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, March 18, 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 – MARCH 18, 2025

Call to Order: Chair Covington

Roll Call

	John Covington, Chair
	Lona Williams

	Andy Ramirez (alternate)

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

ACTION ITEMS

2. **Acceptance of Personnel Committee Meeting minutes**
   Minutes may be accepted by consensus
   a. January 21, 2025 Regular Meeting (pages 4 - 9)
   b. February 18, 2025 Regular Meeting (pages 10 - 13)

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 14 - 15)

6. **Policies and Procedures Manual Updates / Revisions**

a.	Policy 7001	IT – Acceptable Use	pages 16 - 26
b.	Policy 7002	Bring Your Own Device	pages 27 - 31
c.	Policy 7005	Internet Use and Personal Social Media Ethics	pages 32 - 54
	Policy 5100	Press Relations and Social Media Policy	

7. **Update on Policy Tracking Matrix** (pages 55 - 59)
   a. Status of Policy Revisions / Updates

8. **Action List for Future Meetings**

9. **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, January 21, 2025, at 5:30 p.m.

CALL TO ORDER

Chair Covington called the meeting to order at 5:36 p.m. He welcomed Director Lona Williams to the Committee as a member (she was previously the alternate).

ROLL CALL

Directors present:	*John Covington, Lona Williams*
Directors absent:	*None*
Staff present:	*General Manager Dan Jaggers* *Director of Finance and Administration Sylvia Molina* *Director of Information Technology Robert Rasha* *Human Resources Manager Ren Berioso* *Administrative Assistant Cenica Smith*
BCVWD Employee Association reps:	*Andrew Becerra, Ericka Enriquez, Luis Lomeli*
Members of the Public:	*None*

PUBLIC COMMENT: None.

ACTION ITEMS

1. **Adjustments to the Agenda:** None.

2. **Acceptance of the Personnel Committee Meeting minutes**

   a. November 19, 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 45 employees
   - 56 applicants for a temporary Water Utility Worker position
   - Notable anniversaries including Joe Reichenberger (18 years as an employee)

6. **Policies and Procedures Manual Updates / Revisions**
   Human Resources Manager Ren Berioso presented the proposed revisions to the following policies:

   a. Policy 3145 Driver Training and Record Review

Mr. Berioso provided a summary of the new revisions. He noted that, pursuant to the Committee's previous discussion, the changes involved clarifying the process for a 12-month driving probation period, which places an employee under supervision, as well as addressing corrective actions. In collaboration with Association of California Water Agencies Joint Powers Insurance Authority (ACWA JPIA), the policy now requires defensive driving classes for employees who incur points on their driver's licenses, regardless of whether the points are from personal or work-related incidents. These classes are free of charge, and the district will bear any costs for required training.

Chair Covington inquired about the specifics of the policy, especially concerning employees whose job descriptions require driving. He highlighted the issue of what to do with employees who incur points and face probation, specifically regarding the discretion of the General Manager in handling these situations. Covington confirmed that his and Director Ramirez's concerns from a previous meeting had been addressed in the updated policy.

Director Williams raised a question for clarity regarding the policy's mention of department heads and the requirements for the defensive driving course. Department heads who drive are required to take the defensive driving course every four years.

The discussion concluded with the acknowledgment that the policy now includes provisions for disciplinary actions, such as suspension or termination, if an employee accumulates a certain number of points on their driving record, and driving is essential to their job.

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 7004 Email and Communication

Mr. Berioso introduced Policy 7004, explaining that it formalizes existing procedures that have been in use since 2014. These procedures were initially part of an Information Technology (IT) and cybersecurity policy manual created in 2017. The new policy aims to ensure compliance with standards like the California Public Records Act (CPRA) and the California Consumer Privacy Act (CCPA) while securing the district's email and communication systems. The policy is designed to apply to employees, contractors, and third parties involved in district-related functions.

Director Covington sought clarification on the relationship between the newly proposed policy and previous policies. Mr. Berioso clarified that there is a separate employee IT policy manual for staff-related policies. However, the new policy would be included in the general policy handbook for the Board of Directors to review. Berioso confirmed this would also apply to other IT-related policies.

The policy also outlines the retention of business emails, which must be archived indefinitely to comply with the CPRA, meaning that even emails from former employees are retained, Berioso continued. Director Covington inquired about the timeline for email retention under the District's records retention policy, and Mr. Berioso confirmed that emails are retained indefinitely. There was also clarification that email retention must comply with CPRA, meaning any stored emails must be provided if requested.

Further aspects of the policy focus on professional conduct, including using company emails for business purposes only, and monitoring systems in case of suspicious email use. The policy also requires staff to report phishing emails to the IT department. Additionally, the district maintains that all third-party vendor communications must adhere to its secure communication practices.

Director Williams inquired about the frequency of the training and usage restrictions in the policy, specifically regarding the use of emails for personal activities. Williams wanted to confirm that the policy clearly states that employees are prohibited from using District-provided email for non-business purposes, such as creating personal social media accounts. Berioso confirmed that employees are required to use their District email for all business-related communications and must not use it for personal matters.

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.	

c. Policy 7006 Password

Mr. Berioso presented the new IT Policy 7006, focused on password management, aimed at minimizing the risk of unauthorized access and data breaches while ensuring operational integrity and regulatory compliance. He explained that it applies to employees, contractors, and third parties using the District's IT systems, applications, and devices. One of the main highlights of the policy is that passwords must remain confidential, never shared between employees, contractors, or vendors, and any suspected compromises

should be promptly reported to the IT Department. Additionally, the IT Department will audit password compliance, monitor failed login attempts, and enforce disciplinary actions for non-compliance, which could include suspension.

Chair Covington asked if these updates were recent, specifically within the last few months. Mr. Rasha confirmed that the policies had been reviewed in June and July of 2024, and again in January 2025 as part of the District's standard review process.

Director Williams asked if employees were required to periodically change their passwords. Rasha explained that the previous best practice was to require password changes every 90 days, but the National Institute of Standards and Technology (NIST) had updated its framework, and now, the District only requires password changes if a system is compromised or there are invalid login attempts. Rasha added that the district uses a password manager to help employees manage their passwords, and that more sensitive systems, such as financial software, are protected with multi-factor authentication (MFA).

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.	

d. Policy 7011 Cellular Telephone Usage

Mr. Berioso explained that Policy 7011 aims to ensure secure, compliant, and efficient use of cellular devices for District business while protecting sensitive data and adhering to regulatory standards such as the CPRA and CCPA. This policy applies to all district employees who use District-issued cell phones or personal phones for District-related business. Employees have the option to choose between using a District-issued phone or their personal phone, but if they opt for a personal phone, they must adhere to the standards outlined in the policy.

Chair Covington asked whether every employee is issued a cell phone. Berioso clarified that those who frequently conduct District business by phone are provided with one. For employees who only occasionally need to use a phone, personal phones are often used. Mr. Rasha added that personal phones used for District business can be subject to subpoena or disclosure under the CPRA, which is why it is recommended that employees who frequently use their phones for District tasks use a District-issued phone. This is to protect both the employee and the District. Berioso further explained that there is a separate policy for employees who choose to bring their own device (BYOD), and only those in key positions or with authorization from IT can use personal phones for District-related work.

Covington expressed concern over records from personal phones being obtained. Berioso clarified that only records related to District business on a personal phone were subject to disclosure, which was a significant concern addressed by the policy.

The policy includes provisions on data ownership and protection. It mandates that sensitive District data can only be stored or accessed on authorized, encrypted devices

that use District-approved applications. For example, District-issued phones are restricted to approved apps, and employees cannot download unauthorized software. Employees are also responsible for safeguarding their phones, reporting any security incidents, and avoiding tampering with the devices. Supervisors are tasked with ensuring compliance.

Berioso concluded by noting that the policy is reviewed annually by IT, and any revisions will be brought to the Personnel Committee for further review before being submitted to the 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 advised that out of the 70 personnel policies on the Matrix, 68 have been completed. Some will be brought back for revision due to new laws. The focus will now be on IT policies, of which 17 are personnel related. With the Finance and Engineering policies, the project is far from complete, he noted.

8. Receipt of Association of California Water Agencies / Joint Powers Insurance Authority Award

Director of Finance and Administration Sylvia Molina advised of the District's receipt of the President's Special Recognition Award from ACWA JPIA in the liability category. This award, given to agencies with a low ratio of claims over the past three years, was presented to acknowledge the District’s efforts in promoting employee safety and general risk management. The award particularly highlighted the proactive approach taken by the Operations team, which works with heavy equipment, tools, and hazardous materials daily. Mr. Berioso and Mr. Jaggers emphasized the collaborative nature of the achievement, thanking the entire staff, from field workers to administrative teams, for their contributions to maintaining high safety standards. Ms. Molina pointed out that this was the first time the District had received this award, despite participating in the liability programs since 1994.

Chair Covington expressed pride in the award, emphasizing that every employee, regardless of their role or whether they work in the office or the field, contributed to the District’s success in achieving it. He highlighted the risks faced by field staff and credited the District’s leadership for implementing policies that ensure safety. Covington underscored the importance of ongoing efforts, such as safety meetings and resources dedicated to improving safety practices. He acknowledged that past leadership may not have prioritized such efforts, making this recognition even more significant. Director Williams also praised the employees for their conscientiousness in ensuring safety on the job site. She congratulated everyone for earning such a hard-to-get and well-deserved award, recognizing the importance of their continued focus on safety.

9. **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)

10. **Next Meeting Date:**
    Regular Meeting Tuesday, February 18, 2025, at 5:30 p.m.

ADJOURNMENT: *6:30 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 AGENDA
560 Magnolia Avenue, Beaumont, CA 92223

MINUTES OF THE PERSONNEL COMMITTEE MEETING
Tuesday, February 18, 2025, at 5:30 p.m.

CALL TO ORDER

Chair Covington called the meeting to order at 5:45 p.m.

ROLL CALL

Directors present:	*John Covington, Lona Williams*
Directors absent:	*None*
Staff present:	*General Manager Dan Jaggers* *Assistant Director of Finance and Administration Sylvia Molina* *Director of Information Technology Robert Rasha* *Human Resources Manager Ren Berioso* *Executive Assistant Lynda Kerney*
BCVWD Employee Association reps:	*Andrew Becerra, Ericka Enriquez, Luis Lomeli*
Members of the Public:	*None*

PUBLIC COMMENT: None.

ACTION ITEMS

1. **Adjustments to the Agenda:** None.

2. **Report / Update from BCVWD Employees Association:** Luis Lomeli reported that field staff is making more use of the newly renovated facilities at 12th and Palm, and it is clean and safe. He thanked the Committee.

3. **Report / Update from BCVWD Exempt Employees:** None.

4. **Report from Human Resources Department**
   Human Resources Manager Ren Berioso presented highlights of the report:
   - Currently 49 employees
   - Four new hires in Operations
   - 529 applications for the Customer Service Representative position
   - Notable anniversaries including Joe Haggin (23 years)

5. **Policies and Procedures Manual Updates / Revisions**
   Human Resources Manager Ren Berioso presented the proposed revisions to the following policies:

a. Policy 3111 Leave for Crime Victims and Family Members

Mr. Berioso introduced revisions which were made to comply with California Assembly Bill (AB) 2499, which expands leave protections to include victims of domestic violence, sexual assault, and stalking, as well as employees caring for family members impacted by these events. The policy now also incorporates provisions from AB 1041, effective January 2023, which designates additional persons eligible for care leave, and considers other legislation like the Fair Employment and Housing Act (FEHA) and the Americans with Disabilities Act (ADA). The revisions provide clearer definitions of qualifying crimes and the conditions under which employees can take leave, including counseling, medical care, or relocation. The policy also allows employees to use accrued sick leave or vacation for certain types of leave and ensures that employees will not face retaliation for taking leave under these provisions.

Director Williams raised a question regarding the language in the policy, specifically asking why the actual text of AB 1041 and other related laws were not referenced in section 3111.2, which outlines reasons for taking leave, noting that the law might be subject to change. After a discussion, Mr. Berioso and Mr. Jaggers clarified that the language was intentionally kept broad to allow for future updates, as AB 1041 specifically expanded the class of people eligible for care under the law. Chair Covington expressed his understanding of the thorough revisions, acknowledging that legal counsel had made significant contributions to the redline version.

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.	

6. Update on Policy Tracking Matrix

Mr. Berioso reviewed the dashboard and noted 3111 was the last policy to present to the Committee. If approved by the Board, the project is 100 percent complete. IT policies are still in progress and the ones reviewed by the Committee in January will probably go to the next Board meeting.

The Committee recommended the following policies be brought to the March 18, 2025 Personnel Committee meeting for review:

1. *7003 Cloud Computing*
2. *7007 Remote Access*
3. *7108 Wireless Network Security*

by the following vote:

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

7. Annual Human Resources Report

Mr. Berioso reported:

- The District's workforce grew from 43 employees in January 2024 to 45 by the end of the year, with an average of 44 employees.
- A total of 13 new external hires and 10 internal promotions/transfers occurred, with seven employees leaving the organization.
- The average onboarding time for new employees decreased from 38 days in 2023 to 17 days in 2024, with a cost per hire of $1,700.
- Employee retention was improved, with only five voluntary separations and two involuntary separations (including one death), marking the lowest turnover rate in the past five years.
- An informal salary survey was completed, incorporating a 2.5% Cost of Living Adjustment (COLA) based on the August Consumer Price Index.
- The District's benefits enrollment decreased by 2%, though employees continued to opt for medical insurance and retirement benefits.
- In 2024, 16 district-wide training sessions were held, totaling 84 hours of training.
- 88% of annual performance reviews were completed, with 100% of employees meeting or exceeding expectations.
- Risk management showed five workers' compensation claims, with an overall trend of decreasing claims over the past few years.
- Five claims against the District were reported, with ongoing litigation in some cases.
- A total of 34 policy amendments were made in 2024 to comply with legal requirements, including changes to family medical leave and other policies.

