1, 2020, and is codified at §§1798.100–199 of the Civil Code. The Act offers new and wide-ranging privacy rights for California residents, including a right to be informed about personal data collected by a business and rights to access and delete that information, a right to prevent personal information from being sold to third parties, and a right to data portability. The law

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

Information that nominally falls under one or more of the categories of “personal information” cited in §140(o)(A)–(K) is only personal information if it “identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household”

The consumer private right of action only applies to violations of §150(a), which addresses security procedures and practices

The Act does not apply if it is conflict to with the U.S. Constitution

Substantive changes include:

Allowing a business to disclose the consumer’s right to deletion of his/her personal information in a form that is “reasonably accessible to consumers”; previously, the Act required such information to be listed on a business’s website or in its privacy policy

Exempting personal information collected under the California Financial Information Privacy Act; this is in addition to personal information subject to the Gramm–Leach–Bliley Act, which was already exempt under the CCPA

Exempting health care providers and covered entities “to the extent the provider or covered entity maintains patient information in the same manner as medical

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

A.B. 1202. Data brokers. Data brokers must now register with the California Attorney General's office.

A.B. 25. CCPA amendment. One-year exemption for "employee" data.

A.B. 874. CCPA amendment. Adds "reasonably" to the definition of "personal information."

A.B. 1355. CCPA amendment. One-year exemption for "business-to-business" data; numerous drafting errors corrected.

A.B. 1146. CCPA amendment. Exemption for certain information related to motor vehicle repairs and recalls.

A.B. 1130. Breach notification. Adds new types of personal data subject to the state breach notification statute.

Go to an [unofficial version of the Act](#) that incorporates all previous amendments.



This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. [Privacy Policy](#)

**6d Attachment 5**[Go to Previous Versions of this Section](#) ▾

2023 California Code

Vehicle Code - VEH

DIVISION 11 - RULES OF THE ROAD

CHAPTER 12 - Public Offenses

ARTICLE 1 - Driving Offenses

Section 23124.

Universal Citation:

CA Veh Code § 23124 (2023) ○

[◀ Previous](#)[Next ▶](#)

23124. (a) This section applies to a person under the age of 18 years.

(b) Notwithstanding Sections 23123 and 23123.5, a person described in subdivision (a) shall not drive a motor vehicle while using a wireless telephone or an electronic wireless communications device, even if equipped with a hands-free device.

(c) A violation of this section is an infraction punishable by a base fine of twenty dollars (\$20) for a first offense and fifty dollars (\$50) for each subsequent offense.

(d) A law enforcement officer shall not stop a vehicle for the sole purpose of determining whether the driver is violating subdivision (b).

(e) Subdivision (d) does not prohibit a law enforcement officer from stopping a vehicle for a violation of Section 23123 or 23123.5.

(f) This section does not apply to a person using a wireless telephone or a mobile service device for emergency purposes, including, but not limited to, an emergency call to a law enforcement agency, health care provider, fire department, or other emergency services agency or entity.

(g) For the purposes of this section, “electronic wireless communications device” includes, but is not limited to, a broadband personal communication device, specialized mobile radio device, handheld device or laptop computer with mobile data access, pager, and two-way messaging device.

(Amended by Stats. 2013, Ch. 754, Sec. 1. (SB 194) Effective January 1, 2014.)

◀ Previous

Next ▶

Disclaimer: These codes may not be the most recent version. California may have more current or accurate information. We make no warranties or guarantees about the accuracy, completeness, or adequacy of the information contained on this site or the information linked to on the state site. Please check official sources.

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.



**Beaumont-Cherry Valley Water District
Personnel Committee Meeting
January 21, 2025**

Item 7

STAFF REPORT

TO: Personnel Committee
FROM: Ren Berioso, Human Resources Manager
SUBJECT: Policy Tracking Matrix Progress Dashboard

Staff Recommendation

Approve the policies pending review in the next one to two months identified on Table 3, Policy to Work on for Subsequent Meetings, or to direct staff as desired.

Background

At the October 17, 2023 meeting, staff was directed by the Personnel Committee to create a dashboard to outline the progress of the Policies and Procedures Manual updates since year 2021. At the November 21, 2023 meeting, the Personnel Committee approved a dashboard presented by staff which highlights the summary of all policies approved and drafted, and those policies that staff are working on for subsequent meetings.

