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, April 15, 2025 - 4:30 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 – APRIL 15, 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. **Report / Update from BCVWD Employees Association** (no staff report)

Association Representatives		
Andrew Becerra	Luis Lomeli	Ericka Enriquez

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

4. **Human Resources Department Report** (pages 4 - 5)

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

a.	Policy 7003	Cloud Computing Policy	pages 6 - 16
b.	Policy 7005	Internet Use and Personal Social Media Ethics	pages 17 - 35

6. **Update on Policy Tracking Matrix** (page 36)
   a. Status of Policy Revisions / Updates

7. **Action List for Future Meetings**
   a. Human Resources and Risk Management Quarterly Report (Jan-Mar 2025)

8. 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)).

HUMAN RESOURCES REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: **Human Resources Report for the Month of March 2025**

Table 1: Personnel

The below table represents the District's current Workforce.

As of March 31, 2025

Total Current Employees (Excluding Board Members)	47
Full-Time Employees	44
Part-Time	1
Temporary	2
Interns	0
Separations	0
Retired Employee(s)	0

Table 2: New Hires

The table below represents new hires.

As of March 31, 2025

Employee Name	Job Title	Department
None		

Table 3: Anniversaries*

The table below represents BCVWD employee anniversaries.

As of March 31, 2025

Employee Name	Department	Years of Service
Jonathan Medina	Operations	20 years
Daniel K. Jaggers	Executive Officer	13 years
Khalid Sebai	Engineering	1 year
Ceejay Stafford	Finance and Administration	1 year

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

Table 4: Promotions or Division/Title Change

The table below represents promotions or Division/Title Changes.

As of March 31, 2025

Employee Name	Former Title	Changed to
Andrew Vara	Temporary Water Utility Worker I	Regular Water Utility Worker I
Omar Garcia-Zamora	Temporary Water Utility Worker I	Regular Water Utility Worker I

Table 5: Recruitment

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

As of March 31, 2025

Position	Department	Update
Customer Service Representative I	Finance and Administration	Candidate Onboarding as of March 17, 2025

Table 6: Separation/Retirement

The table below represents employees separating from BCVWD.

As of March 31, 2025

Employee Name	Position Held	Department	Last Day
None			

Table 7: Communications

The table below represents HR communications to BCVWD employees.

As of March 31, 2025

Communication	Topic
HR Memo 25-009 Defensive Driving Class – April 3, 2025	Safety
HR Memo 25-010 Upcoming Employee Benefits Survey – Action Required	Benefits

Staff Report Prepared by Ren Berioso, Human Resources Manager

Beaumont-Cherry Valley Water District
Personnel Committee
April 15, 2025

Item 5a

STAFF REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: **Policies and Procedures Manual Updates / Revisions establishing Information Technology Policy 7003 Cloud Computing Policy**

Staff Recommendation

Recommend the Information Technology (IT) Policy 7003 Cloud Computing Policy to move forward to the next Board of Directors meeting, or direct staff as desired.

Executive Summary

Staff proposes IT Policy 7003 Cloud Computing Policy to establish clear guidelines and security requirements for the use of cloud-based services and hosted applications at Beaumont-Cherry Valley Water District (BCVWD). It ensures that all cloud service providers (CSPs) are vetted, authorized, and compliant with NIST standards, state regulations, and the California Public Records Act. The proposed policy promotes secure, ethical, and responsible use of cloud technologies to protect District data and support transparency, accountability, and operational efficiency.

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 MISAC award for excellence in IT governance for the past two years.

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

Discussion

The Cloud Computing Policy is significant as it safeguards the integrity, security, and compliance of BCVWD's cloud-based systems by ensuring all services are vetted, approved, and aligned with cybersecurity best practices. It also upholds transparency and accountability by enforcing adherence to state regulations, including the California Public Records Act.

Table 1, Summary of Policy Sections, outlines the proposed Cloud Computing Policy that was drafted by HR and IT Departments.

Table 1 – Summary of Policy Sections

TABLE 1	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	**No Section**	**NIST and CPRA**	BCVWD uses secure IT systems, follows NIST standards, and complies with CPRA to ensure transparency and data protection.	**Consider establishing Section 7003.1** Introduction	No fiscal impact.
2	**No Section**	**NIST**	The IT Department ensures that all cloud services and providers used by BCVWD are properly vetted, authorized, and secured in compliance with District standards.	**Consider establishing Section 7003.2** Purpose	No fiscal impact.
3	**No Section**	**NIST**	This policy applies to all employees, contractors, and third parties who use or manage cloud services that store, process, or transmit District data.	**Consider establishing Section 7003.3** Scope	No fiscal impact.
4	**No Section**	**NIST**	All cloud-based systems are pre-approved by the IT Department, supported by a business justification, and formalized through agreements that define data protection, access, and breach notification requirements	**Consider establishing Sections 7003.4.1.a to c** Policy Details	No fiscal impact.