Director Williams inquired about the inclusion of temporary employees in the recruitment pie chart, asking if they were counted as internal hires when they transitioned to full-time positions. Mr. Berioso confirmed that they were, which explained the high percentage of internal hires. Williams also expressed satisfaction with the improvements in employee retention and compensation adjustments, noting that it was encouraging to see the District becoming a more attractive place to work. She also commented on the importance of making long-term adjustments to reduce turnover, particularly in relation to compensation and career opportunities. She acknowledged the thoroughness of the report and said she appreciated the transparency in presenting the data, particularly regarding the turnover and training efforts.

Chair Covington commented on the overall improvement in employee retention and compensation, emphasizing that it is important to recognize the contributions of the entire staff. He highlighted that the District has made significant progress compared to previous years, with retention rates improving and compensation adjustments addressing concerns that led to turnover in the past. Covington also reflected on the organizational improvements, such as the decrease in onboarding time and the greater focus on internal promotions. He acknowledged the efforts of HR in enhancing the overall work environment. Covington concurred with the motion to receive and file the report, indicating no further need for discussion at the full Board level.

8. **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)
   - Update on Cal OSHA report
   - Update on driver incidents / training

9. **Next Meeting Date:**
   Regular Meeting Tuesday, March 18, 2025, at 5:30 p.m.

ADJOURNMENT: *6:25 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
March 18, 2025

Item 5

HUMAN RESOURCES REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: **Human Resources Department Report for the Month of February 2025**

Table 1: Personnel

The below table represents the District's current Workforce.

As of February 28, 2025

Total Current Employees (Excluding Board Members)	47
Full-Time Employees	42
Part-Time	1
Temporary	4
Interns	0
Separations	2
Retired Employee(s)	0

Table 2: New Hires

The table below represents new hires.

As of February 28, 2025

Employee Name	Job Title	Department
None		

Table 3: Anniversaries*

The below table represents BCVWD employee anniversaries.

As of February 28, 2025

Employee Name	Department	Years of Service
James Bean	Operations	26 years

**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 February 28, 2025

Employee Name	Former Title	Changed to
None		

Table 5: Recruitment

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

As of February 28, 2025

Position	Department	Update
Customer Service Representative I	Finance and Administration	Posting Closed 02/06/2025 Interviews Ongoing

Table 6: Separation/Retirement

The below table represents employees separating from BCVWD.

As of February 28, 2025

Employee Name	Position Held	Department	Last Day
Vanessa Barbo	Customer Service Representative I	Finance and Administration	02/06/2025
Marlon Jones	Temporary Water Utility Worker I	Operations	02/20/2025

Table 7: Communications

The below table represents HR communications to BCVWD employees.

As of February 28, 2025

Communication	Topic
HR Memo 25-004, Exclusive Discounted Travel Benefit for BCVWD Employees	Benefits
HR Memo 25-005, Exclusive Discounted Travel Benefit for BCVWD Board of Directors	Benefits
HR Memo 25-006 Active Shooter Assailant Training	Workplace Safety
HR Memo 25-007, President's Day Holiday Closure and Holiday Pay Reminder	Holiday
HR Memo 25-007 Employee Appreciation Day Celebration March 4 2025	Engagement

Staff Report Prepared by Ren Berioso, Human Resources Manager

Beaumont-Cherry Valley Water District
Personnel Committee
March 18, 2025

Item 6a

STAFF REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: **Policies and Procedures Manual Updates / Revisions establishing Information Technology Policy 7001 Acceptable Use Policy**

Staff Recommendation

Recommend the proposed Information Technology (IT) Policy 7001 Acceptable Use Policy 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 7001 Acceptable Use Policy with sections that provide guidelines for the responsible and secure use of Beaumont-Cherry Valley Water District's (BCVWD) IT resources. The revision aligns with National Institute of Standards and Technology (NIST) principles and complies with California state laws such as the California Public Records Act (CPRA) to ensure transparency, accountability, and data protection. Additionally, the proposed policy defines acceptable and prohibited activities, covering areas such as IT security, internet and email usage, third-party compliance, remote work guidelines, and enforcement measures.

Background

At the November 19, 2024 meeting, the Director of IT requested the Personnel Committee to review the Employee IT Policy Handbook to ensure alignment with the District's strategic goals, legal requirements, and regulatory standards. In partnership with IT, Human Resources (HR) staff facilitated the review and presented the proposed policy draft to Legal Counsel to ensure compliance with applicable labor laws. The handbook and the IT and Cybersecurity Policy Manual, both updated annually, outline technology policies, security measures, and employee expectations aligned with the NIST framework and industry best practices. These efforts have strengthened BCVWD's cybersecurity framework and contributed to the District receiving the Municipal Information Systems Association of California (MISAC) award for excellence in IT governance for the past two years.

Discussion

The Acceptable Use Policy is essential because it safeguards BCVWD's IT resources, ensures cybersecurity, protects sensitive data, and maintains compliance with legal and regulatory standards. Table A, Summary of Policy Sections, outlines the proposed Acceptable Use Policy that was drafted by HR and IT Departments.

Table A – Summary of Policy 7001 Sections

TABLE A	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	**NIST**	This policy ensures IT resources are used responsibly in alignment with NIST-and state cybersecurity regulations.	**Consider establishing Section 7001.1** Introduction	No fiscal impact.
2	**NIST**	IT Department safeguards the IT assets and resources while aligning with NIST guidelines and California cybersecurity laws.	**Consider establishing Section 7001.2** Purpose	No fiscal impact.
3	**NIST**	Applies to all individuals including employees, contractors, and third parties who use BCVWD's IT resources, computers, applications, and devices.	**Consider establishing Section 7001.3** Scope.	No fiscal impact.
4	**NIST**	District IT resources are used primarily for authorized business purposes, with limited personal use allowed as long as it does not interfere with work, compromise security, or violate policies, and are not used for personal gain, solicitation, or activities that could harm BCVWD's reputation	**Consider establishing Sections 7001.4.1.a to c** General Use	No fiscal impact.
5	**NIST**	Employees must protect District data and IT resources, follow NIST guidelines and California laws, use secure authentication per Policy 7006, and promptly report security incidents to IT through the designated system.	**Consider establishing Sections 7001.4.2.a to d** Security and Confidentiality	No fiscal impact.
6	**NIST**	Employees are not permitted to use District IT resources for unauthorized, illegal, or inappropriate activities.	**Consider establishing Sections 7001.4.3.a to b** Prohibited Activities	No fiscal impact.
7	**NIST**	BCVWD's internet and email are used primarily for business purposes, with professionalism, security, and compliance with Policy 7004 and the Internet and Social Media Policy, while personal email use is strictly limited.	**Consider establishing Sections 7001.4.4.a to d** Internet and Email Use	No fiscal impact.

TABLE A	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
8	**NIST**	IT, if needed, may monitor and audit IT resource usage to ensure compliance, and employees are aware that there is no expectation of privacy when using District systems	**Consider establishing Sections 7001.4.5.a to b** Monitoring Privacy	No fiscal impact.
9	**NIST**	The District follows the law.	**Consider establishing Sections 7001.4.6.a to b** Compliance with Local and State Laws	No fiscal impact.
10	**NIST, CPRA**	Employees follow acceptable use standards when accessing District IT resources remotely, ensure secure access with authorized devices, and are aware that failed login attempts are monitored for security threats.	**Consider establishing Sections 7001.4.7.a to c** Remote Work Guidelines	No fiscal impact.
11	**NIST**	Contractors and third parties comply with this policy, and their access to District IT resources are monitored by the IT Department to ensure compliance	**Consider establishing Sections 7001.4.8.a to b** Third-Party Compliance	No fiscal impact.
12	**NIST**	District systems will display a login banner referencing the Acceptable Use Policy, and users do acknowledge compliance by logging in, with the IT Department ensuring updates as needed.	**Consider establishing Sections 7001.4.9.a to b** Policy Acknowledgment	No fiscal impact.
13	**FEHA and At-Will Employment**	Violations of this policy may lead to disciplinary action, IT access suspension, termination, or legal consequences, depending on severity.	**Consider establishing Sections 7001.4.10.a** Enforcement	No fiscal impact.
14	**NIST**	IT Department annually reviews and updates the Acceptable Use Policy to ensure compliance, effectiveness, and alignment with NIST standards, regulations, and evolving technology needs	**Consider establishing Sections 7001.5** Review and Revision Policy	No fiscal impact.

Fiscal Impact

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

Attachments

1. Proposed new Policy 7001: Acceptable Use Policy
2. NIST: Understanding the Cybersecurity Framework
3. California Public Records Act FAQs

Staff Report prepared by Ren Berioso, Human Resources Manager

POLICY TITLE: ACCEPTABLE USE POLICY
POLICY NUMBER: 7001

7001.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) relies on Information Technology (IT) resources as essential tools for conducting business efficiently and securely. This policy ensures these resources are used responsibly, ethically, 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) to ensure transparency and accountability in public records management.

7001.2 Purpose. The purpose of this policy is to define acceptable use of BCVWD's IT resources, safeguard District assets, and prevent unauthorized use that could compromise security, productivity, or compliance with legal and regulatory requirements.

7001.3 Scope. This policy applies to all employees, contractors, and third parties who access BCVWD's IT resources, including but not limited to computers, networks, email systems, internet services, and mobile devices.

7001.4 Policy Details

7001.4.1 General Use

a. District IT resources are to be used solely for authorized business purposes in support of BCVWD's mission.
b. Limited personal use of District IT resources is permitted, provided it does not interfere with work responsibilities, compromise security, or violate District policies.
c. Employees must not use District IT resources for personal gain, solicitation, or activities that could reflect negatively on BCVWD.

7001.4.2 Security and Confidentiality

a. Employees must safeguard District data and IT resources from unauthorized access, disclosure, alteration, or destruction, in compliance with NIST guidelines and applicable California laws.
b. Employees must immediately report suspected security incidents, including unauthorized access, data breaches, or loss of District devices, to the IT Department.
c. Employees must immediately adhere to Policy 7006: Password (policy) and secure authentication methods to access IT resources.
d. Employees must report incidents through the district's designated incident reporting system or by contacting the IT Department directly for immediate assistance.

7001.4.3 Prohibited Activities

a. Employees are prohibited from using District IT resources to:
    - Access, create, or distribute offensive, discriminatory, or illegal content.
    - Download or install unauthorized software or access malicious websites.
    - Violate copyright laws or intellectual property rights.
    - Develop, implement, or access artificial intelligence (AI) or Internet of Things (IoT) technologies without prior approval from the IT Department and compliance with relevant District policies.
    - Store District data on personal cloud services (e.g., Google Drive, Dropbox) or external devices unless explicitly authorized by the IT Department.
b. Employees must not disable, or bypass IT security controls implemented by the District).

7001.4.4 Internet and Email Use

a. Internet access provided by BCVWD is intended for business use. Excessive or

inappropriate personal internet usage is not permitted.

b. Email communications must comply with Policy 7004 Email and Communication , maintaining professionalism and security.
c. Personal email accounts must not be used for District-related business, nor should personal email be accessed on District devices unless explicitly authorized.
d. Employees must adhere to Policy 7005 Internet and Social Media Policy when accessing or engaging on social media platforms using District IT resources.

7001.4.5 Monitoring Privacy

a. BCVWD reserves the right to monitor and audit the use of IT resources to ensure compliance with this policy. Monitoring will be conducted in accordance with applicable laws and District procedures.
b. Employees should have no expectation of privacy when using District IT resources.

7001.4.6 Compliance with Local and State Laws

a. Employees must comply with applicable state and local laws governing IT resource use, including public records laws such as the California Public Records Act (CPRA).
b. Use of District IT resources for political advocacy, lobbying, or other activities restricted by public agencies is prohibited.

7001.4.7 Remote Work Guidelines

a. Employees must adhere to all acceptable use standards when accessing District IT resources from remote locations.
b. Employees are responsible for ensuring secure access to District systems, including using authorized devices and maintaining a secure home network.
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.

7001.4.8 Third-Party Compliance

a. Contractors and third parties must adhere to the terms of this policy when accessing District IT resources.
b. Third-party use must be monitored at all times if access is granted to a District system by the Information Technology Department to ensure compliance with District policies.

7001.4.9 Policy Acknowledgement

a. District computer systems will display a login banner or notification referencing the Acceptable Use Policy. By logging into these systems, users acknowledge their understanding of and compliance with the policy.
b. The IT Department will ensure the login banners are updated to reflect any changes to the Acceptable Use Policy.

7001.4.10Enforcement

a. Violations of this policy may result in disciplinary action, including suspension of IT access, termination of employment, or legal action, depending on the severity of the violation.

7001.5 Review and Revision Policy. BCVWD will review Policy 7001 Acceptable Use Policy annually to ensure it remains current and effective in addressing the needs of the organization and any changes in the regulatory or technological landscape. 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?

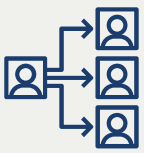
NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business 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.

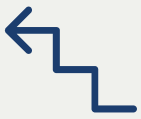
1. IDENTIFY

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

FEDERAL TRADE COMMISSION

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

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR SMALL BUSINESS

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

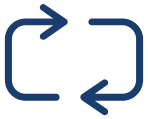
Have a plan for:

- 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

SBA U.S. Small Business Administration

Homeland Security

Item 6a 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

Beaumont-Cherry Valley Water District
Personnel Committee
March 18, 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 7002 Bring Your Own Device**

Staff Recommendation

Recommend the proposed Information Technology (IT) Policy 7002 Bring Your Own Device to move forward to the next Board of Directors meeting, or direct staff as desired.

Executive Summary

Staff proposes IT Policy 7002 Bring Your Own Device (BYOD) to establish guidelines for the secure and compliant use of personal devices in District operations. To reduce cybersecurity risks and ensure compliance with regulations such as the California Public Records Act (CPRA), the policy prohibits using personal devices for District business and restricts access to the guest wireless network. Employees are encouraged to use District-issued technology, with enforcement measures including disciplinary actions, audits, and annual reviews.