Discussion:

Table 1-Summary of Policy Approval Tracking (All Policies)

Department	On Matrix	Draft Created	Committee / Board Reviewed Drafts	Board Approved	% Complete
Board Administration ¹	26	23	1	0	0.00%
Engineering ²	8	8	1	1	12.50%
Finance	15	15	8	5	33.33%
Human Resources	70	70	68	68	97.14%
Information Technology ³	17	17	0	0	0.00%
TOTALS	136	132	78	74	54.41%

Table 2 – Recommended Policies to be added to the Policy Matrix

Item	Policy Subject	Policy Contents
None		

¹ Previously titled “Administration” but added clarifier that is specific to the Board of Directors.

² Includes four (4) policies identified previously as “Operations”

³ 15 Policies were identified by IT to go to the Personnel Committee.



Table 3 – Policies To Work on for Subsequent Meetings

Item	Policy No.	Priorities Listed	Draft Size	Selected for Processing	Estimated Committee Presentation
1	3111	Leave For Crime Victims	4 pages	January	February
2	7001	Acceptable Use (policy)	1 page	January	February
3	7002	Bring Your Own Device	1 page	January	February
4	7015	Security Awareness Training	2 pages	January	February

Numbered for ease of selection and reference, not for level of priority.

Fiscal Impact

There is no financial impact.