TABLE 1	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
5	**No Section**	**NIST**	Cloud service providers meet NIST security standards, undergo a risk assessment, encrypt data, enable MFA, support audit functions, disclose data storage locations, and provide security certifications, with BCVWD reserving the right to review compliance	**Consider establishing Sections 7003.4.2.a to g** Security and Risk Management	No fiscal impact.
6	**No Section**	**NIST and CPRA**	BCVWD retains full ownership of its cloud data, which must be returned and securely deleted upon contract termination, remain compliant with CPRA and state laws, and not be used by providers for analytics, profiling, or marketing.	**Consider establishing Sections 7003.4.3.a to d** Data Ownership and Compliance	No fiscal impact.
7	**No Section**	**NIST**	Cloud service providers offer SLAs covering performance and breach response, obtain written approval for subcontracting, and maintain an incident response plan with prompt notification of security incidents.	**Consider establishing Sections 7003.4.4.a to b** Vendor Requirements and Service Level Agreements (SLAs)	No fiscal impact.

TABLE 1	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
8	**No Section**	**NIST**	Employees must use only IT-approved cloud platforms, avoid unauthorized services, and promptly report any suspected cloud-related security incidents to the IT Department.	**Consider establishing Sections 7003.4.5.a to c** Employee Responsibilities	No fiscal impact.
9	**No Section**	**NIST**	The IT Department reviews IT policies annually to ensure its effectiveness, regulatory compliance, alignment with NIST standards, and relevance to the District's evolving needs, making updates as necessary.	**Consider establishing Sections 7003.5** Review and Revision Policy	No fiscal impact.

Fiscal Impact

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

Attachment/s

1. Proposed new Policy 7003: Cloud Computing Policy
2. NIST: Understanding the Cybersecurity Framework
3. California Public Records Act FAQs

Staff Report prepared by Ren Berioso, Human Resources Manager

POLICY TITLE: CLOUD COMPUTING POLICY
POLICY NUMBER: 7003

7003.1 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.

7003.2 Purpose . The purpose of this policy is to establish guidelines and security requirements for the use of cloud-based services and hosted applications. It is designed to ensure that all Cloud Service Providers (CSPs) and systems used by BCVWD are vetted, authorized, and managed in accordance with District security and compliance standards.

7003.3 Scope. This policy applies to all BCVWD employees, contractors, and third parties who use or manage cloud services that store, process, or transmit District data. It also applies to any vendor or consultant providing hosted solutions or cloud-based services to the District.

7003.4 Policy Details

7003.4.1 Cloud Service Approval and Procurement

a. All cloud-based systems must be reviewed and approved by the Information Technology Department prior to procurement or use.
b. Departments must submit a business justification and needs assessment for cloud services.
c. Approved cloud vendors must enter into formal agreements with BCVWD, including clear terms on data protection, access, and breach notification.

7003.4.2 Security and Risk Management

a. Personal devices such as cellphones, a Cloud vendors must meet minimum NIST security standards (e.g., NIST SP 800-53 or equivalent).
b. A third-party risk assessment must be conducted by the Information Technology Department prior to onboarding any new cloud service.
c. Data stored in the cloud must be encrypted at rest and in transit using current industry standards.
d. Multi-factor authentication (MFA) must be enabled for all administrative and user access to cloud services
e. CSPs must maintain system logs, access records, and support audit functionality as required by BCVWD, and made available to the Information Technology Department upon request.
f. Cloud vendors must disclose the geographic location(s) where BCVWD data will be stored. Storage or processing of District data outside of the United States must be approved in writing by the Information Technology Department prior to implementation.
g. Cloud service providers must provide, upon request, third-party security certifications or audit reports (e.g., SOC 2 Type II, ISO 27001, or equivalent). BCVWD reserves the right to periodically review or audit the provider's security posture to ensure compliance with District requirements.

7003.4.3 Data Ownership and Compliance

a. BCVWD retains full ownership and rights to all data stored in cloud systems.
b. Cloud contracts must include terms for the return of all District data upon termination of

service. Providers must return the data in a readable format and provide written certification that all District data, including backups, has been securely deleted from their systems within 30 days of contract termination.

c. All cloud-stored data is subject to CPRA and applicable local and state laws.
d. CSPs must agree not to use District data for analytics, profiling, or marketing.