Background

At the November 19, 2024 meeting, the Director of IT requested the Personnel Committee to review the Employee IT Policy Handbook to ensure alignment with the District's strategic goals, legal requirements, and regulatory standards. In partnership with IT, Human Resources (HR) staff facilitated the review and presented the proposed policy draft to Legal Counsel to ensure compliance with applicable federal, state and local labor laws. The handbook and the IT and Cybersecurity Policy Manual, both updated annually, outline technology policies, security measures, and employee expectations aligned with the National Institute of Standards and Technology (NIST) framework and industry best practices. These efforts have strengthened BCVWD's cybersecurity framework and contributed to the District receiving the MISAC award for excellence in IT governance for the past two years.

Discussion

The Bring Your Own Device policy is significant as it protects BCVWD's cybersecurity, regulatory compliance, and operational integrity by mitigating risks associated with personal devices, ensuring adherence to CPRA, preventing unauthorized access, and reinforcing IT security best practices to safeguard critical infrastructure and sensitive data.

Table A, Summary of Policy Sections, outlines the proposed Bring Your Own Device policy that was drafted by HR and IT Departments.

Table A – Summary of Policy Sections

TABLE A	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	**NIST**	At the District, the policy ensures the responsible and secure use of technology in compliance with NIST principles and CPRA safeguarding cybersecurity, transparency, and data protection.	**Consider establishing Section 7002.1** Introduction	No fiscal impact.
2	**NIST**	The IT Department ensures that the District mitigates security and legal risks while ensuring employees have the necessary resources to work effectively.	**Consider establishing Section 7002.2** Purpose	No fiscal impact.
3	**NIST**	This policy applies to all employees, contractors, and third parties using personal devices for BCVWD operations or system access.	**Consider establishing Section 7002.3** Scope	No fiscal impact.
4	**NIST**	Personal devices are strictly prohibited from connecting to BCVWD's network or systems without written IT authorization, and employees must request necessary District-owned equipment, ensuring compliance with CPRA and minimizing legal risks	**Consider establishing Sections 7002.4.1.a to c** General Use on Personal Devices	No fiscal impact.
5	**NIST**	Personal devices may connect to BCVWD's guest wireless network for internet access only, but they must not interact with internal systems, and employees must implement basic security measures like password protection.	**Consider establishing Sections 7002.4.2.a to c** Limited Wireless Internet Use	No fiscal impact.
6	**NIST**	To ensure compliance with the CPRA, personal devices must not be used for District business, and employees are responsible for conducting all work-related communications on District-owned equipment	**Consider establishing Sections 7002.4.3.a to b** Public Record Act Compliance	No fiscal impact.

TABLE A	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
7	**NIST**	BCVWD encourages employees to coordinate with the IT Department for necessary District-owned resources, ensuring security, compliance, and the integrity of operations while preventing data leaks or breaches	**Consider establishing Sections 7002.4.4.a to b** Encouragement of District-Provided Resources	No fiscal impact.
8	**NIST and CPPA**	Unauthorized devices connected to BCVWD's network will be disconnected and reported, while any approved personal device use must comply with NIST security guidelines, and employees are required to report security incidents to IT immediately.	**Consider establishing Sections 7002.4.5.a to c** Security and Confidentiality	No fiscal impact.
9	**FEHA and At-Will Employment**	Policy violations result in disciplinary action, including loss of IT access, termination, or legal consequences, while the IT Department reserves the right to audit network access and conduct compliance checks	**Consider establishing Sections 7002.4.6.a to b** Enforcement	No fiscal impact.
10	**NIST**	IT Department annually reviews and updates the Bring Your Own Device policy to ensure compliance, effectiveness, and alignment with NIST standards, regulations, and evolving technology needs	**Consider establishing Sections 7002.5** Review and Revision Policy	No fiscal impact.

Fiscal Impact

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

Attachments

1. Proposed new Policy 7002 Bring Your Own Device
2. Attachments for NIST and CPRA are all available in Staff Report Item 6a

Staff Report prepared by Ren Berioso, Human Resources Manager

POLICY TITLE: BRING YOUR OWN DEVICE
POLICY NUMBER: 7002

7002.1 Introduction.
Beaumont-Cherry Valley Water District (BCVWD) relies on Information Technology (IT) resources as essential tools for conducting business efficiently and securely. This policy ensures these resources are used responsibly, ethically, 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) to ensure transparency and accountability in public records management.

7002.2 Purpose . The purpose of this policy is to define the District's stance on the use of personal devices (Bring Your Own Device or BYOD) for District-related activities. This policy seeks to mitigate risks such as data breaches, non-compliance with regulatory requirements, and potential legal exposure while ensuring employees have the necessary resources to conduct District business effectively.

7002.3 Scope. This policy applies to all employees, contractors, and third parties who use personal devices, including but not limited to laptops, smartphones, Internet of Things (IoT) devices, or peripherals, in connection with BCVWD operations or systems.

7002.4 Policy Details

7002.4.1 General Use on Personal Devices

a. Personal devices, including but not limited to computers, laptops, keyboards, mice, printers, Internet of Things (IoT) devices, or any other equipment, are strictly prohibited from being connected to BCVWD's network, systems, or resources unless explicitly authorized in writing by the Information Technology Department.
b. Employees must communicate all technology needs to the Information Technology Department to ensure they are provided with the necessary District-owned equipment to perform their duties.
c. Personal devices must not be used to conduct District business except when explicitly approved. There are rare exceptions to this rule where the Information Technology Department may approve the use of a personal device for business purposes. In those cases, written approval will be provided by the Information Technology Department with an understanding that the device must comply with CPRA requirements for any potential legal inquiries.

7002.4.2 Limited Wireless Internet Use

a. Personal devices such as cellphones, are permitted to connect to BCVWD's guest wireless internet network for the sole purpose of providing internet connectivity.
b. Personal devices connected to the guest wireless network must not access or attempt to interact with any internal District systems, applications, or data.
c. Employees must ensure their personal devices adhere to basic security measures, such as password protection, when accessing the guest wireless network.

7002.4.3 Public Records Act Compliance

a. Any use of personal devices for District business may subject those devices to California Public Records Act (CPRA) requests or subpoenas. This policy prohibits such use to ensure that only District-owned equipment is subject to compliance requests
b. Employees are responsible for ensuring that all District-related communications and work

are conducted using District-owned devices to maintain compliance with applicable regulations.

7002.4.4 Encouragement of District-Provided Resources

a. BCVWD highly encourages employees to communicate with the IT Department regarding technology needs to ensure they are provided with District-owned resources that meet their job requirements.
b. This approach ensures the security, compliance, and integrity of District operations while preventing potential data leaks or breaches.

7002.4.5 Security and Confidentiality

a. Unauthorized devices, if found connected to the district network or systems, will be immediately disconnected, and the incident will be reported to the employee's immediate supervisor.
b. Any approved use of personal devices (e.g., under unique exceptions) must comply with NIST security guidelines, including device encryption, secure passwords, and multi-factor authentication.
c. Employees must report any suspected security incidents involving personal devices used in connection with District resources to the IT Department immediately

7002.4.6 Enforcement

a. Violations of this policy may result in disciplinary action, including revocation of access to District IT resources, termination of employment, or legal action, depending on the severity of the violation.
b. The IT Department reserves the right to audit network access logs and perform regular compliance checks to ensure adherence to this policy.

7002.5 Review and Revision Policy. BCVWD will review Policy 7002 Bring Your Own Device annually to ensure it remains current and effective in addressing the needs of the organization and any changes in the regulatory or technological landscape. 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 the use of personal devices. Necessary updates or revisions will be made to ensure the policy continues to meet the District's requirements and supports its mission.

.

Beaumont-Cherry Valley Water District
Personnel Committee
March 18, 2025

Item 6c

STAFF REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: **Policies and Procedures Manual Updates / Revisions**
1. **Establishing Information Technology Policy 7005 Internet Use and Personal Social Media Ethics, and**
2. **Amending Policy 5100 Press Relations and Social Media Policy**

Staff Recommendation

Recommend the establishment of Information Technology (IT) Policy 7005 Internet Use and Personal Social Media Ethics, and the amendment of Policy 5100 Press Relations and Social Media 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 7005 Internet Use and Personal Social Media Ethics, which sets forth clear guidelines for the responsible use of District-provided internet resources and the ethical and legally compliant use of personal social media by District employees. This policy outlines standards for acceptable internet usage, cybersecurity best practices, and appropriate social media conduct to protect the District's integrity, reduce cybersecurity risks, and ensure compliance with applicable state and federal regulations.

The adoption of Policy 7005 will also support the related amendment of Policy 5100 Press Relations and Social Media Policy, by removing provisions related to the ethical use of personal social media and disciplinary actions for policy violations, which will now be addressed under the new policy.

Background

At the November 19, 2024 meeting, the Director of IT requested the Personnel Committee to review the Employee IT Policy Handbook to ensure alignment with the District's strategic goals, legal requirements, and regulatory standards. In partnership with IT, Human Resources (HR) staff facilitated the review and presented the proposed policy drafts to Legal Counsel to ensure compliance with applicable federal, state and local labor laws. The handbook and the IT and Cybersecurity Policy Manual, both updated annually, outline technology policies, security measures, and employee expectations aligned with the NIST framework and industry best practices. These efforts have strengthened BCVWD's cybersecurity framework and contributed to the District receiving the MISAC award for excellence in IT governance for the past two years.

Discussion

Policy 7005 Internet Use and Personal Social Media Ethics

The Internet Use and Personal Social Media Ethics policy is essential since it safeguards BCVWD's cybersecurity, ensures compliance with state regulations, protects the District's public

image, and mitigates risks associated with internet and social media use. Table A, Summary of Policy Sections, outlines the proposed Policy 7005 that was drafted by HR and IT Departments.

Table A – Summary of Policy 7005 Sections

TABLE A	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	**NIST**	BCVWD's IT resources are used securely, ethically, and in compliance with NIST principles and state regulations to protect data and maintain transparency.	**Consider establishing Section 7005.1** Introduction	No fiscal impact.
2	**NIST**	IT Department protects BCVWD's public image, enhances cybersecurity, and ensures legal compliance.	**Consider establishing Section 7005.2** Purpose	No fiscal impact.
3	**NIST**	Required compliance for all employees, contractors, and third parties using District IT resources for internet access or using personal social media engagement.	**Consider establishing Section 7005.3** Scope	No fiscal impact.
4	**NIST**	Internet use is limited to work-related activities, avoiding aimless browsing and cybersecurity risks such as phishing or unverified downloads. The District monitors internet usage to ensure security and compliance, while personal devices on District networks must adhere to Policy 7002 and use the guest Wi-Fi only.	**Consider establishing Sections 7005.4.1.a to e** Internet Use Guidelines	No fiscal impact.
5	**California Government Code § 19572 (aa)** **Government Code § 3206**	Employees must not represent BCVWD on personal social media without authorization, must use disclaimers for personal opinions, and must avoid disclosing confidential information or misleading the public	**Consider establishing Sections 7005.4.2.a to f** Personal Social Media Guidelines	No fiscal impact.
6	**California Government Code § 19572 (aa)** **Government Code § 3206**	Employees are prohibited from misusing District resources or posting inappropriate content on personal social media, with violations subject to disciplinary action under Policy 3175.	**Consider establishing Sections 7005.4.3.a to h** Prohibited Content	No fiscal impact.

TABLE A	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
7	**NIST and CPRA**	Employees must follow cybersecurity best practices, use secure District devices, avoid unapproved cloud services, and report threats to IT immediately	**Consider establishing Sections 7005.4.4.a to i** Cybersecurity Measures	No fiscal impact.
8	**NIST and CPRA**	The District follows the law.	**Consider establishing Sections 7005.4.5.a to c** Public Records Act Compliance	No fiscal impact.
9	**NIST**	BCVWD provides periodic training on internet safety, social media best practices, and compliance, while employees are encouraged to report concerns to IT.	**Consider establishing Sections 7005.4.6.a to b** Training and Awareness	The cost of the training module and application, which are both accounted for in the annual budget.
10	**FEHA**	IT Department reserves the right to audit network access and conduct compliance checks	**Consider establishing Sections 7005.4.7.a** Enforcement	No fiscal impact.
11	**NIST**	IT Department annually reviews and updates the Internet and Social Media policy to ensure compliance, effectiveness, and alignment with industry standards.	**Consider establishing Sections 7005.5** Review and Revision Policy	No fiscal impact.

Policy 5100 Press Relations and District Social Media Policy

To avoid overlapping of policy sections, the adoption of Policy 7005 will support the amendment of Policy 5100 Press Relations and Social Media Policy (adopted May 11, 2022) by removing provisions related to personal social media use and disciplinary actions. These elements will be consolidated under Policy 7005 to improve clarity, reduce redundancy, and align with modern IT governance standards. Table B Summary of Policy Changes, outlines the proposed changes to Policy 5100.

Table B – Summary of Policy 5100 Changes

TABLE B	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	**Policy 5100 Title**	**None**	Press Relations and Social Media Policy	**Consider changing the Title to "Press Relations and District Social Media Policy"**	No fiscal impact.
2	**Section 5100.3 Personal Use of Social Media**	**California Government Code § 19572 (aa)** **Government Code § 3206**	The District follows the law.	**Removed this section as this is included in the new Policy 7005.**	No fiscal impact.
3	**None**	**First Amendment of the US Constitution**	The District follows the law.	**Consider adding 5100.8.4 First Amendment right.**	
4	**All Sections**	**None**	The current policy is still enforced per applicable laws.	**Revised the numbering and improved some language contents.**	No fiscal impact.

Fiscal Impact

Policy 7005: the fiscal impact is the direct cost related to the training material, and the indirect cost of employees using District time to complete the training. All costs are accounted for in the annual budget.