Attachments

1. Policy Approval Tracking Matrix

Staff Report prepared by Ren Berioso, Human Resources Manager

**Policy Approval Tracking
BCVWD Policy Manual Project**

Policy Number	New Policy Number	Section	Policy Name	HR's Recommendation Responsible Department	Drafted by BCVWD Staff	Approved by Legal Counsel	Presented to Committee	Provisionally Approved by Committee	Presented to Board of Directors	Approved by Board of Directors	Adoption Date	Resolution Number
2	1005	General	Contractual Provisions	Human Resources	Additional Edits	6/28/2021	7/19/2021	7/22/2021	4/14/2021	10/13/2021	10/13/2021	21-018
3	1010	General	Policy Manual	Human Resources	Additional Edits	3/15/2021	N/A	N/A	1/8/2025	4/14/2021	4/14/2021	21-006
5	2010	Administration	Equal Opportunity	Human Resources	Yes	3/15/2021	3/22/2021	3/22/2021	4/14/2021	4/14/2021	4/14/2021	21-006
6	2015	Administration	Access to Personnel Records	Human Resources	Yes	3/15/2021	3/22/2021	3/22/2021	4/14/2021	4/14/2021	4/14/2021	24-006
7	2020	Administration	Harassment	Human Resources	Yes	3/15/2021	3/22/2021	3/22/2021	4/14/2021	4/14/2021	4/14/2021	24-006
N/A	2025	Administration	Sexual Harassment	Human Resources	Yes	3/15/2021	3/22/2021	3/22/2021	4/14/2021	4/14/2021	4/14/2021	21-006
8	3000	Personnel	Whistleblower Protection	Human Resources	Yes	4/12/2021	7/19/2021	7/26/2021	10/13/2021	10/13/2021	10/13/2021	21-018
N/A	3001	Personnel	Employee Status	Human Resources	Yes	4/12/2021	6/1/2021	6/21/2021	10/13/2021	10/13/2021	10/13/2021	21-018
N/A	3002	Personnel	Employee Information and Emergency	Human Resources	Yes	4/12/2021	7/19/2021	7/20/2021	10/13/2021	10/13/2021	10/13/2021	21-018
9	3005	Personnel	Employee Groups	Human Resources	Yes	7/13/2021	9/20/2021	9/20/2021	10/13/2021	10/13/2021	10/13/2021	21-018
N/A	3006	Personnel	Compensation	Human Resources	Yes	7/13/2021	9/20/2021	9/20/2021	10/13/2021	10/13/2021	10/13/2021	21-018
10 & 49	3010	Personnel	Performance Evaluation	Human Resources	Yes	8/3/2021	9/20/2021	9/20/2021	10/13/2021	10/13/2021	10/13/2021	21-018
11	3015	Personnel	Performance Evaluation-General	Human Resources	Yes	8/3/2021	9/20/2021	9/20/2021	10/13/2021	10/13/2021	10/13/2021	21-018
12	3020	Personnel	Health and Welfare Benefits	Human Resources	Yes	5/10/2022	5/17/2022	5/17/2022	6/8/2022	6/8/2022	6/8/2022	22-019
13	3025	Personnel	Pay Periods	Human Resources	Yes	10/12/2021	11/15/2021	11/15/2021	5/11/2022	5/11/2022	5/11/2022	22-016
14	3030	Personnel	Gift Acceptance Guidelines	Human Resources	Yes	10/12/2021	4/19/2022	4/19/2022	5/11/2022	5/11/2022	5/11/2022	22-016
15	3035	Personnel	Outside Employment	Human Resources	Yes	10/12/2021	4/19/2022	4/19/2022	5/11/2022	5/11/2022	5/11/2022	22-016
16	3040	Personnel	Letters of Recommendation	Human Resources	Yes	6/28/2024	7/16/2024	7/16/2024	8/14/2024	8/14/2024	8/14/2024	24-012
17	3045	Personnel	Executive Officer	Human Resources	Yes	7/29/2024	8/20/2024	8/20/2024	8/14/2024	8/14/2024	8/14/2024	24-012
18	3050	Personnel	Volunteer Personnel Workers'	Human Resources	Yes	5/2/2024	6/18/2024	6/18/2024	8/14/2024	8/14/2024	8/14/2024	24-012
19	3055	Personnel	Work Hours, Overtime, and Standby	Human Resources	Yes	6/14/2024	7/19/2024	7/19/2024	9/14/2024	9/14/2024	9/14/2024	22-038
20 (incorrect)	3060	Personnel	Continuity of Service	Human Resources	Yes	4/8/2024	4/16/2024	4/16/2024	5/16/2024	5/16/2024	5/16/2024	24-007
21	3070	Personnel	Reduction in Force	Human Resources	Yes	5/2/2024	6/18/2024	6/18/2024	7/10/2024	7/10/2024	7/10/2024	24-010
22	3075	Personnel	Holidays	Human Resources	Yes	1/16/2024	1/16/2024	1/16/2024	2/14/2024	2/14/2024	2/14/2024	24-002
24	3085	Personnel	Vacation	Human Resources	Yes	1/18/2022	1/17/2023	1/17/2023	2/8/2023	2/8/2023	2/8/2023	25-005
25	3090	Personnel	Sick Leave	Human Resources	Yes	1/18/2022	1/17/2023	1/17/2023	2/8/2023	2/8/2023	2/8/2023	25-007