7003.4.4 Vendor Requirements and Service Level Agreements (SLAs)

a. All CSPs must provide service level agreements (SLAs) outlining performance, uptime, response times, and breach notification procedures.
b. Subcontracting cloud services requires written approval by BCVWD and must include equal security obligations.
c. CSPs must maintain an incident response plan and provide timely notification of any actual or suspected security incidents.

7003.4.5 Employee Responsibilities

a. Employees must use only IT-approved cloud platforms for storing or sharing District data.
b. Use of unauthorized cloud storage services (e.g., personal Google Drive, Dropbox) is strictly prohibited.
c. Employees must report suspected cloud-related security incidents to the Information Technology Department immediately.

7003.5 Review and Revision Policy. The Information Technology Department will review the "Cloud Computing Policy" annually to ensure it remains current and effective in addressing the needs of the organization and any changes in regulatory or technological requirements. During the review process, the policy will be evaluated for its effectiveness, compliance with relevant regulations, alignment with the National Institute of Standards and Technology (NIST), and adherence to applicable local and state laws governing IT resource usage. Necessary updates or revisions will be made to ensure the policy continues to meet the District's requirements and supports its mission.

Understanding THE NIST CYBERSECURITY FRAMEWORK

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

And does it apply to you?

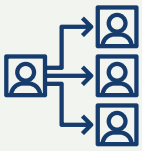
NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

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

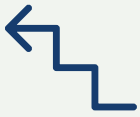
1. IDENTIFY

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

Create and share a company cybersecurity policy that covers:



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



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

2. PROTECT

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

LEARN MORE AT: FTC.gov/SmallBusiness

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

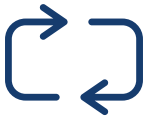
Have a plan for:

- 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 5a 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
April 15, 2025

Item 5b

STAFF REPORT

TO: Personnel Committee

FROM: Ren Berioso, Human Resources Manager

SUBJECT: **Policies and Procedures Manual Updates / Revisions amending Information Technology Policy 7005 Internet Use and Personal Social Media Ethics**

Staff Recommendation

Approve the revision of Information Technology (IT) Policy 7005 Internet Use and Personal Social Media Ethics (policy) to move forward to the next Board of Directors meeting, or direct staff as desired.

Executive Summary

At the March 18 Personnel Committee meeting, HR staff proposed IT Policy 7005 – Internet Use and Personal Social Media Ethics, outlining standards for the responsible use of District internet resources and employee's ethical conduct on personal social media. The Committee raised concerns about potential conflicts with employees' First Amendment rights and directed HR staff to seek legal counsel for further guidance.

Background

At the March 18 Personnel Committee meeting, Human Resources (HR) staff proposed the implementation of IT Policy Number 7005 – Internet Use and Personal Social Media Ethics (the "Policy"), which was adapted from Section 5100.3 of Policy Number 5100, Press Relations and Social Media Ethics. The proposed Policy outlines clear guidelines for the appropriate use of District-provided internet resources, as well as the ethical and legally compliant use of personal social media by District employees.

During the meeting, the Committee discussed concerns related to restrictions on posting prohibited content on personal social media during employees' private time. These concerns centered on the potential implications for employees' First Amendment rights under the United States Constitution. As a result, the Personnel Committee directed staff to seek guidance from legal counsel on this matter.

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

Discussion

The 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 personal social media use. Table A, Summary of Policy Revisions, outlines the proposed Policy 7005 that was drafted by HR and IT Departments, and was reviewed by Legal Counsel.

Table A – Summary of Policy Revisions

TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
1	7005.4.1.b	NIST	The District does not allow employees to browse the internet for personal reasons.	Consider adding language "personal reasons"	No fiscal impact.
2	7005.4.2.e	NIST	The District follows the law.	Legal counsel recommends striking out the "mislead" language.	No fiscal impact.
3	7005.4.3. b,c and f	First Amendment of the US Constitution	The District follows the law.	Consider the legal counsel's modification of the section that protects the employees right to First Amendment. However, the language also states that there are limitations to the right if this violates the law, or impacts the District's efficiency and integrity.	No fiscal impact.

TABLE A	Policy Section	State / Federal Law requirement	BCVWD current practice	Policy Section and Language to Consider	Fiscal Impact of Section
4	**7005.4.5. a, b and c**	**CPRA**	The District follows the law.	Legal counsel added "presumptively" subject to CPRA. Legal counsel also recommends change of language to "disclosure".	No fiscal impact.