Attachments

1. Proposed new Policy 7005 Internet Use and Personal Social Media Ethics
2. Side-by-Side version of Policy 7005 Internet Use and Personal Social Media Ethics
3. Redlined version of Policy 5100 Press Relations and District Social Media Policy
4. Clean version of Policy 5100 Press Relations and District Social Media Policy
5. Side-by-Side version of Policy 5100 Press Relations and District Social Media Policy

Staff Report prepared by Ren Berioso, Human Resources Manager

POLICY TITLE: INTERNET USE AND PERSONAL SOCIAL MEDIA ETHICS POLICY
POLICY NUMBER: 7005

7005.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) relies on Information Technology (IT) resources as essential tools for conducting business efficiently and securely. This policy ensures these resources are used responsibly, ethically, 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) to ensure transparency and accountability in public records management.

7005.2 Purpose . The purpose of this policy is to define acceptable use of the internet and social media by BCVWD employees, contractors, and third parties. The policy seeks to protect the District's public image, mitigate cybersecurity risks, and ensure compliance with legal and regulatory requirements.

7005.3 Scope. This policy applies to all employees, contractors, and third parties using District IT resources to access the internet or engage on social media platforms for personal or professional purposes.

7005.4 Policy Details

7005.4.1 Internet Use Guidelines

a. Internet use must align with Policy 7001 Acceptable Use Policy and be limited to activities that directly support District business.
b. Employees should avoid browsing the internet aimlessly. Internet access should be intentional and limited to work-related activities.
c. Employees must not click on suspicious links, respond to phishing attempts, or download content from unverified sources.
d. The district monitors internet usage to protect cybersecurity, detect potential threats, and ensure compliance with this policy. Monitoring will be conducted in accordance with applicable laws and District procedures
e. Use of personal devices on District networks must comply with Policy 7002 Bring Your Own Device and is limited to the guest wi-fi network

7005.4.2 Personal Social Media Guidelines

a. Employees must not represent or speak on behalf of BCVWD on personal social media platforms unless explicitly authorized to do so by the General Manager or his or her designee.
b. Employees must avoid posting content that could give the impression they are speaking on behalf of BCVWD. Employees are encouraged to include a disclaimer such as, "The opinions expressed here are my own and do not reflect the views of BCVWD."
c. Employees must exercise professionalism and discretion when posting on any personal social media, especially when their role with BCVWD could create the perception they are speaking in an official capacity.
d. Employees must not disclose sensitive or confidential District information on personal social media platforms.
e. Employees must take care to avoid any personal social media activity that could be construed as representing BCVWD without explicit authorization. This includes refraining from commenting on District operations, policies, or events in a way that could mislead the public.
f. Employees are reminded that privacy settings on personal social media platforms are not

foolproof, and posts or interactions may become public or be shared widely. Employees should exercise caution to protect their personal and professional reputation, as well as the District's integrity

7005.4.3 Prohibited Content. As public officials, employees are held to a higher standard of conduct. All District staff are required to adhere to the ethical standards outlined in this policy and all applicable laws. Any misuse of District resources or posting inappropriate content in the employee's personal social media accounts in violation of these standards may result in disciplinary action, up to and including termination of employment (Please refer to the Disciplinary Actions or Terminations policy for more information). Inappropriate content includes, but is not limited to:

a. Violence, profanity, obscenity, nudity, or pornographic content or language,
b. The content is found to discriminate against any creed, race, gender, sexual orientation, age, religion or national origin, as well as any other category protected by state or federal laws,
c. Threats, slander, or defamation of any kind.
d. Illegal acts of any kind or encouragement thereof,
e. Information that compromises the security or well-being of any District staff member, partner, resident or stakeholder,
f. Comments, links, posts, advertisements, or articles soliciting businesses, trade or commerce,
g. Content that violates copyright laws, or
h. Content that violates local, state or federal laws.

7005.4.4 Cybersecurity Measures

a. Employees must adhere to NIST best practices by avoiding insecure websites (e.g., those without HTTPS) and reporting suspicious online activity to the IT Department immediately.
b. All District-provided devices must be equipped with secure browsing tools, such as firewalls and antivirus software, to protect against cybersecurity threats.
c. Employees are responsible for ensuring their internet use does not expose District systems to unnecessary risks, such as malware or data breaches.
d. All District computer systems are equipped with software designed to ensure compliance with safe internet practices and block known malicious websites. However, as cybersecurity threats evolve, employees must remain vigilant. Any suspicious websites, pop-ups, or online activities should be reported immediately to the Information Technology Department for evaluation and mitigation.
e. Employees are expected to stay informed about evolving cybersecurity threats and participate in periodic training provided by the District. Adopting a proactive approach to internet safety, such as verifying website legitimacy and avoiding unfamiliar links, is critical to protecting District systems and data.
f. District computer systems are configured to use encrypted communications (e.g., HTTPS) to secure internet activities. Employees must ensure they do not transmit sensitive District information over unencrypted connections or through insecure platforms.
g. Employees must report any cybersecurity incidents related to internet or social media usage to the Information Technology Department immediately, including unauthorized access attempts, suspicious pop-ups, or phishing messages.
h. Employees are prohibited from using personal email accounts or personal cloud storage services (e.g., Google Drive, Dropbox) for storing, transmitting, or accessing District data unless discussed and authorized by the Information Technology Department.
i. The use of cloud-based services for District business must comply with the Cloud Computing Policy and be explicitly approved by the Information Technology Department.

7005.4.5 Public Records Act Compliance

a. All internet and personal social media activities conducted on District-owned devices or networks are subject to the California Public Records Act (CPRA) and may be disclosed upon request.
b. Using personal devices for District business may subject those devices to subpoenas or CPRA requests.
c. To ensure compliance with the CPRA and limit potential exposure to subpoenas, employees must use only District-approved email accounts and cloud resources for all District-related activities. Personal email accounts and unauthorized cloud services are strictly prohibited for District business.

7005.4.6 Training and Awareness

a. BCVWD will provide periodic training to employees on safe internet use, social media best practices, and compliance with this policy. These training sessions will align with the District's Security Awareness and Training Policy to ensure comprehensive employee education on cybersecurity and compliance.
b. Employees are encouraged to report any concerns related to the internet or social media usage to the Information Technology Department.

7005.4.7 Enforcement

a. The IT Department reserves the right to monitor and audit internet and social media activity conducted on District systems to ensure compliance with this policy.

7005.5 Review and Revision Policy. BCVWD will review Policy 7005 Internet Use and Personal Social Media Ethics annually to ensure it remains current and effective in addressing the needs of the organization and any changes in the regulatory or technological landscape. 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 internet and social media use. Necessary updates or revisions will be made to ensure the policy continues to meet the district's requirements and supports its mission.

CURRENT POLICY

POLICY TITLE: PRESS RELATIONS AND SOCIAL MEDIA POLICY
POLICY NUMBER: 5100

5100.1 **Purpose.** The purpose of the press relations and social media policy is to work supportively with press relations (media) and to disseminate information of public interest and concern in an accurate, complete, and timely manner. Public Relations and Social Media are vital in outreach efforts that help engage the community quickly and relevantly. It allows stakeholders to communicate with the District and quickly access important information. The District currently manages social media activities across several platforms, such as Facebook, Twitter, and YouTube. This policy will establish clear guidelines for the appropriate use of current policies, which may be updated from time to time and future press relations and social media activities.

5100.2 **Press Relations and Social Media Use.** The District will use press relations and social media to share timely, relevant information that keeps stakeholders up to date on what is happening in the District and with water in his or her community. The goal of social media activity will be to share information about District subjects, events, reminders, District updates, or other District press relations and informal notices. Social media shall also share critical information that needs to reach stakeholders quickly. The use of social media is to complement but not replace other communication methods regarding District activities and business.

1. The General Manager or his/her designee is designated as the District's Public Information Officer (PIO) and is responsible for implementing this policy. When the PIO is unavailable, he or she shall select an authorized designee.

2. The PIO shall coordinate District responses with the Board President to ensure the District meets the Board of Director's communications goals.

3. Employees and elected officials who engage with consumers or members of the Press shall use courtesy, politeness, and professionalism. Any media inquiries received by district staff will be referred immediately to Department Directors or the General Manager (if any Department Director is unavailable), who shall directly forward the media inquiry and contact information to the PIO and Board President (as necessary) for a response.

4. The General Manager, the Board President, or his/her designee will prioritize inquiries from the news media and respond as efficiently as possible.

5. When contacted by the PIO for information needed to respond to a media inquiry, all staff shall provide the PIO with accurate and complete information available for the response. The General Manager or Designee will identify if additional time is needed to address a media inquiry.

6. At the discretion of the PIO and the Board President, if it is determined that a District response is best achieved by having staff or a consultant speak on behalf of the District on a particular topic, he or she may designate an authorized spokesperson to assist with the District's response.

7. To assure that all members of the Board of Directors have accurate, complete, and timely information to fulfill responsibilities to represent the District affairs, members of the Board of Directors shall inform the PIO by email of the substance of significant media inquiries and for an official response.

8. The General Manager must approve official BCVWD social media accounts before being established. The PIO and the assigned social media administrators will manage or post on social media platforms.

PROPOSED POLICY

POLICY TITLE: INTERNET USE AND PERSONAL SOCIAL MEDIA ETHICS POLICY
POLICY NUMBER: 7005

7005.1 Introduction.
Beaumont-Cherry Valley Water District (BCVWD) relies on Information Technology (IT) resources as essential tools for conducting business efficiently and securely. This policy ensures these resources are used responsibly, ethically, 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) to ensure transparency and accountability in public records management.

7005.2 Purpose. The purpose of this policy is to define acceptable use of the internet and social media by BCVWD employees, contractors, and third parties. The policy seeks to protect the District's public image, mitigate cybersecurity risks, and ensure compliance with legal and regulatory requirements.

7005.3 Scope. This policy applies to all employees, contractors, and third parties using District IT resources to access the internet or engage on social media platforms for personal or professional purposes.

7005.4 Policy Details

7005.4.1 Internet Use Guidelines

a. Internet use must align with Policy 7001 Acceptable Use Policy and be limited to activities that directly support District business.
b. Employees should avoid browsing the internet aimlessly. Internet access should be intentional and limited to work-related activities.
c. Employees must not click on suspicious links, respond to phishing attempts, or download content from unverified sources.
d. The district monitors internet usage to protect cybersecurity, detect potential threats, and ensure compliance with this policy. Monitoring will be conducted in accordance with applicable laws and District procedures
e. Use of personal devices on District networks must comply with Policy 7002 Bring Your Own Device and is limited to the guest wi-fi network

7005.4.2 Personal Social Media Guidelines

a. Employees must not represent or speak on behalf of BCVWD on personal social media platforms unless explicitly authorized to do so by the General Manager or his or her designee.
b. Employees must avoid posting content that could give the impression they are speaking on behalf of BCVWD. Employees are encouraged to include a disclaimer such as, "The opinions expressed here are my own and do not reflect the views of BCVWD."
c. Employees must exercise professionalism and discretion when posting on any personal social media, especially when their role with BCVWD could create the perception they are speaking in an official capacity.
d. Employees must not disclose sensitive or confidential District information on personal social media platforms.
e. Employees must take care to avoid any personal social media activity that could be construed as representing BCVWD without explicit authorization. This includes refraining from commenting on District operations, policies, or events in a way that could mislead

9. Content shared on District social media platforms shall comply with Section 5100.6 below. "Content" includes, but is not limited to, posts, shares, comments, likes, intentions, and reactions.

10. While an informal tone is appropriate, communication via social media represents the District and shall remain professional. Official District social media shall not be used for political purposes, conduct private commercial transactions, engage in private business activities, or other personal use. Inappropriate use of official District social media may result in disciplinary action, up to and including termination of employment.

11. *Assigned staff and management shall monitor and evaluate social media platforms on* an ongoing basis.

5100.3 **Personal Use of Social Media.**

Please see Section 7005.4.2

1. District employees and the Board of Directors may have personal accounts on any social media platform of his or her choice. These accounts shall remain private and shall not be used to share work-related information.

2. District employees and the Board of Directors shall avoid using personal accounts to comment on posts regarding official District business.

3. District email accounts and passwords shall not be used with personal social media accounts.

5100.4 **General Policies.**

1. All District accounts shall clearly state they are maintained by the District and include the official logo. The assigned social media administrator will fully understand and comply with user agreements for each social media platform. Administrators will also comply with state and federal regulations and District policies.

2. Social media content shall reflect the District's mission, vision, values, and initiatives. The BCVWD assigned consultant or the assigned social media administrator should monitor social media accounts, content, and conversations on a frequent, ongoing basis. Images may not include photos of a person or private property without written consent.

3. Model releases shall be used to obtain the permission of identifiable people. Images, videos, and graphics that do not belong to the District must be vetted to ensure copyright laws do not protect him or her or that the intended use falls within fair-use standards.

4. The District shall cite the source of any image, graphic, or video not owned by the District. Free-use photos can be found using stock photography sites or advanced search engine features.

5. Social Media accounts, including the administrative account access, shall be established, controlled, and managed by BCVWD Information Technology Department with the direction and approval of the General Manager or his/her designee.

5100.5 **Correcting Misinformation.**

Responding to public comments or questions and diffusing potentially harmful conversations is a critical component of social media management. The social media administrator shall conduct frequent reviews of social media accounts, correct any misinformation, and notify the General Manager or designee immediately in the event

the public.

f. Employees are reminded that privacy settings on personal social media platforms are not foolproof, and posts or interactions may become public or be shared widely. Employees should exercise caution to protect their personal and professional reputation, as well as the District's integrity

7005.4.3 Prohibited Content. As public officials, employees are held to a higher standard of conduct. All District staff are required to adhere to the ethical standards outlined in this policy and all applicable laws. Any misuse of District resources or posting inappropriate content in the employee's personal social media accounts in violation of these standards may result in disciplinary action, up to and including termination of employment (Please refer to the Disciplinary Actions or Terminations policy for more information). Inappropriate content includes, but is not limited to:

a. Violence, profanity, obscenity, nudity, or pornographic content or language,
b. The content is found to discriminate against any creed, race, gender, sexual orientation, age, religion or national origin, as well as any other category protected by state or federal laws,
c. Threats, slander, or defamation of any kind,
d. Illegal acts of any kind or encouragement thereof,
e. Information that compromises the security or well-being of any District staff member, partner, resident or stakeholder,
f. Comments, links, posts, advertisements, or articles soliciting businesses, trade or commerce,
g. Content that violates copyright laws, or
h. Content that violates local, state or federal laws.