26	3095	Personnel	Family and Medical Leave	Human Resources	Yes	10/2/2024	11/21/2024	11/21/2024	12/14/2024	12/14/2024	12/14/2024	22-043
N/A	3096	Personnel	Pregnancy Disability Leave	Human Resources	Yes	9/1/2022	9/20/2022	9/20/2022	12/14/2022	12/14/2022	12/14/2022	22-043
N/A	3100	Personnel	Lactation Accommodation	Human Resources	Yes	8/25/2022	9/20/2022	9/20/2022	12/14/2022	12/14/2022	12/14/2022	22-043
27	3105	Personnel	Bereavement Leave	Human Resources	Yes	5/17/2022	5/17/2022	5/17/2022	6/8/2022	6/8/2022	6/8/2022	22-019
28	3105	Personnel	Personal Leave of Absence	Human Resources	Yes	6/28/2024	7/16/2024	7/16/2024	8/14/2024	8/14/2024	8/14/2024	24-012
29	3110	Personnel	Jury and Witness Duty	Human Resources	Yes	10/5/2023	10/17/2023	11/21/2023	12/13/2023	12/13/2023	1/10/2024	23-031
N/A	3111	Personnel	Leave for Crime Victims and Family	Human Resources	Yes	12/6/2024	1/17/2025	1/17/2025	2/8/2025	2/8/2025	2/8/2025	25-005
30	3115	Personnel	Return to Work Policy	Human Resources	Yes	1/11/2023	1/17/2023	1/17/2023	2/8/2023	2/8/2023	2/8/2023	25-005
31	3120	Personnel	Occupational Injury and Illness	Human Resources	Yes	1/11/2023	1/17/2023	1/17/2023	2/8/2023	2/8/2023	2/8/2023	25-005
N/A	3121	Personnel	Infectious Disease Control	Human Resources	Yes	2/2/2023	2/21/2023	2/21/2023	3/15/2023	3/15/2023	3/15/2023	25-009
N/A	3122	Personnel	Workplace Violence	Human Resources	Yes	2/2/2024	1/16/2024	1/16/2024	2/14/2024	2/14/2024	2/14/2024	24-002
32	3125	Personnel	Uniforms and Protective Clothing	Human Resources	Yes	3/14/2023	3/21/2023	4/18/2023	5/10/2023	5/10/2023	5/10/2023	23-013
33	3130	Personnel	Employee Training, Education and Occupational Certification and Succession and Workforce Planning	Human Resources	Yes	6/29/2024	8/20/2024	8/20/2024	9/17/2024	9/17/2024	9/17/2024	24-014
34	3135	Personnel	Occupational Certification and Succession and Workforce Planning	Human Resources	Yes	6/14/2022	8/16/2022	8/16/2022	9/17/2022	9/17/2022	9/17/2022	22-028
N/A	3136	Personnel	Respiratory Protection Program	Human Resources	Yes	9/10/2024	9/18/2024	9/18/2024	10/9/2024	10/9/2024	10/9/2024	24-018
35	3140	Personnel	Respiratory Protection Program	Human Resources	Yes	6/29/2024	7/16/2024	7/16/2024	8/14/2024	8/14/2024	8/14/2024	24-012
36	3145	Personnel	Driver Training and Record Review	Human Resources	Yes	10/2/2024	3/21/2025	3/21/2025	4/12/2025	4/12/2025	4/12/2025	23-010
37	3150	Personnel	District Vehicle Usage	Human Resources	Yes	2/5/2024	3/19/2024	4/16/2024	5/16/2024	5/16/2024	5/16/2024	24-007
38	3151	Personnel	Personal Vehicle Usage	Human Resources	Yes	2/5/2024	3/19/2024	3/19/2024	4/10/2024	4/10/2024	4/10/2024	24-006
39	3160	Personnel	HIPAA Compliance and Security Officer	Human Resources	Yes	5/2/2024	6/18/2024	6/18/2024	7/10/2024	7/10/2024	7/10/2024	24-010
41	3170	Personnel	Smoke Free Workplace and Tobacco	Human Resources	Yes	2/5/2024	3/19/2024	3/19/2024	4/10/2024	4/10/2024	4/10/2024	24-006
42	3175	Personnel	Disciplinary Action or Terminations	Human Resources	Yes	6/29/2024	7/16/2024	8/20/2024	9/17/2024	9/17/2024	9/17/2024	24-014
Proposed	3176	Personnel	Transfers and Voluntary Demotion	Human Resources	Yes	9/10/2024	9/18/2024	9/18/2024	10/9/2024	10/9/2024	10/9/2024	24-018
43	3180	Personnel	Neopison-Employment of Relatives	Human Resources	Yes	4/8/2024	4/16/2024	6/18/2024	7/10/2024	7/10/2024	7/10/2024	24-010
44	3185	Personnel	Employee Separation	Human Resources	Yes	5/2/2024	6/18/2024	6/18/2024	7/10/2024	7/10/2024	7/10/2024	24-010
47	3200	Personnel	Grievance Procedures	Human Resources	Yes	5/2/2024	6/18/2024	6/18/2024	7/10/2024	7/10/2024	7/10/2024	24-010
48	3205	Personnel	Substance Abuse	Human Resources	Yes	12/6/2021	4/19/2022	4/19/2022	5/11/2022	5/11/2022	5/11/2022	22-016
N/A	3206	Personnel	FMCSA Clearinghouse Registration	Human Resources	No	12/6/2021	4/19/2022	4/19/2022	5/11/2022	5/11/2022	5/11/2022	22-016