Fiscal Impact

No fiscal impact in the revisions of this policy

Attachments

1. Redlined version of Policy 7005: Internet Use and Personal Social Media Ethics
2. Clean version of Policy 7005: Internet Use and Personal Social Media Ethics
3. Side-by-Side version of Policy 7005 Internet Use and Personal Social Media Ethics
4. Blog: Can You Be Fired For Social Media Posts In California

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~~for personal reasons. 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~~ 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~~as an employee of the District.
f. Employees are reminded that privacy settings on personal social media platforms are not

Commented [RTG1]: I would consider whether you want to include this language. On the one hand, when expressing a political opinion, I see how it would be helpful to have the employee add the disclaimer. On the other hand, if the employee is posting a photo that may not reflect well on the District (e.g., excessive drunkenness or provocative clothing), the disclaimer might just call attention to the fact that the person is associated with the District. Up to your discretion on this one.

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. Employees should conduct themselves in a manner consistent with the highest level of integrity, decorum, and professionalism in their personal use of social media. Employees are free to express themselves as private citizens on social media to the extent that their speech does not impair working relationships, impede the performance of duties, impair discipline and harmony among co-workers, compromise the integrity, effectiveness, or efficiency of the District, or harm the public trust and credibility of the District or its personnel. 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.) District staff should refrain from the following in their public social media use~~Inappropriate content includes, but is not limited to~~:

a. Violence, profanity, obscenity, nudity, or pornographic content or language;
b. ~~The c~~Content that ~~is found to discriminate~~ unlawfully harasses members of any class of persons protected by state or federal laws, including but not limited to, ~~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 of violence or other unlawful acts, 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 illegal business~~es~~, trade or commerce;
g. Content that violates copyright laws; or
h. Content that violates local, state or federal laws.

Violations of this policy will be handled on a case by case basis. If an employee has any doubts about content they intend to post on social media, they are encouraged to contact a supervisor, Human Resources or the General Manager to ensure compliance with the policy. Employees are cautioned that while t~~T~~he First Amendment ~~rights~~ may offer some protection if an employee acts in a purely private capacity. ~~However, these~~Such protection~~s~~ ~~are~~is ~~are~~is not absolute and certain types of ~~does not cover all~~ private speech may form the basis of discipline if sufficiently detrimental to the District and its interests. ~~social media posts if such conduct disrupts the workplace, violates the District's code of conduct, or erodes the District's ability to function effectively~~.

7005.4.4 Cybersecurity Measures

a. Employees must adhere to NIST best practices by avoiding insecure websites (e.g., those without HTTPS) and report~~ing~~ 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 presumptively 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, discovery, or CPRA requests.
c. To ensure compliance with the CPRA and limit potential ~~exposure to subpoenas~~disclosure, 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.

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 for personal reasons. 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 as an employee of the District.
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. Employees should conduct themselves in a manner consistent with the highest level of integrity, decorum, and professionalism in their personal use of social media. Employees are free to express themselves as private citizens on social media to the extent that their speech does not impair working relationships, impede the performance of duties, impair discipline and harmony among co-workers, compromise the integrity, effectiveness, or efficiency of the District, or harm the public trust and credibility of the District or its personnel. 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.) District staff should refrain from the following in their public social media use:

a. Violence, profanity, obscenity, nudity, or pornographic content or language;
b. Content that unlawfully harasses members of any class of persons protected by state or federal laws, including but not limited to, any creed, race, gender, sexual orientation, age, religion or national origin;
c. Threats of violence or other unlawful acts, 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 illegal business, trade or commerce;
g. Content that violates copyright laws; or
h. Content that violates local, state or federal laws.

Violations of this policy will be handled on a case by case basis. If an employee has any doubts about content they intend to post on social media, they are encouraged to contact a supervisor, Human Resources or the General Manager to ensure compliance with the policy. Employees are cautioned that while the First Amendment may offer some protection if an employee acts in a purely private capacity. Such protection is not absolute and certain types of private speech may form the basis of discipline if sufficiently detrimental to the District and its interests. .

7005.4.4 Cybersecurity Measures

a. Employees must adhere to NIST best practices by avoiding insecure websites (e.g., those without HTTPS) and report 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 presumptively 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, discovery, or CPRA requests.
c. To ensure compliance with the CPRA and limit potential disclosure, 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.

5b Attachment 3

CURRENT 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 the public.
f. Employees are reminded that privacy settings on personal social media platforms are not

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~~for personal reasons. 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~~ 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.A

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~~as an employee of the District.
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.