7005.4.4 Cybersecurity Measures

a. Employees must adhere to NIST best practices by avoiding insecure websites (e.g., those without HTTPS) and reporting suspicious online activity to the IT Department immediately.
b. All District-provided devices must be equipped with secure browsing tools, such as firewalls and antivirus software, to protect against cybersecurity threats.
c. Employees are responsible for ensuring their internet use does not expose District systems to unnecessary risks, such as malware or data breaches.
d. All District computer systems are equipped with software designed to ensure compliance with safe internet practices and block known malicious websites. However, as cybersecurity threats evolve, employees must remain vigilant. Any suspicious websites, pop-ups, or online activities should be reported immediately to the Information Technology Department for evaluation and mitigation.
e. Employees are expected to stay informed about evolving cybersecurity threats and participate in periodic training provided by the District. Adopting a proactive approach to internet safety, such as verifying website legitimacy and avoiding unfamiliar links, is critical to protecting District systems and data.
f. District computer systems are configured to use encrypted communications (e.g., HTTPS) to secure internet activities. Employees must ensure they do not transmit sensitive District information over unencrypted connections or through insecure platforms.
g. Employees must report any cybersecurity incidents related to internet or social media usage to the Information Technology Department immediately, including unauthorized access attempts, suspicious pop-ups, or phishing messages.
h. Employees are prohibited from using personal email accounts or personal cloud storage services (e.g., Google Drive, Dropbox) for storing, transmitting, or accessing District data unless specifically instructed by the Information Technology Department.
i. The use of cloud-based services for District business must comply with the Cloud

h. Employees are prohibited from using personal email accounts or personal cloud storage services (e.g., Google Drive, Dropbox) for storing, transmitting, or accessing District data unless discussed and authorized by the Information Technology Department.

of an adverse situation. If the situation cannot be resolved, the social media administrator will publicly provide District contact information or other resources and follow up with stakeholders privately regarding his or her concerns.

5100.6 **Content Policies.** Social media content shall be posted consistently, regularly, and with timely and relevant information. Posts shall be scheduled in advance while also allowing flexibility to implement changes and share urgent information quickly and efficiently.

1. Posts can include but are not limited to: emergencies, water supply and conservation information; District updates on initiatives, objectives, and projects; community engagement; leaks, service outages, maintenance/repairs; press releases, holiday closures, and more.
2. Social media administrators shall use the best judgment when posting or engaging on platforms and determining what is suitable to share on behalf of the District. Topics to avoid include legal claims or lawsuits, personnel matters, controversial issues, personal opinions, and political issues.
3. When applicable, content shall be explicitly tailored to each platform's audience and user experience. For example, platforms such as Nextdoor provide an opportunity to engage with a population interested in safety, events, and community. In contrast, platforms such as Instagram provide a way to connect with stakeholders in a fun, visually-based manner. Facebook allows an image with more detail than platforms like Twitter, but both enable linking to additional information.
4. Information shall be relevant to the District's intended audience, presented clearly, and easily understood. Content shall always include proper grammar, spelling, and appropriate tone. The social media administrator will always check facts before posting any information.

5100.7 **Prohibited Content.** Responses from the public that include prohibited content will be removed at the discretion of the General Manager or his/her designee. District staff and representatives of BCVWD who violate this policy and any social media accounts that violate this policy may be subject to disciplinary action, up to and including termination of employment. Content containing any of the following material will be removed immediately. Inappropriate content includes, but is not limited to:

1. Violence, profanity, obscenity, nudity, or pornographic content or language,
2. The content is found to discriminate against any creed, race, gender, sexual orientation, age, religion, or national origin, as well as any other category protected by state or federal laws,
3. Threats, slander, or defamation of any kind,
4. Illegal acts of any kind or encouragement thereof,
5. Information that compromises the security or well-being of any District staff member, partner, resident, or stakeholder,
6. Comments, links, posts, advertisements, or articles soliciting business or commerce,
7. Content that violates copyright laws, or

Please see Section 7005.4.3

Computing Policy and be explicitly approved by the Information Technology Department.

7005.4.5 Public Records Act Compliance

a. All internet and personal social media activities conducted on District-owned devices or networks are subject to the California Public Records Act (CPRA) and may be disclosed upon request.
b. Using personal devices for District business may subject those devices to subpoenas or CPRA requests.
c. To ensure compliance with the CPRA and limit potential exposure to subpoenas, employees must use only District-approved email accounts and cloud resources for all District-related activities. Personal email accounts and unauthorized cloud services are strictly prohibited for District business.

7005.4.6 Training and Awareness

a. BCVWD will provide periodic training to employees on safe internet use, social media best practices, and compliance with this policy. These training sessions will align with the District's Security Awareness and Training Policy to ensure comprehensive employee education on cybersecurity and compliance.
b. Employees are encouraged to report any concerns related to the internet or social media usage to the Information Technology Department.

7005.4.7 Enforcement

a. The IT Department reserves the right to monitor and audit internet and social media activity conducted on District systems to ensure compliance with this policy.

7005.5 Review and Revision Policy. BCVWD will review Policy 7005 Internet Use and Personal Social Media Ethics " annually to ensure it remains current and effective in addressing the needs of the organization and any changes in the regulatory or technological landscape. 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 internet and social media use. Necessary updates or revisions will be made to ensure the policy continues to meet the district's requirements and supports its mission.

8. Content that violates local, state, or federal laws.

5100.8 **Emergency Response.** Social media use shall be limited to the District's PIO, Board President, or as authorized, Board members or designated spokespeople in an emergency or crisis scenario. Social media activities shall occur to announce an emergency, provide updates during the emergency, and share when the emergency is resolved. The District's emergency updates are not intended to take responsibility for emergency communications for regional emergencies; rather, the District will communicate information specifically relating to the District and water service.

5100.9 **State Regulations.** All District content, including social media posts, comments, messages, and other interactions, shall be mindful of and comply with the following state regulations:

1. **California Public Records Act.** All social media content found on BCVWD accounts may be subject to the California Public Records Act. Content posted– including prohibited and non-prohibited content, responses to comments, and messages from the public– shall be monitored, tracked, and retained so that it can be easily retrieved if necessary, according to Public Record Act laws.

2. **Ralph M. Brown Act.** The Brown Act protects the public's right to attend and participate in meetings of local legislative bodies, such as meetings held by a Board of Directors. All Brown Act rules shall be followed when engaging online, including on social media. Interactions between Board members on social media platforms, including comments and messages, can be regarded as a meeting. The Board of Directors is encouraged to follow the Brown Act when engaging in posts or discussions.

3. **Fair Political Practices Commission (FPPC).** The Fair Political Practices Commission (FPPC) is designed to ensure the fairness and integrity of California's political process by enforcing the Political Reform Act. Regulations state that all Board members must be represented equally regarding public outreach, media relations, and social media. Use of pictures, quotes, or other social media content involving Board members must comply with FPPC regulations.

5100.10 **Ongoing Evaluation.** The District shall continuously review social media accounts to ensure alignment with the District Board of Directors' policy direction and District-defined mission, vision, directives, and policies and procedures. District issues identified by staff that are not aligned with the said mission, vision, directives, and policies and procedures shall be corrected, deleted, or adjusted.

5100.11 **Personal Opinion.** The Board of Directors members and District Employees have the right to express an opinion regarding matters of public concern. Members of the Board of Directors and District employees who write correspondence to media or post on social media platforms may not use official district stationary or items symbolizing a direct connection to BCVWD. If a member of the Board of Directors or BCVWD employee identifies as a district representative on a Personal Opinion correspondence, email, or social media posts, he or she shall state that his or her outlined views do not represent the views of the District but of the individual's opinion.

BEAUMONT-CHERRY VALLEY WATER DISTRICT

POLICY TITLE: PRESS RELATIONS AND DISTRICT SOCIAL MEDIA POLICY
POLICY NUMBER: 5100

5100.1 **Purpose.** The purpose of the press relations and social media policy is to work supportively with press relations (media) and to disseminate information of public interest and concern in an accurate, complete, and timely manner. Public Relations and Social Media are vital in outreach efforts that help engage the community quickly and relevantly. It allows stakeholders to communicate with the District and quickly access important information. The District currently manages social media activities across several platforms, such as Facebook, Twitter, and YouTube. This policy will establish clear guidelines for the appropriate use of current policies, which may be updated from time to time and future press relations and social media activities.

5100.2 **Press Relations and Social Media Use.** The District will use press relations and social media to share timely, relevant information that keeps stakeholders up to date on what is happening in the District and with water in his or her community. The goal of social media activity will be to share information about District subjects, events, reminders, District updates, or other District press relations and informal notices. Social media shall also share critical information that needs to reach stakeholders quickly. The use of social media is to complement but not replace other communication methods regarding District activities and business.

1. The General Manager or his/her designee is designated as the District's Public Information Officer (PIO) and is responsible for implementing this policy. When the PIO is unavailable, he or she shall select an authorized designee.

2. The PIO shall coordinate District responses with the Board President to ensure the District meets the Board of Director's communications goals.

3. Employees and elected officials who engage with consumers or members of the Press shall use courtesy, politeness, and professionalism. Any media inquiries received by district staff will be referred immediately to Department Directors or the General Manager (if any Department Director is unavailable), who shall directly forward the media inquiry and contact information to the PIO and Board President (as necessary) for a response.

4. The General Manager, the Board President, or his/her designee will prioritize inquiries from the news media and respond as efficiently as possible.

5. When contacted by the PIO for information needed to respond to a media inquiry, all staff shall provide the PIO with accurate and complete information available for the response. The General Manager or Designee will identify if additional time is needed to address a media inquiry.

6. At the discretion of the PIO and the Board President, if it is determined that a District response is best achieved by having staff or a consultant speak on behalf of the District on a particular topic, he or she may designate an authorized spokesperson to assist with the District's response.

7. To assure that all members of the Board of Directors have accurate, complete, and timely information to fulfill responsibilities to represent the District affairs, members of the Board of Directors shall inform the PIO by email of the substance of significant media inquiries and for an official response.

8. The General Manager or his/her designee must approve official BCVWD social media accounts before being established. The PIO and the assigned social media administrators will manage or post on social media platforms.

9. Content shared on District social media platforms shall comply with Section 5100.6 below. "Content" includes, but is not limited to, posts, shares, comments, likes, intentions, and reactions.

10. While an informal tone is appropriate, communication via social media represents the District and shall remain professional. Official District social media shall not be used for political purposes, conduct private commercial transactions, engage in private business activities, or other personal use. Inappropriate use of official District social media may result in disciplinary action, up to and including termination of employment.

11. Assigned staff and management shall monitor and evaluate social media platforms on an ongoing basis.

~~5100.3 **Personal Use of Social Media.**~~

~~1. District employees and the Board of Directors may have personal accounts on any social media platform of his or her choice. These accounts shall remain private and shall not be used to share work-related information.~~

~~2. District employees and the Board of Directors shall avoid using personal accounts to comment on posts regarding official District business.~~

~~3. District email accounts and passwords shall not be used with personal social media accounts.~~

5100.34 **General Policies.**

1. All District social media accounts shall clearly state they are maintained by the District and include the official logo. The assigned social media administrator will fully understand and comply with user agreements for each social media platform. Administrators will also comply with state and federal regulations and District policies.

2. Social media content shall reflect the District's mission, vision, values, and initiatives. The BCVWD assigned consultant or the assigned social media administrator should monitor social media accounts, content, and conversations on a frequent, ongoing basis. Images may not include photos of a person or private property without written consent.

3. Model releases shall be used to obtain the permission of identifiable people. Images, videos, and graphics that do not belong to the District must be vetted to ensure copyright laws do not protect him or her or that the intended use falls within fair-use standards.

4. The District shall cite the source of any image, graphic, or video not owned by the District. Free-use photos can be found using stock photography sites or advanced search engine features.

5. Social Media accounts, including the administrative account access, shall be established, controlled, and managed by BCVWD Information Technology Department with the direction and approval of the General Manager or his/her designee.

5100.45 **Correcting Misinformation.**

Responding to public comments or questions and diffusing potentially harmful conversations is a critical component of social media management. The social media administrator shall conduct frequent reviews of social

media accounts, correct any misinformation, and notify the General Manager or designee immediately in the event of an adverse situation. If the situation cannot be resolved, the social media administrator will publicly provide District contact information or other resources and follow up with stakeholders privately regarding his or her concerns.

5100.56 **Content Policies.** Social media content shall be posted consistently, regularly, and with timely and relevant information. Posts shall be scheduled in advance while also allowing flexibility to implement changes and share urgent information quickly and efficiently.

1. Posts can include but are not limited to: emergencies; water supply and conservation information; District updates on initiatives, objectives, and projects; community engagement; leaks, service outages, maintenance/repairs; press releases, holiday closures, and more.

2. Social media administrators shall use the best judgment when posting or engaging on platforms and determining what is suitable to share on behalf of the District. Topics to avoid include legal claims or lawsuits, personnel matters, controversial issues, personal opinions, and political issues.

3. When applicable, content shall be explicitly tailored to each platform's audience and user experience. For example, platforms such as Nextdoor provide an opportunity to engage with a population interested in safety, events, and community. In contrast, platforms such as Instagram provide a way to connect with stakeholders in a fun, visually-based manner. Facebook allows an image with more detail than platforms like Twitter, but both enable linking to additional information.

4. Information shall be relevant to the District's intended audience, presented clearly, and easily understood. Content shall always include proper grammar, spelling, and appropriate tone. The social media administrator will always check facts before posting any information.