Priority Legend:
Yellow Highlight = Highest Priority
Light Blue Highlight = Lowest Priority

**Policy Approval Tracking
BCVWD Policy Manual Project**

Policy Number	New Policy Number	Section	Policy Name	HR's Recommendation Responsible Department	Drafted by BCVWD Staff	Approved by Legal Counsel	Presented to Committee	Provisionally Approved by Committee	Presented to Board of Directors	Approved by Board of Directors	Adoption Date	Resolution Number
50	3215	Personnel	Personnel Action Form (PAF)	Human Resources	Yes	4/8/2024	4/16/2024	4/16/2024	5/16/2024	5/16/2024	5/16/2024	24-007
N/A	3220	Personnel	Recruitment, Selection and Onboarding	Human Resources	Yes	2/5/2024	3/19/2024	3/19/2024	4/10/2024	4/10/2024	4/10/2024	24-006
N/A	3225	Personnel	Employee Leave Donation Program and Workers' Compensation	Human Resources	Yes	2019	2019	2019	10/9/2019	10/9/2019	10/9/2019	19-011
N/A	3230	Personnel	Accommodations for Disability	Human Resources	No	5/9/2023	5/16/2023	5/16/2023	6/14/2023	6/14/2023	6/14/2023	23-017
N/A	3235	Personnel	Military Leave	Human Resources	Yes	6/14/2023	8/15/2023	11/21/2023	12/13/2023	12/13/2023	1/10/2024	23-031
N/A	3240	Personnel	Dress Code and Personal Standards	Human Resources	Yes	4/8/2024	4/16/2024	4/16/2024	5/16/2024	5/16/2024	5/16/2024	24-007
N/A	3255	Personnel	Other Mandated Leaves of Absence	Human Resources	No	9/10/2024	9/18/2024	9/18/2024	10/9/2024	10/9/2024	10/9/2024	24-018
1	4005	Board of Directors	Basis of Authority	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
2	4010	Board of Directors	Members of the Board of Directors	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
3	4015	Board of Directors	Committees of the Board of Directors	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
4	4020	Board of Directors	Board President	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
5	4025	Board of Directors	Board Meetings	Administration	Yes	Verbal Review during	N/A	Directed to Full Board	12/8/2021	12/8/2021	1/11/2023	2023-02
6	4030	Board of Directors	Board Meeting Agenda	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
7	4035	Board of Directors	Board Meeting Conduct	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
8	4040	Board of Directors	Board Actions and Decisions	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
9	4045	Board of Directors	Attendance at Meetings	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
10	4050	Board of Directors	Minutes of Board Meetings	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
11	4055	Board of Directors	Rules of Order for Board and	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
12	4060	Board of Directors	Training, Education and Conferences	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
13 & 16	4065	Board of Directors	Remuneration, Director Per Diem Fees	Administration	Yes	6/30/2021	N/A	Directed to Full Board	7/14/2021	7/14/2021	7/14/2021	2021-12
14	4070	Board of Directors	Payment of Expenses Incurred on	Administration	Yes	6/30/2021	N/A	Directed to Full Board	7/14/2021	7/14/2021	7/14/2021	2021-12
15	4075	Board of Directors	Expenditure Reimbursement	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
17	4080	Board of Directors	Membership in Associations	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
18	4085	Board of Directors	Ethics Training	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
19	4090	Board of Directors	Code of Ethics	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
20	4095	Board of Directors	Ethics Policy	Administration	Yes	N/A	N/A	Direct to Board (Ad Hoc?)				
N/A	4100	Board of Directors	Electronic Communications and Data Devices at Dais	Administration	Yes	6/28/2021	N/A	Directed to Full Board	7/14/2021	7/14/2021	7/14/2021	2021-11
N/A	4110	Board of Directors	Communications, Social Media and PR	Administration	Yes							
N/A	4120	Board of Directors	Legislative Advocacy	Administration	Yes							
N/A	4200	Board of Directors	Candidate Statement Fees	Administration	Yes							
1	5005	Operations	Emergency Preparedness	Human Resources	Yes	7/29/2024	8/20/2024	8/20/2024	9/17/2024	9/17/2024	9/17/2024	24-014
2	5010	Operations	Emergency Response Guideline for Hostile or Violent Incidents	Human Resources	Yes	11/8/2022	11/15/2022	11/15/2022	12/14/2022	12/14/2022	12/14/2022	22-043
4	5020	Operations	Environmental Health and Safety	Human Resources	Yes	7/29/2024	8/20/2024	8/20/2024	9/17/2024	9/17/2024	9/17/2024	24-014
5	5025	Operations	Illness and Injury Prevention Program	Human Resources	Yes	9/10/2024	9/18/2024	9/18/2024	10/9/2024	10/9/2024	10/9/2024	24-018
6	5030	Operations	Budget Preparation	Finance	Yes	11/8/2022	11/15/2022	11/15/2022	12/14/2022	12/14/2022	12/14/2022	22-043
N/A	5031	Operations	User Fee Cost Recovery	Finance	Yes	11/15/2022	N/A	N/A	12/14/2022	12/14/2022	12/14/2022	22-039
7	5035	Operations	Fixed-Asset Accounting Control	Finance	Yes	N/A	N/A	Direct to Full Board				
8	5040	Operations	Fixed-Asset Capitalization	Finance	Yes	N/A	N/A	Direct to Full Board				
9	5045	Operations	Investment of District Funds	Finance	Yes	11/15/2023	12/5/2024	12/5/2024	12/11/2024	12/11/2024	12/11/2024	24-021
N/A	5046	Operations	Other Post-Employment Benefits	Finance	Yes	5/10/2022	N/A	8/1/2024	8/14/2024	8/14/2024	8/14/2024	24-012
N/A	5047	Operations	Pension Funding	Finance	Yes	8/10/2023	8/17/2024	8/17/2024	8/14/2024	8/14/2024	8/14/2024	24-012
N/A	5048	Operations	Issuance and Management of Long-Term Debt	Finance	No							
10	5050	Operations	Customer Payment Arrangements	Finance	Yes	11/25/2024	12/5/2024	12/5/2024				
11	5055	Operations	Employment of Consultants and	Finance	Yes							
12	5060	Operations	Employment of Outside Contractors	Finance	Yes							
13	5065	Engineering	Easement Abandonment	Engineering	Yes		N/A	Direct to Full Board				
14	5066	Engineering	Easement Acceptance	Engineering	No		N/A	Direct to Full Board				
15	5070	Engineering	Encroachment Permits	Engineering	Yes		N/A	Direct to Full Board				
16	5075	Operations	Credit Card Usage	Finance	Yes		8/17/2024	8/17/2024				