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. Employees should conduct themselves in a manner consistent with the highest level of integrity, decorum, and professionalism in their personal use of social media. Employees are free to express themselves as private citizens on social media to the extent that their speech does not impair working relationships, impede the performance of duties, impair discipline and harmony among co-workers, compromise the integrity, effectiveness, or efficiency of the District, or harm the public trust and credibility of the District or its personnel. 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.) District staff should refrain from the following in their public social media use~~Inappropriate content includes, but is not limited to~~:

a. Violence, profanity, obscenity, nudity, or pornographic content or language;
b. ~~The c~~Content that ~~is found to discriminate~~ unlawfully harasses members of any class of persons protected by state or federal laws, including but not limited to, ~~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 of violence or other unlawful acts, 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 illegal business~~es~~, trade or commerce;
g. Content that violates copyright laws; or
h. Content that violates local, state or federal laws.

Violations of this policy will be handled on a case by case basis. If an employee has any doubts about content they intend to post on social media, they are encouraged to contact a supervisor, Human Resources or the General Manager to ensure compliance with the policy. Employees are cautioned that while t~~T~~he First Amendment ~~rights~~ may offer some protection if an employee acts in a purely private capacity. ~~However, these~~Ssuch protections ~~are~~is ~~are~~is not absolute and certain types of ~~does not cover all~~ private speech may form the basis of discipline if sufficiently detrimental to the District and its interests. ~~social media posts if such conduct disrupts the workplace, violates the District's code of conduct, or erodes the District's ability to function effectively~~.

7005.4.4 Cybersecurity Measures

a. Employees must adhere to NIST best practices by avoiding insecure websites (e.g., those without HTTPS) and report~~ing~~ 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

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.

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 presumptively 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, discovery, or CPRA requests.
c. To ensure compliance with the CPRA and limit potential ~~exposure to subpoenas~~disclosure, 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

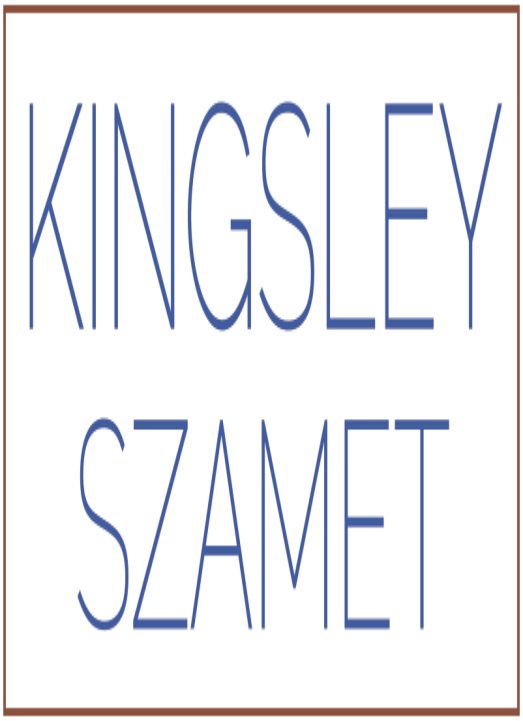
a. BCVWD will provide periodic training to employees on safe internet use, social media best practices, and compliance with this policy. These training sessions will align with the District's Security Awareness and Training Policy to ensure comprehensive employee education on cybersecurity and compliance.
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.

Attachment 4



(818) 990-8300

Employee Rights Blog

Can You Be Fired For Social Media Posts In California?

Posted by Eric Kingsley | Sep 17, 2024 | 0 Comments

Can you be fired for social media posts? You might think your social media is your own personal space. However, a reckless post could cost you your job. This article provides a clear understanding of employee rights and employer limitations regarding social media conduct so you can navigate this tricky territory with confidence.

The legal landscape for social media posts and their impact on employment can be difficult to understand and apply...clear-cut answers aren't always easy to find. Outcomes often depend on various factors. These include the content of the post, company policies, state laws, and even broader legal concepts like freedom of speech and protected concerted activity. This makes it essential for employees to be aware of their specific rights and responsibilities.

Table Of Contents:

The Rise Of Social Media And Workplace Concerns

Social media has transformed how we communicate and interact. Platforms like Facebook, Instagram, Twitter, and even LinkedIn are now integral parts of our personal and professional lives. While this connectivity has benefits, it's also brought new challenges to the workplace. Employers now worry about employees' online activity reflecting poorly on the company. They are also concerned about potential disruption to the work environment.

Can Employers Legally Fire You For Your Social Media Posts?

Yes, in most cases, they can. The First Amendment guarantees freedom of speech. However, this protection primarily applies to government restrictions, not private employers. In the United States, most employment is considered at-will. This means employers generally have the right to terminate employees for a variety of reasons. This includes social media posts. The exception is if the reasons arediscriminatory or retaliatory. What you post on social media can be considered a lawful reason for termination if it negatively impacts the employer's reputation or operations. This is true even on your personal accounts and outside of work hours.