5100.67 **Prohibited Content.** Responses from the public that include prohibited content will be removed at the discretion of the General Manager or his/her designee. District staff and representatives of BCVWD who violate this policy and any social media accounts that violate this policy may be subject to disciplinary action, up to and including termination of employment (Please rRefer to Policy 3175 Disciplinary Actions or Terminations policy). Content containing any of the following material will be removed immediately. Inappropriate content includes, but is not limited to:

1. Violence, profanity, obscenity, nudity, or pornographic content or language,
2. The content is found to discriminate against any creed, race, gender, sexual orientation, age, religion, or national origin, as well as any other category protected by state or federal laws,
3. Threats, slander, or defamation of any kind,
4. Illegal acts of any kind or encouragement thereof,
5. Information that compromises the security or well-being of any District staff member, partner, resident, or stakeholder,
6. Comments, links, posts, advertisements, or articles soliciting business or commerce,
7. Content that violates copyright laws, or
8. Content that violates local, state, or federal laws.

5100.78 **Emergency Response.** Social media use shall be limited to the District's PIO, Board President, or as authorized, Board members or designated spokespeople in an emergency or crisis scenario. Social media activities shall occur to announce an emergency, provide updates during the emergency, and share when the emergency is resolved. The District's emergency updates are not intended to take responsibility for emergency communications for regional emergencies; rather, the District will communicate information specifically relating to the District and water service.

5100.89 **State and Federal Regulations.** All District content, including social media posts, comments, messages, and other interactions, shall be mindful of and comply with the following state and federal regulations:

1. **California Public Records Act.** All social media content found on BCVWD accounts may be subject to the California Public Records Act. Content posted– including prohibited and non-prohibited content, responses to comments, and messages from the public-- shall be monitored, tracked, and retained so that it can be easily retrieved if necessary, according to Public Record Act laws.

2. **Ralph M. Brown Act.** The Brown Act protects the public's right to attend and participate in meetings of local legislative bodies, such as meetings held by a Board of Directors. All Brown Act rules shall be followed when engaging online, including on social media. Interactions between Board members on social media platforms, including comments and messages, can be regarded as a meeting. The Board of Directors is encouraged to follow the Brown Act when engaging in posts or discussions.

3. **Fair Political Practices Commission (FPPC).** The Fair Political Practices Commission (FPPC) is designed to ensure the fairness and integrity of California's political process by enforcing the Political Reform Act. Regulations state that all Board members must be represented equally regarding public outreach, media relations, and social media. Use of pictures, quotes, or other social media content involving Board members must comply with FPPC regulations.

3.4. **First Amendment of the United States Constitution.** Public officials and employees managing official agency social media accounts shall not block users or delete comments based on viewpoint, criticism, or dissenting opinions, in accordance with First Amendment protections. Blocking or content moderation is permitted only in cases of threats, harassment, or content that violates the agency's established social media guidelines.

5100.910 **Ongoing Evaluation.** The District shall continuously review social media accounts to ensure alignment with the District Board of Directors' policy direction and District-defined mission, vision, directives, and policies and procedures. District issues identified by staff that are not aligned with the said mission, vision, directives, and policies and procedures shall be corrected, deleted, or adjusted.

5100.101 **Personal Opinion.** The Board of Directors members and District Employees have the right to express an opinion regarding matters of public concern. Members of the Board of Directors and District employees who write correspondence to media or post on social media platforms may not use official district stationary or items symbolizing a direct connection to BCVWD. If a member of the Board of Directors or BCVWD employee identifies as a dDistrict representative on a pPersonal oOpinion correspondence, email, or social media posts, he or she shall state that his or her outlined views do not represent the views of the District but of the individual's opinion .(Please sSee Policy 7005 for more information).

BEAUMONT-CHERRY VALLEY WATER DISTRICT

POLICY TITLE: PRESS RELATIONS AND DISTRICT SOCIAL MEDIA POLICY
POLICY NUMBER: 5100

5100.1 **Purpose.** The purpose of the press relations and social media policy is to work supportively with press relations (media) and to disseminate information of public interest and concern in an accurate, complete, and timely manner. Public Relations and Social Media are vital in outreach efforts that help engage the community quickly and relevantly. It allows stakeholders to communicate with the District and quickly access important information. The District currently manages social media activities across several platforms, such as Facebook, Twitter, and YouTube. This policy will establish clear guidelines for the appropriate use of current policies, which may be updated from time to time and future press relations and social media activities.

5100.2 **Press Relations and Social Media Use.** The District will use press relations and social media to share timely, relevant information that keeps stakeholders up to date on what is happening in the District and with water in his or her community. The goal of social media activity will be to share information about District subjects, events, reminders, District updates, or other District press relations and informal notices. Social media shall also share critical information that needs to reach stakeholders quickly. The use of social media is to complement but not replace other communication methods regarding District activities and business.

1. The General Manager or his/her designee is designated as the District's Public Information Officer (PIO) and is responsible for implementing this policy. When the PIO is unavailable, he or she shall select an authorized designee.

2. The PIO shall coordinate District responses with the Board President to ensure the District meets the Board of Director's communications goals.

3. Employees and elected officials who engage with consumers or members of the Press shall use courtesy, politeness, and professionalism. Any media inquiries received by district staff will be referred immediately to Department Directors or the General Manager (if any Department Director is unavailable), who shall directly forward the media inquiry and contact information to the PIO and Board President (as necessary) for a response.

4. The General Manager, the Board President, or his/her designee will prioritize inquiries from the news media and respond as efficiently as possible.

5. When contacted by the PIO for information needed to respond to a media inquiry, all staff shall provide the PIO with accurate and complete information available for the response. The General Manager or Designee will identify if additional time is needed to address a media inquiry.

6. At the discretion of the PIO and the Board President, if it is determined that a District response is best achieved by having staff or a consultant speak on behalf of the District on a particular topic, he or she may designate an authorized spokesperson to assist with the District's response.

7. To assure that all members of the Board of Directors have accurate, complete, and timely information to fulfill responsibilities to represent the District affairs, members of the Board of Directors shall inform the PIO by email of the substance of significant media inquiries and for an official response.

8. The General Manager or his/her designee must approve official BCVWD social media

accounts before being established. The PIO and the assigned social media administrators will manage or post on social media platforms.

9. Content shared on District social media platforms shall comply with Section 5100.6 below. "Content" includes, but is not limited to, posts, shares, comments, likes, intentions, and reactions.

10. While an informal tone is appropriate, communication via social media represents the District and shall remain professional. Official District social media shall not be used for political purposes, conduct private commercial transactions, engage in private business activities, or other personal use. Inappropriate use of official District social media may result in disciplinary action, up to and including termination of employment.

11. Assigned staff and management shall monitor and evaluate social media platforms on an ongoing basis.

5100.3 **General Policies.**

1. All District social media accounts shall clearly state they are maintained by the District and include the official logo. The assigned social media administrator will fully understand and comply with user agreements for each social media platform. Administrators will also comply with state and federal regulations and District policies.

2. Social media content shall reflect the District's mission, vision, values, and initiatives. The BCVWD assigned consultant or the assigned social media administrator should monitor social media accounts, content, and conversations on a frequent, ongoing basis. Images may not include photos of a person or private property without written consent.

3. Model releases shall be used to obtain the permission of identifiable people. Images, videos, and graphics that do not belong to the District must be vetted to ensure copyright laws do not protect him or her or that the intended use falls within fair-use standards.

4. The District shall cite the source of any image, graphic, or video not owned by the District. Free-use photos can be found using stock photography sites or advanced search engine features.

5. Social Media accounts, including the administrative account access, shall be established, controlled, and managed by BCVWD Information Technology Department with the direction and approval of the General Manager or his/her designee.

5100.4 **Correcting Misinformation.**
Responding to public comments or questions and diffusing potentially harmful conversations is a critical component of social media management. The social media administrator shall conduct frequent reviews of social media accounts, correct any misinformation, and notify the General Manager or designee immediately in the event of an adverse situation. If the situation cannot be resolved, the social media administrator will publicly provide District contact information or other resources and follow up with stakeholders privately regarding his or her concerns.

5100.5 **Content Policies.** Social media content shall be posted consistently, regularly, and with timely and relevant information. Posts shall be scheduled in advance while also allowing flexibility to implement changes and share urgent information quickly and efficiently.

1. Posts can include but are not limited to: emergencies; water supply and conservation information; District updates on initiatives, objectives, and projects; community engagement; leaks, service outages, maintenance/repairs; press releases, holiday closures, and more.

2. Social media administrators shall use the best judgment when posting or engaging on platforms and determining what is suitable to share on behalf of the District. Topics to avoid include legal claims or lawsuits, personnel matters, controversial issues, personal opinions, and political issues.

3. When applicable, content shall be explicitly tailored to each platform's audience and user experience. For example, platforms such as Nextdoor provide an opportunity to engage with a population interested in safety, events, and community. In contrast, platforms such as Instagram provide a way to connect with stakeholders in a fun, visually-based manner. Facebook allows an image with more detail than platforms like Twitter, but both enable linking to additional information.

4. Information shall be relevant to the District's intended audience, presented clearly, and easily understood. Content shall always include proper grammar, spelling, and appropriate tone. The social media administrator will always check facts before posting any information.

5100.6 **Prohibited Content.** Responses from the public that include prohibited content will be removed at the discretion of the General Manager or his/her designee. District staff and representatives of BCVWD who violate this policy and any social media accounts that violate this policy may be subject to disciplinary action, up to and including termination of employment (Please refer Policy 3175 Disciplinary Actions or Terminations policy). Content containing any of the following material will be removed immediately. Inappropriate content includes, but is not limited to:

1. Violence, profanity, obscenity, nudity, or pornographic content or language,

2. The content is found to discriminate against any creed, race, gender, sexual orientation, age, religion, or national origin, as well as any other category protected by state or federal laws,

3. Threats, slander, or defamation of any kind,

4. Illegal acts of any kind or encouragement thereof,

5. Information that compromises the security or well-being of any District staff member, partner, resident, or stakeholder,

6. Comments, links, posts, advertisements, or articles soliciting business or commerce,

7. Content that violates copyright laws, or

8. Content that violates local, state, or federal laws.

5100.7 **Emergency Response.** Social media use shall be limited to the District's PIO, Board President, or as authorized, Board members or designated spokespeople in an emergency or crisis scenario. Social media activities shall occur to announce an emergency, provide updates during the emergency, and share when the emergency is resolved. The District's emergency updates are not intended to take responsibility for emergency communications for regional emergencies; rather, the District will communicate information specifically relating to the District and water service.

5100.8 **State and Federal Regulations.** All District content, including social media posts, comments, messages, and other interactions, shall be mindful of and comply with the following state and federal regulations:

1. **California Public Records Act.** All social media content found on BCVWD accounts may be subject to the California Public Records Act. Content posted– including prohibited and non-prohibited content, responses to comments, and messages from the public-- shall be monitored, tracked, and retained so that it can be easily retrieved if necessary, according to Public Record Act laws.

2. **Ralph M. Brown Act.** The Brown Act protects the public's right to attend and participate in meetings of local legislative bodies, such as meetings held by a Board of Directors. All Brown Act rules shall be followed when engaging online, including on social media. Interactions between Board members on social media platforms, including comments and messages, can be regarded as a meeting. The Board of Directors is encouraged to follow the Brown Act when engaging in posts or discussions.

3. **Fair Political Practices Commission (FPPC).** The Fair Political Practices Commission (FPPC) is designed to ensure the fairness and integrity of California's political process by enforcing the Political Reform Act. Regulations state that all Board members must be represented equally regarding public outreach, media relations, and social media. Use of pictures, quotes, or other social media content involving Board members must comply with FPPC regulations.

4. **First Amendment of the United States Constitution**. Public officials and employees managing official agency social media accounts shall not block users or delete comments based on viewpoint, criticism, or dissenting opinions, in accordance with First Amendment protections. Blocking or content moderation is permitted only in cases of threats, harassment, or content that violates the agency's established social media guidelines.

5100.9 **Ongoing Evaluation.** The District shall continuously review social media accounts to ensure alignment with the District Board of Directors' policy direction and District-defined mission, vision, directives, and policies and procedures. District issues identified by staff that are not aligned with the said mission, vision, directives, and policies and procedures shall be corrected, deleted, or adjusted.

5100.10 **Personal Opinion.** The Board of Directors and District Employees have the right to express an opinion regarding matters of public concern. Members of the Board of Directors and District employees who write correspondence to media or post on social media platforms may not use official district stationary or items symbolizing a direct connection to BCVWD. If a member of the Board of Directors or BCVWD employee identifies as a district representative on a Personal Opinion correspondence, email, or social media posts, he or she shall state that his or her outlined views do not represent the views of the District but of the individual's opinion (Please see Policy 7005 for more information).

CURRENT POLICY

POLICY TITLE: PRESS RELATIONS AND SOCIAL MEDIA POLICY
POLICY NUMBER: 5100

5100.1 **Purpose.** The purpose of the press relations and social media policy is to work supportively with press relations (media) and to disseminate information of public interest and concern in an accurate, complete, and timely manner. Public Relations and Social Media are vital in outreach efforts that help engage the community quickly and relevantly. It allows stakeholders to communicate with the District and quickly access important information. The District currently manages social media activities across several platforms, such as Facebook, Twitter, and YouTube. This policy will establish clear guidelines for the appropriate use of current policies, which may be updated from time to time and future press relations and social media activities.

5100.2 **Press Relations and Social Media Use.** The District will use press relations and social media to share timely, relevant information that keeps stakeholders up to date on what is happening in the District and with water in his or her community. The goal of social media activity will be to share information about District subjects, events, reminders, District updates, or other District press relations and informal notices. Social media shall also share critical information that needs to reach stakeholders quickly. The use of social media is to complement but not replace other communication methods regarding District activities and business.