Priority Legend:
 Yellow Highlight = Highest Priority
 Light Blue Highlight = Lowest Priority



**Beaumont-Cherry Valley Water District
Personnel Committee Meeting
January 21, 2025**

Item 8

STAFF REPORT

TO: Board of Directors
FROM: Finance and Administration Department
SUBJECT: Acknowledge the ACWA JPIA President's Special Recognition Award

Staff Recommendation

Acknowledge the President's Special Recognition Award from the Association of California Water Agencies Joint Powers Insurance Authority (ACWA/JPIA) for the Liability category.

Executive Summary

BCVWD has been honored with the ACWA/JPIA President's Special Recognition Award in the Liability category, which is based on maintaining a low loss ratio over a three-year period. This reflects BCVWD's commitment to safety and effective risk management. It marks the District's first recognition in this category, highlighting its dedication to operational excellence, and was presented to the Board of Directors at the January 8, 2025 meeting.

Background

The Association of California Water Agencies Joint Powers Insurance Authority (ACWA/JPIA) is a partnership of water agencies that collectively share risks associated with water purveyance and it requires its member agencies to demonstrate a strong commitment to effective safety and risk management programs. Each year, ACWA/JPIA recognizes agencies achieving a Loss Ratio of 20% or less over three years, comparing paid claims and case reserves to deposit premiums. This evaluation applies to the Liability, Property, or Workers' Compensation Programs.

BCVWD has been a member since 1987 for the General Liability and Property programs, and 1994 for Workers' Compensation. For the period from October 2020 to September 2023, BCVWD received the Liability Program award, reflecting its commitment to safety, risk reduction, and operational reliability through regular training and best practices.

Discussion

At the January 8, 2025, Board meeting, the ACWA/JPIA Liability Program award for October 2020 to September 2023 was received and filed as part of the reports section. As one of the few awards directly reflecting the contributions of Operations, staff would like to specifically highlight the safety aspect of this recognition and express gratitude to all staff, particularly the Operations team, for their continued diligence in maintaining a safe and efficient work environment.

Fiscal Impact: None.

Attachments

1. President's Special Recognition Award

Staff Report prepared by Sylvia Molina, Assistant Director of Finance and Administration

President's Special Recognition Award

*The President of the
ACWA JPIA
hereby gives Special Recognition to*

Beaumont-Cherry Valley Water District

*for achieving a low ratio of "Paid Claims and Case Reserves" to "Deposit Premiums"
in the Liability Program for the period 10/01/2020 - 09/30/2023
announced at the Board of Directors' Meeting in Palm Desert.*



Melody McDonald

Melody McDonald, President

December 02, 2024