Reasons You Could Get Fired For A Social Media Post

There are many situations where a social media post can justify your firing. Posting offensive

content like racist or sexist remarks can create a hostile work environment. This goes against legal obligations for employers under Title VII of the Civil Rights Act. Employers might terminate employees who violate a clearly communicated social media policy.

Some posts, even those seemingly unrelated to work, can raise red flags for employers. Sharing confidential information, like company secrets or financial details, is grounds for termination. It poses an economic risk to the organization. Spreading gossip about coworkers or engaging in public bashing of clients or the company itself can be perceived as detrimental to the workplace atmosphere. This could lead to termination.

Engaging in illegal activities, even outside work, can damage a company's reputation if publicly shared on your social media. This can lead to job loss. Posting provocative or controversial opinions can sometimes also result in termination. This is particularly true if these views conflict with the values of the company. It's also risky if your views are perceived as potentially offensive to customers. Take the example of Justine Sacco in 2013. She lost her job because of a racist tweet, demonstrating how a single social media post can have far-reaching consequences.

Exceptions To At-Will Employment

Although at-will employment highlights the broad powers of employers, there are limitations. Employees cannot be fired for discriminatory reasons based on certain factors. This includes race, religion, national origin, sex, disability, age (over 40), or genetic information. You can't be fired for posting about protected characteristics. This includes things like your religious beliefs or political affiliation, for example.

The National Labor Relations Act (NLRA) offers another protection: "protected concerted activity." You are within your legal rights to engage in discussions about wages, work conditions, or forming a union, even on social media. This is important because it allows employees to collectively address workplace concerns without fear of reprisal. If you are fired for exercising these rights, it could be considered wrongful termination.

Employer Monitoring And Social Media Policies

The reality is that many employers use social media to screen job candidates. In fact, 70% of employers admit to checking social media accounts before making a hiring decision.

Employers can often get away with this because social media platforms are usually public spaces. This makes them fair game for employers to access. This monitoring even extends to existing employees. Employers sometimes check posts for violations of company policies or potential harm to the company's image.

That's why companies often have social media policies outlining appropriate online conduct for employees. These policies will often discourage posts that might reflect poorly on the company or cause friction within the work environment. It's best to be aware of and adhere to your company's policy to avoid unwanted scrutiny. If your employer doesn't have a written social media policy, talk to HR. Encourage them to develop one. A clearly defined policy benefits both employees and the employer. It does this by outlining expectations and preventing potential misinterpretations.

The Fine Line: How To Stay Safe On Social Media

So how do you enjoy your social media freedom while safeguarding your job? Understanding your rights and employer limitations regarding social media conduct is critical. Below are several points for employees to consider when engaging on social media:

- Understand your company's social media policy and adhere to it.
- Avoid sharing confidential information about your coworkers or the company.
- Think twice before venting frustrations about your employer publicly.
- Be mindful of the impact your posts can have on your employment.
- Regularly review and clean up your social media profiles.

Remember, what might seem harmless to you could be detrimental to your employer's image. Even seemingly private messages can become public. If you're unsure about posting something, err on the side of caution. Your job security is worth protecting. It's also a good idea to make your social media accounts private or limit who can see your posts. Be aware that even deleting a post doesn't always erase it completely. Screenshots can preserve harmful content even after it's removed.

FAQs About Can You Be Fired For Social Media Posts?

FAQ 1: Can An Employer Fire An Employee For Social Media Posts?

In many cases, yes. It's a complicated issue that depends on a lot of things. This is why understanding the law is important. You also need to know your company's social media policy and stay mindful about what you post online. This will help you avoid facing serious repercussions.

FAQ 2: Can You Be Dismissed For Social Media Posts?

Absolutely, and it happens frequently. Research indicates that one in ten job seekers aged 16 to 34 has experienced job rejection because of content found on their social media profiles. You can read more about this on BBC Worklife. Remember, recruiters also use social media to vet candidates. In fact, 90% of them use search engines to gather more information than what's provided on your resume. Managing your online image is critical. Think of your online profiles as an extension of your professional persona. Make sure they're portraying the best version of yourself.

FAQ 3: Should Employees Be Disciplined For Social Media Posts?

Whether employees should be disciplined for social media posts is a subjective and contextual matter. Disciplining an employee is within the rights of an employer under certain circumstances. For instance, they may do so for sharing offensive content, violating company policy, leaking confidential information, or bullying or harassing other employees or customers.