1. The General Manager or his/her designee is designated as the District's Public Information Officer (PIO) and is responsible for implementing this policy. When the PIO is unavailable, he or she shall select an authorized designee.
2. The PIO shall coordinate District responses with the Board President to ensure the District meets the Board of Director's communications goals.
3. Employees and elected officials who engage with consumers or members of the Press shall use courtesy, politeness, and professionalism. Any media inquiries received by district staff will be referred immediately to Department Directors or the General Manager (if any Department Director is unavailable), who shall directly forward the media inquiry and contact information to the PIO and Board President (as necessary) for a response.
4. The General Manager, the Board President, or his/her designee will prioritize inquiries from the news media and respond as efficiently as possible.
5. When contacted by the PIO for information needed to respond to a media inquiry, all staff shall provide the PIO with accurate and complete information available for the response. The General Manager or Designee will identify if additional time is needed to address a media inquiry.
6. At the discretion of the PIO and the Board President, if it is determined that a District response is best achieved by having staff or a consultant speak on behalf of the District on a particular topic, he or she may designate an authorized spokesperson to assist with the District's response.
7. To assure that all members of the Board of Directors have accurate, complete, and timely information to fulfill responsibilities to represent the District affairs, members of the Board of Directors shall inform the PIO by email of the substance of significant media inquiries and for an official response.
8. The General Manager must approve official BCVWD social media accounts before being established. The PIO and the assigned social media administrators will manage or post on social media platforms.

PROPOSED POLICY

POLICY TITLE: PRESS RELATIONS AND DISTRICT SOCIAL MEDIA POLICY
POLICY NUMBER: 5100

5100.1 **Purpose.** The purpose of the press relations and social media policy is to work supportively with press relations (media) and to disseminate information of public interest and concern in an accurate, complete, and timely manner. Public Relations and Social Media are vital in outreach efforts that help engage the community quickly and relevantly. It allows stakeholders to communicate with the District and quickly access important information. The District currently manages social media activities across several platforms, such as Facebook, Twitter, and YouTube. This policy will establish clear guidelines for the appropriate use of current policies, which may be updated from time to time and future press relations and social media activities.

5100.2 **Press Relations and Social Media Use.** The District will use press relations and social media to share timely, relevant information that keeps stakeholders up to date on what is happening in the District and with water in his or her community. The goal of social media activity will be to share information about District subjects, events, reminders, District updates, or other District press relations and informal notices. Social media shall also share critical information that needs to reach stakeholders quickly. The use of social media is to complement but not replace other communication methods regarding District activities and business.

1. The General Manager or his/her designee is designated as the District's Public Information Officer (PIO) and is responsible for implementing this policy. When the PIO is unavailable, he or she shall select an authorized designee.
2. The PIO shall coordinate District responses with the Board President to ensure the District meets the Board of Director's communications goals.
3. Employees and elected officials who engage with consumers or members of the Press shall use courtesy, politeness, and professionalism. Any media inquiries received by district staff will be referred immediately to Department Directors or the General Manager (if any Department Director is unavailable), who shall directly forward the media inquiry and contact information to the PIO and Board President (as necessary) for a response.
4. The General Manager, the Board President, or his/her designee will prioritize inquiries from the news media and respond as efficiently as possible.
5. When contacted by the PIO for information needed to respond to a media inquiry, all staff shall provide the PIO with accurate and complete information available for the response. The General Manager or Designee will identify if additional time is needed to address a media inquiry.
6. At the discretion of the PIO and the Board President, if it is determined that a District response is best achieved by having staff or a consultant speak on behalf of the District on a particular topic, he or she may designate an authorized spokesperson to assist with the District's response.
7. To assure that all members of the Board of Directors have accurate, complete, and timely information to fulfill responsibilities to represent the District affairs, members of the Board of Directors shall inform the PIO by email of the substance of significant media inquiries and for an official response.
8. The General Manager or his/her designee must approve official BCVWD social media accounts before being established. The PIO and the assigned social media administrators will manage or post on social

9. Content shared on District social media platforms shall comply with Section 5100.6 below. "Content" includes, but is not limited to, posts, shares, comments, likes, intentions, and reactions.

10. While an informal tone is appropriate, communication via social media represents the District and shall remain professional. Official District social media shall not be used for political purposes, conduct private commercial transactions, engage in private business activities, or other personal use. Inappropriate use of official District social media may result in disciplinary action, up to and including termination of employment.

11. Assigned staff and management shall monitor and evaluate social media platforms on an ongoing basis.

5100.3 **Personal Use of Social Media.**

1. District employees and the Board of Directors may have personal accounts on any social media platform of his or her choice. These accounts shall remain private and shall not be used to share work-related information.

2. District employees and the Board of Directors shall avoid using personal accounts to comment on posts regarding official District business.

3. District email accounts and passwords shall not be used with personal social media accounts.

5100.4 **General Policies.**

1. All District accounts shall clearly state they are maintained by the District and include the official logo. The assigned social media administrator will fully understand and comply with user agreements for each social media platform. Administrators will also comply with state and federal regulations and District policies.

2. Social media content shall reflect the District's mission, vision, values, and initiatives. The BCVWD assigned consultant or the assigned social media administrator should monitor social media accounts, content, and conversations on a frequent, ongoing basis. Images may not include photos of a person or private property without written consent.

3. Model releases shall be used to obtain the permission of identifiable people. Images, videos, and graphics that do not belong to the District must be vetted to ensure copyright laws do not protect him or her or that the intended use falls within fair-use standards.

4. The District shall cite the source of any image, graphic, or video not owned by the District. Free-use photos can be found using stock photography sites or advanced search engine features.

5. Social Media accounts, including the administrative account access, shall be established, controlled, and managed by BCVWD Information Technology Department with the direction and approval of the General Manager or his/her designee.

5100.5 **Correcting Misinformation.**

Responding to public comments or questions and diffusing potentially harmful conversations is a critical component of social media management. The social media administrator shall conduct frequent reviews of social media accounts, correct any misinformation, and notify the General Manager or designee immediately in the event

media platforms.

9. Content shared on District social media platforms shall comply with Section 5100.6 below. "Content" includes, but is not limited to, posts, shares, comments, likes, intentions, and reactions.

10. While an informal tone is appropriate, communication via social media represents the District and shall remain professional. Official District social media shall not be used for political purposes, conduct private commercial transactions, engage in private business activities, or other personal use. Inappropriate use of official District social media may result in disciplinary action, up to and including termination of employment.

11. Assigned staff and management shall monitor and evaluate social media platforms on an ongoing basis.

~~5100.3 **Personal Use of Social Media.**~~

~~1. District employees and the Board of Directors may have personal accounts on any social media platform of his or her choice. These accounts shall remain private and shall not be used to share work-related information.~~

~~2. District employees and the Board of Directors shall avoid using personal accounts to comment on posts regarding official District business.~~

~~3. District email accounts and passwords shall not be used with personal social media accounts.~~

5100.34 **General Policies.**

1. All District social media accounts shall clearly state they are maintained by the District and include the official logo. The assigned social media administrator will fully understand and comply with user agreements for each social media platform. Administrators will also comply with state and federal regulations and District policies.

2. Social media content shall reflect the District's mission, vision, values, and initiatives. The BCVWD assigned consultant or the assigned social media administrator should monitor social media accounts, content, and conversations on a frequent, ongoing basis. Images may not include photos of a person or private property without written consent.

3. Model releases shall be used to obtain the permission of identifiable people. Images, videos, and graphics that do not belong to the District must be vetted to ensure copyright laws do not protect him or her or that the intended use falls within fair-use standards.

4. The District shall cite the source of any image, graphic, or video not owned by the District. Free-use photos can be found using stock photography sites or advanced search engine features.

5. Social Media accounts, including the administrative account access, shall be established, controlled, and managed by BCVWD Information Technology Department with the direction and approval of the General Manager or his/her designee.

5100.45 **Correcting Misinformation.**

of an adverse situation. If the situation cannot be resolved, the social media administrator will publicly provide District contact information or other resources and follow up with stakeholders privately regarding his or her concerns.

5100.6 **Content Policies.** Social media content shall be posted consistently, regularly, and with timely and relevant information. Posts shall be scheduled in advance while also allowing flexibility to implement changes and share urgent information quickly and efficiently.

1. Posts can include but are not limited to: emergencies; water supply and conservation information; District updates on initiatives, objectives, and projects; community engagement; leaks, service outages, maintenance/repairs; press releases, holiday closures, and more.

2. Social media administrators shall use the best judgment when posting or engaging on platforms and determining what is suitable to share on behalf of the District. Topics to avoid include legal claims or lawsuits, personnel matters, controversial issues, personal opinions, and political issues.

3. When applicable, content shall be explicitly tailored to each platform's audience and user experience. For example, platforms such as Nextdoor provide an opportunity to engage with a population interested in safety, events, and community. In contrast, platforms such as Instagram provide a way to connect with stakeholders in a fun, visually-based manner. Facebook allows an image with more detail than platforms like Twitter, but both enable linking to additional information.

4. Information shall be relevant to the District's intended audience, presented clearly, and easily understood. Content shall always include proper grammar, spelling, and appropriate tone. The social media administrator will always check facts before posting any information.

5100.7 **Prohibited Content.** Responses from the public that include prohibited content will be removed at the discretion of the General Manager or his/her designee. District staff and representatives of BCVWD who violate this policy and any social media accounts that violate this policy may be subject to disciplinary action, up to and including termination of employment. Content containing any of the following material will be removed immediately. Inappropriate content includes, but is not limited to:

1. Violence, profanity, obscenity, nudity, or pornographic content or language,

2. The content is found to discriminate against any creed, race, gender, sexual orientation, age, religion, or national origin, as well as any other category protected by state or federal laws,

3. Threats, slander, or defamation of any kind,

4. Illegal acts of any kind or encouragement thereof,

5. Information that compromises the security or well-being of any District staff member, partner, resident, or stakeholder,

6. Comments, links, posts, advertisements, or articles soliciting business or commerce,

7. Content that violates copyright laws, or

Responding to public comments or questions and diffusing potentially harmful conversations is a critical component of social media management. The social media administrator shall conduct frequent reviews of social media accounts, correct any misinformation, and notify the General Manager or designee immediately in the event of an adverse situation. If the situation cannot be resolved, the social media administrator will publicly provide District contact information or other resources and follow up with stakeholders privately regarding his or her concerns.

5100.~~56~~ **Content Policies.** Social media content shall be posted consistently, regularly, and with timely and relevant information. Posts shall be scheduled in advance while also allowing flexibility to implement changes and share urgent information quickly and efficiently.

1. Posts can include but are not limited to: emergencies; water supply and conservation information; District updates on initiatives, objectives, and projects; community engagement; leaks, service outages, maintenance/repairs; press releases, holiday closures, and more.

2. Social media administrators shall use the best judgment when posting or engaging on platforms and determining what is suitable to share on behalf of the District. Topics to avoid include legal claims or lawsuits, personnel matters, controversial issues, personal opinions, and political issues.

3. When applicable, content shall be explicitly tailored to each platform's audience and user experience. For example, platforms such as Nextdoor provide an opportunity to engage with a population interested in safety, events, and community. In contrast, platforms such as Instagram provide a way to connect with stakeholders in a fun, visually-based manner. Facebook allows an image with more detail than platforms like Twitter, but both enable linking to additional information.

4. Information shall be relevant to the District's intended audience, presented clearly, and easily understood. Content shall always include proper grammar, spelling, and appropriate tone. The social media administrator will always check facts before posting any information.

5100.~~67~~ **Prohibited Content.** Responses from the public that include prohibited content will be removed at the discretion of the General Manager or his/her designee. District staff and representatives of BCVWD who violate this policy and any social media accounts that violate this policy may be subject to disciplinary action, up to and including termination of employment (Please refer to Policy 3175 Disciplinary Actions or Terminations). Content containing any of the following material will be removed immediately. Inappropriate content includes, but is not limited to:

1. Violence, profanity, obscenity, nudity, or pornographic content or language,

2. The content is found to discriminate against any creed, race, gender, sexual orientation, age, religion, or national origin, as well as any other category protected by state or federal laws,

3. Threats, slander, or defamation of any kind,

4. Illegal acts of any kind or encouragement thereof,

5. Information that compromises the security or well-being of any District staff member, partner, resident, or stakeholder,

8. Content that violates local, state, or federal laws.

5100.8 **Emergency Response.** Social media use shall be limited to the District's PIO, Board President, or as authorized, Board members or designated spokespeople in an emergency or crisis scenario. Social media activities shall occur to announce an emergency, provide updates during the emergency, and share when the emergency is resolved. The District's emergency updates are not intended to take responsibility for emergency communications for regional emergencies; rather, the District will communicate information specifically relating to the District and water service.

5100.9 **State Regulations.** All District content, including social media posts, comments, messages, and other interactions, shall be mindful of and comply with the following state regulations:

1. **California Public Records Act.** All social media content found on BCVWD accounts may be subject to the California Public Records Act. Content posted– including prohibited and non-prohibited content, responses to comments, and messages from the public-- shall be monitored, tracked, and retained so that it can be easily retrieved if necessary, according to Public Record Act laws.

2. **Ralph M. Brown Act.** The Brown Act protects the public's right to attend and participate in meetings of local legislative bodies, such as meetings held by a Board of Directors. All Brown Act rules shall be followed when engaging online, including on social media. Interactions between Board members on social media platforms, including comments and messages, can be regarded as a meeting. The Board of Directors is encouraged to follow the Brown Act when engaging in posts or discussions.

3. **Fair Political Practices Commission (FPPC).** The Fair Political Practices Commission (FPPC) is designed to ensure the fairness and integrity of California's political process by enforcing the Political Reform Act. Regulations state that all Board members must be represented equally regarding public outreach, media relations, and social media. Use of pictures, quotes, or other social media content involving Board members must comply with FPPC regulations.

5100.10 **Ongoing Evaluation.** The District shall continuously review social media accounts to ensure alignment with the District Board of Directors' policy direction and District-defined mission, vision, directives, and policies and procedures. District issues identified by staff that are not aligned with the said mission, vision, directives, and policies and procedures shall be corrected, deleted, or adjusted.