The appropriateness of disciplinary actions depends on many things. Consider the company's social media policy, the nature and severity of the post, state and federal laws, the intent of the employee, and the overall context. All of these must be taken into account.

FAQ 4: Can You Get Fired For Using Social Media At Work?

This mostly depends on your company's specific policies on internet and social media use during work hours. Many organizations restrict personal social media usage while employees are on company time. This is often due to fear of decreased productivity or breaches in security.

Some businesses might allow social media usage during breaks or designated times. However, they may prohibit it during active work periods. However, remember the NLRA protections on

protected concerted activity. Even during work hours, employees can engage in discussions regarding work conditions, wages, or forming a union using social media platforms. Firing an employee for this is illegal. To avoid potential misunderstandings, you must thoroughly understand your company's policies on social media usage at work.

Conclusion

Social media is undeniably a double-edged sword for employees. It offers you a way to express your opinions and stay connected. It can also be useful for building professional networks and accessing valuable resources. However, there is always the risk of getting caught in a web of consequences. Whether or not you can be fired for a social media post depends on numerous variables.

Navigating social media responsibly is key to ensuring you stay on the safe side. This helps keep your job secure and protect your professional reputation. Ultimately, when it comes to social media in the context of your employment, remember a few things. Exercise common sense, be aware of policies and the law, and practice responsible use. These are the most effective shields against potential job loss.

Share

About The Author

Eric Kingsley

Eric B. Kingsley is a 2024 "Best In Law" Award winner, 2024 Consumer Attorneys of California Presidential Award of Merit recipient, and has litigated over 150 class actions. He is an AV peer rated attorney and a prolific speaker at various seminars on employment law.

Comments

There are no comments for this post. Be the first and Add your Comment below.

Beaumont-Cherry Valley Water District
Personnel Committee Meeting
April 15, 2025

Item 6

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	9	9	34.62%
Engineering[2]	8	8	1	1	12.50%
Finance	15	15	10	8	53.33%
Human Resources	**70**	**70**	**70**	**70**	**100%**
Information Technology[3]	18	18	10	5	17.64%
TOTALS	**137**	**133**	**95**	**90**	**65.69%**

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	7009	Drone Usage Policy	2 pages	April	May
2	7010	Electronic Signature Policy	2 pages	April	May
3	7012	Accessibility Policy	2 pages	April	May

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	Members, and Victims of Domestic	Human Resources	Yes	12/6/2024	2/18/2025	2/18/2025	3/11/2025	3/11/2025	3/11/2025	25-008
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	1/25/2025	2/17/2025	2/17/2025	4/12/2025			
2	4010	Board of Directors	Members of the Board of Directors	Administration	Yes	1/25/2025	2/17/2025	3/17/2025	4/12/2025			
3	4015	Board of Directors	Committees of the Board of Directors	Administration	Yes	3/5/2025	3/17/2025	3/17/2025	4/12/2025			
4	4020	Board of Directors	Duties of Board President and Officers	Administration	Yes	1/25/2025	2/17/2025	2/18/2025	4/12/2025			
5	4025	Board of Directors	Board Meetings	Administration	Yes	3/5/2025	2/18/2025	3/17/2025	4/12/2025			
6	4030	Board of Directors	Board Meeting Agendas	Administration	Yes	1/25/2025	2/18/2025	3/17/2025	4/12/2025			
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	1/25/2025	2/17/2025	3/17/2025	4/12/2025			
9	4045	Board of Directors	Attendance at Meetings	Administration	Yes							
10	4050	Board of Directors	Minutes of Board Meetings	Administration	Yes							
11	4055	Board of Directors	Rules of Order for Board and	Administration	Yes	3/5/2025	3/17/2025	3/17/2025	4/12/2025			
12	4060	Board of Directors	Training, Education and Conferences	Administration	Yes	6/30/2021			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			7/14/2021	Revisions Requested on	7/14/2021	21-012
14	4070	Board of Directors	Payment of Expenses Incurred on	Administration	Yes							
15	4075	Board of Directors	Expenditure Reimbursement	Administration	Yes							
17	4080	Board of Directors	Membership in Associations	Administration	Yes							
18	4085	Board of Directors	Ethics Training	Administration	Yes							
19	4090	Board of Directors	Code of Ethics	Administration	Yes							
20	4095	Board of Directors	Ethics Policy	Administration	Yes							
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
N/A	5100	Operations	Press Relations and District Social	IT/Personnel	Yes	3/5/2025	3/18/2025					
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				
1	6005	Miscellaneous	Purpose of Board Policies	Combined with 1010	Yes		N/A	Direct to Board (Ad Hoc?)				
2	6010	Miscellaneous	Adoption, Amendment of Policies	Combined with 1010	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	3/18/2025	3/27/2025			
N/A	8001	Information Technology	Access Control Policy	Information Technology	Yes			Board Closed Session				
N/A	8002	Information Technology	IT Hardware and Software Procurement	Information Technology	Yes			Board Closed Session				
N/A	8003	Information Technology	Workstations, Servers, and Network	Information Technology	Yes			Board Closed Session				
N/A	8004	Information Technology	Asset Management Policy	Information Technology	Yes			Board Closed Session				
N/A	8005	Information Technology	Backup and Disaster Recovery Policy	Information Technology	Yes			Board Closed Session				
N/A	7002	Information Technology	Bring Your Own Device (BYOD) Policy	IT/Personnel	Yes	1/26/2025	3/11/2025	3/18/2025	3/27/2025			
N/A	8006	Information Technology	Change Management Policy	Information Technology	Yes			Board Closed Session				
N/A	7003	Information Technology	Cloud Computing Policy	IT/Personnel	Yes	3/10/2025						
N/A	8007	Information Technology	Third-Party Risk Assessment Policy	Information Technology	Yes			Board Closed Session				
N/A	8008	Information Technology	Configuration Management Policy	Information Technology	Yes			Board Closed Session				
N/A	8009	Information Technology	Cybersecurity Policy	Information Technology	Yes			Board Closed Session				
N/A	8010	Information Technology	Data Breach Notification Policy	Information Technology	Yes			Board Closed Session				
N/A	8011	Information Technology	Data Classification Policy	Information Technology	Yes			Board Closed Session				
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	8012	Information Technology	Encryption Policy	Information Technology	Yes			Board Closed Session				
N/A	8013	Information Technology	Incident Response Policy	Information Technology	Yes			Board Closed Session				
N/A	8014	Information Technology	Information Security Policy	Information Technology	Yes			Board Closed Session				
N/A	7005	Information Technology	Internet and Social Media Policy	IT/Personnel	Yes	1/26/2025	3/11/2025					
N/A	8015	Information Technology	Mobile Device Management Policy	Information Technology	Yes			Board Closed Session				
N/A	8016	Information Technology	Network Security Policy	Information Technology	Yes			Board Closed Session				
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	8017	Information Technology	Patch Management Policy	Information Technology	Yes			Board Closed Session				
N/A	8018	Information Technology	Physical Security Policy	Information Technology	Yes			Board Closed Session				
N/A	8019	Information Technology	Privacy Policy	Information Technology	Yes			Board Closed Session				
N/A	7007	Information Technology	Remote Access Policy	IT/Personnel	Yes	3/10/2025						
N/A	8020	Information Technology	Risk Management Policy	Information Technology	Yes			Board Closed Session				
N/A	7008	Information Technology	Wireless Network Security Policy	IT/Personnel	Yes	3/10/2025						
N/A	8021	Information Technology	Server Management Policy	Information Technology	Yes			Board Closed Session				
N/A	8022	Information Technology	Software Development Policy	Information Technology	Yes			Board Closed Session				
N/A	8023	Information Technology	Third-Party Vendor Management Policy	Information Technology	Yes			Board Closed Session				
N/A	7009	Information Technology	Drone Use Policy	IT/Personnel	Yes							
N/A	8024	Information Technology	IT Asset Disposal (ITAD) or Electronic	Information Technology	Yes			Board Closed Session				
N/A	7010	Information Technology	Electronic Signature Policy	IT/Personnel	Yes							
N/A	8025	Information Technology	Asset Protection and Fraud Policy	Information Technology	Yes			Board Closed Session				
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	8026	Information Technology	Electronic Communications and Data	Information Technology	Yes			Board Closed Session				
N/A	8027	Information Technology	Computer and Business Continuity	Information Technology	Yes			Board Closed Session				
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	8028	Information Technology	Security and Technology Access for	Information Technology	Yes			Board Closed Session				

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
N/A	7015	Information Technology	Security Awareness and Training Policy	IT/Personnel	Yes	N/A	1/21/2025					
N/A	8029	Information Technology	Data Ethics Policy	Information Technology	Yes			Board Closed Session				
N/A	7016	Information Technology	IoT (Internet of Things) Security Policy	IT/Personnel	Yes							
N/A	8030	Information Technology	Data Loss Prevention (DLP) Policy	Information Technology	Yes			Board Closed Session				
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							
N/A	8031	Information Technology	Electronica Data Retention and Records	Information Technology	Yes							
N/A	8032	Information Technology	Major IT Project Implementation	Information Technology	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