5100.11 **Personal Opinion.** The Board of Directors members and District Employees have the right to express an opinion regarding matters of public concern. Members of the Board of Directors and District employees who write correspondence to media or post on social media platforms may not use official district stationary or items symbolizing a direct connection to BCVWD. If a member of the Board of Directors or BCVWD employee identifies as a district representative on a Personal Opinion correspondence, email, or social media posts, he or she shall state that his or her outlined views do not represent the views of the District but of the individual's opinion.

6. Comments, links, posts, advertisements, or articles soliciting business or commerce,

7. Content that violates copyright laws, or

8. Content that violates local, state, or federal laws.

5100.~~7~~8 **Emergency Response.** Social media use shall be limited to the District's PIO, Board President, or as authorized, Board members or designated spokespeople in an emergency or crisis scenario. Social media activities shall occur to announce an emergency, provide updates during the emergency, and share when the emergency is resolved. The District's emergency updates are not intended to take responsibility for emergency communications for regional emergencies; rather, the District will communicate information specifically relating to the District and water service.

5100.~~8~~9 **State and Federal Regulations.** All District content, including social media posts, comments, messages, and other interactions, shall be mindful of and comply with the following state regulations:

1. **California Public Records Act.** All social media content found on BCVWD accounts may be subject to the California Public Records Act. Content posted– including prohibited and non-prohibited content, responses to comments, and messages from the public– shall be monitored, tracked, and retained so that it can be easily retrieved if necessary, according to Public Record Act laws.

2. **Ralph M. Brown Act.** The Brown Act protects the public's right to attend and participate in meetings of local legislative bodies, such as meetings held by a Board of Directors. All Brown Act rules shall be followed when engaging online, including on social media. Interactions between Board members on social media platforms, including comments and messages, can be regarded as a meeting. The Board of Directors is encouraged to follow the Brown Act when engaging in posts or discussions.

3. **Fair Political Practices Commission (FPPC).** The Fair Political Practices Commission (FPPC) is designed to ensure the fairness and integrity of California's political process by enforcing the Political Reform Act. Regulations state that all Board members must be represented equally regarding public outreach, media relations, and social media. Use of pictures, quotes, or other social media content involving Board members must comply with FPPC regulations.

~~3.~~4. **First Amendment of the United States Constitution**. Public officials and employees managing official agency social media accounts shall not block users or delete comments based on viewpoint, criticism, or dissenting opinions, in accordance with First Amendment protections. Blocking or content moderation is permitted only in cases of threats, harassment, or content that violates the agency's established social media guidelines.

5100.~~9~~10 **Ongoing Evaluation.** The District shall continuously review social media accounts to ensure alignment with the District Board of Directors' policy direction and District-defined mission, vision, directives, and policies and procedures. District issues identified by staff that are not aligned with the said mission, vision, directives, and policies and procedures shall be corrected, deleted, or adjusted.

5100.~~10~~1 **Personal Opinion.** The Board of Directors ~~members~~ and District Employees have the right to express an opinion regarding matters of public concern. Members of the Board of Directors and District employees who write correspondence to media or post on social media platforms may not use official district stationary or items symbolizing a direct connection to BCVWD. If a member of the Board of Directors or BCVWD employee identifies as a district representative on a Personal Opinion correspondence, email, or social media posts, he or she shall state that his or her outlined views do not represent the views of the District but of the individual's opinion. (Please see Policy 7005 for more information).

Beaumont-Cherry Valley Water District
Personnel Committee Meeting
March 18, 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	4	1	3.85%
Engineering[2]	8	8	1	1	12.50%
Finance	15	15	8	8	53.33%
Human Resources	**70**	**70**	**70**	**70**	**100%**
Information Technology[3]	17	17	6	3	17.64%
TOTALS	**136**	**132**	**89**	**83**	**61.03%**

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] 17 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	7003	Cloud Computing (policy)	2 pages	March	April
2	7007	Remote Access	2 pages	March	April
3	7018	Wireless Network Security	2 pages	March	April

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
	1000	General	*Definitions*	Human Resources	Yes	6/28/2021	7/19/2021	7/20/2021	10/13/2021	10/13/2021	10/13/2021	21-018
2	1005	General	Contractual Provisions	Human Resources	Yes	2/16/2021	2/22/2021	2/22/2021	4/14/2021	4/14/2021	4/14/2021	21-006
	1010	General	Policy Manual	Human Resources	Yes	N/A	N/A	N/A	1/8/2025	1/8/2025	1/8/2025	25-001
3	2000	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
5	2010	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	21-006
6	2015	Personnel	Harassment	Human Resources	Yes	1/2/2024	1/16/2024	1/16/2024	2/14/2024	2/14/2024	2/14/2024	24-006
7	2020	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
N/A	2025	Administration	Whistleblower Protection	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	Employee Status	Human Resources	Yes	4/12/2021	7/19/2021	7/20/2021	10/13/2021	10/13/2021	10/13/2021	21-018
N/A	3001	Personnel	Employee Information and Emergency	Human Resources	Yes	4/12/2021	6/21/2021	6/21/2021	10/13/2021	10/13/2021	10/13/2021	21-018
N/A	3002	Personnel	Employee Groups	Human Resources	Yes	4/12/2021	5/17/2021	5/17/2021	10/13/2021	10/13/2021	10/13/2021	21-018
9	3005	Personnel	Compensation	Human Resources	Yes	7/13/2021	7/19/2021	7/20/2021	10/13/2021	10/13/2021	10/13/2021	21-018
N/A	3006	Personnel	~~Prevailing Wage~~ Public Works Contractor-	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	Employee Performance Evaluation	Human Resources	Yes	7/13/2021	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	12/10/2021	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	11/21/2024	1/8/2025	1/8/2025	1/8/2025	25-001
18	3050	Personnel	Volunteer Personnel Workers'	Human Resources	Yes	5/2/2024	6/18/2024	7/16/2024	8/14/2024	8/14/2024	8/14/2024	24-012
19	3055	Personnel	Work Hours, Overtime, and Standby	Human Resources	Yes	6/14/2022	7/19/2022	7/19/2022	9/14/2022	9/14/2022	9/14/2022	22-028
20	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
20 (incorrect)	3065	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
21	3070	Personnel	Holidays	Human Resources	Yes	1/2/2024	1/16/2024	1/16/2024	2/14/2024	2/14/2024	2/14/2024	24-002
22	3075	Personnel	Vacation	Human Resources	Yes	11/8/2022	1/17/2023	1/17/2023	2/8/2023	2/8/2023	2/8/2023	23-005
24	3085	Personnel	Sick Leave	Human Resources	Yes	4/8/2024	1/16/2024	4/16/2024	5/16/2024	5/16/2024	5/16/2024	24-007
25	3090	Personnel	Family and Medical Leave	Human Resources	Yes	10/2/2024	11/21/2024	11/21/2024	1/8/2025	1/8/2025	1/8/2025	25-001
26	3095	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	3096	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	3100	Personnel	Bereavement Leave	Human Resources	Yes	5/10/2022	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	2/18/2025	2/18/2025	3/11/2025	3/11/2025	3/11/2025	
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	23-005
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	23-005
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	23-009
N/A	3122	Personnel	Workplace Violence	Human Resources	Yes	1/2/2024	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	Human Resources	Yes	6/29/2024	7/16/2024	8/20/2024	9/17/2024	9/17/2024	9/17/2024	24-014
34	3135	Personnel	Occupational Certification and	Human Resources	Yes	6/14/2022	8/16/2022	8/16/2022	9/17/2022	9/17/2022	9/14/2022	22-028
N/A	3136	Personnel	Succession and Workforce Planning	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	11/19/2024	1/21/2025	2/12/2025	2/12/2025	2/12/2025	25-004
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		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	Nepotism-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
51	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	Human Resources	Yes	2019	2019	2019	10/9/2019	10/9/2019	10/9/2019	19-011
N/A	3230	Personnel	Workers' Compensation	Human Resources	Yes	5/9/2023	5/16/2023	5/16/2023	6/14/2023	6/14/2023	6/14/2023	23-017
N/A	3231	Personnel	Accommodations for Disablity	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	Direct to Board (Ad Hoc?)				
2	4010	Board of Directors	Members of the Board of Directors	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
3	4015	Board of Directors	Committees of the Board of Directors	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
4	4020	Board of Directors	Board President	Administration	Yes		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 Agendas	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
7	4035	Board of Directors	Board Meeting Conduct and Decorum	Administration	Yes	N/A	1/13/2025	1/13/2025	1/23/2025	1/23/2025	1/23/2025	25-002
8	4040	Board of Directors	Board Actions and Decisions	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
9	4045	Board of Directors	Attendance at Meetings	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
10	4050	Board of Directors	Minutes of Board Meetings	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
11	4055	Board of Directors	Rules of Order for Board and	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
12	4060	Board of Directors	Training, Education and Conferences	Administration	Yes	6/30/2021	N/A	Directed to Full Board	7/14/2021	7/14/2021	7/14/2021	21-012
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	Revisions Requested on	7/14/2021	21-012
14	4070	Board of Directors	Payment of Expenses Incurred on	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
15	4075	Board of Directors	Expenditure Reimbursement	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
17	4080	Board of Directors	Membership in Associations	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
18	4085	Board of Directors	Ethics Training	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
19	4090	Board of Directors	Code of Ethics	Administration	Yes		N/A	Direct to Board (Ad Hoc?)				
20	4095	Board of Directors	Ethics Policy	Administration	Yes		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	Personnel	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	Personnel	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	Personnel	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	Direct to Full Board				
8	5040	Operations	Fixed-Asset Capitalization	Finance	Yes		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	8/1/2024	8/1/2024	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	Alternative Payment Plans	Finance	Yes	11/25/2024	12/5/2024	1/2/2025	1/8/2025	1/8/2025	1/8/2025	25-001
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		8/1/2024					

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
17	5080	Operations	Purchasing	Finance	Yes		N/A	Direct to Full Board				
18	5085	Operations	Disposal of Surplus Property or	Finance	Yes	11/27/2024	12/5/2024	12/5/2024	1/8/2025	1/8/2025	1/8/2025	25-001
19	5090	Operations	Records Retention	Administration	Yes	4/28/2023	4/18/2023	5/16/2023	6/14/2023	6/14/2023	6/14/2023	23-017
N/A	5095	Operations	District Residences and Facility	Human Resources	Yes	7/21/2020	6/21/2021	Requested edits, sent to	Requested Edits	10/28/2021	10/28/2021	21-019
3	6015	Miscellaneous	Public Complaints	Human Resources	Yes	N/A	N/A	N/A	1/8/2025	1/8/2025	1/8/2025	25-001
4	5110	Miscellaneous	Claims Against the District	Finance	Yes	11/15/2023	11/7/2024	11/7/2024	1/8/2025	1/8/2025	1/8/2025	25-001
6	5115	Engineering	District Standards for the Furnishing of	Engineering	Yes		N/A	Direct to Full Board				
7	5120	Miscellaneous	Environmental Review Guidelines	Engineering	Yes		N/A	Direct to Full Board				
8	5125	Miscellaneous	Annexation	Engineering	Yes		N/A	Direct to Full Board				
9	5130	Miscellaneous	Construction Requirements	Engineering	Yes		N/A	Direct to Full Board				
5	6025	Miscellaneous	Public Documents and Public Records	Administration	Yes	4/28/2023	4/18/2023	5/16/2023	6/14/2023	6/14/2023	6/14/2023	23-017
N/A	6020	Miscellaneous	Copying Public Documents	Administration	Yes		N/A	Direct to Full Board				
N/A	7001	Information Technology	Acceptable Use Policy	IT/Personnel	Yes	1/26/2025	3/11/2025					
N/A	7002	Information Technology	Bring Your Own Device (BYOD) Policy	IT/Personnel	Yes	1/26/2025	3/11/2025					
N/A	7003	Information Technology	Cloud Computing Policy	IT/Personnel	Yes	3/10/2025						
N/A	7004	Information Technology	Email and Communication Policy	IT/Personnel	Yes	1/2/2025	1/21/2025	1/21/2025	2/27/2025	2/27/2025	2/27/2025	25-007
N/A	7005	Information Technology	Internet and Social Media Policy	IT/Personnel	Yes	1/26/2025	3/11/2025					
N/A	7006	Information Technology	Password Policy	IT/Personnel	Yes	1/2/2025	1/21/2025	1/21/2025	2/27/2025	2/27/2025	2/27/2025	25-007
N/A	7007	Information Technology	Remote Access Policy	IT/Personnel	Yes	3/10/2025						
N/A	7008	Information Technology	Wireless Network Security Policy	IT/Personnel	Yes	3/10/2025						
N/A	7009	Information Technology	Drone Use Policy	IT/Personnel	Yes							
N/A	7010	Information Technology	Electronic Signature Policy	IT/Personnel	Yes							
N/A	7011	Information Technology	Cellular Telephone Usage Policy	IT/Personnel	Yes	1/2/2025	1/21/2025	1/21/2025	2/27/2025	2/27/2025	2/27/2025	25-007
N/A	7012	Information Technology	Accessibility Policy	IT/Personnel	Yes							
N/A	7013	Information Technology	Personally Identifiable Information (PII)	IT/Personnel	Yes							
N/A	7014	Information Technology	Artificial Intelligence (AI) Policy	IT/Personnel	Yes							
N/A	7015	Information Technology	Security Awareness and Training Policy	IT/Personnel	Yes	N/A	1/21/2025					
N/A	7016	Information Technology	IoT (Internet of Things) Security Policy	IT/Personnel	Yes							
10	5135	Miscellaneous	District Responsibility for Soil	Engineering	No		N/A	Direct to Full Board				
N/A	7017	Information Technology	Non-IT Approved Software Purchasing	IT/Personnel	Yes							

Color Code
Present to Committee
Present to Board
Removed
Slated for Committee
Tabled or Lost
Added to Matrix

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