RESOLUTION 2025-18

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE BEAUMONT - CHERRY VALLEY WATER DISTRICT AMENDING THE DISTRICT'S POLICIES AND PROCEDURES MANUAL

WHEREAS, on March 18, 2009 the Board of Directors of the Beaumont-Cherry Valley Water District adopted Resolution 2009-05, establishing a Policy and Procedures Manual applicable to Board of Directors and District staff; and

WHEREAS, upon review and discussion, the Personnel Committee, the ad hoc Board Policies Committee, and the Finance and Audit Committee of the Board of Directors recommended revisions to the Policy and Procedures Manual; and

WHEREAS, the Board of Directors has reviewed and considered the revisions to the subject policies attached hereto and listed below, finds the new or revised policies relevant and acceptable, and it to be in the best interests of the District that the following actions be taken,

NOW THEREFORE, BE IT RESOLVED by the Board of Directors of the Beaumont-Cherry Valley Water District as follows:

The BCVWD Policies and Procedures Manual sections are revised or replaced per the attached exhibits as indicated below:

	Replace or Revise Policy:	**With the New or Revised Policy:**
A	Part II Section 9 Attendance at Meetings	4045 Attendance at Meetings as corrected
B	Part II Section 10 Minutes of Board Meetings	4050 Minutes of Board Meetings
C	Part II, Section 16 Membership in Associations	4080 Membership in Associations
D	New policy	7007 Remote Access
E	New policy	7008 Wireless Network Security

ADOPTED this 11TH day of JUNE, 2025, by the following vote:

AYES: COVINGTON, HOFFMAN, RAMIREZ, SLAWSON, WILLIAMS
NOES:
ABSTAIN:
ABSENT:

ATTEST:

Director Daniel Slawson, President of the Board of Directors of the Beaumont-Cherry Valley Water District

Director Andy Ramirez, Secretary to the Board of Directors of the Beaumont-Cherry Valley Water District

Attached Exhibits

A 4045 Attendance at Meetings
B 4050 Minutes of Board Meetings
C 4080 Membership in Associations
D 7007 Remote Access
E 7008 Wireless Network Security

EXHIBIT A

POLICY TITLE: ATTENDANCE AT MEETINGS
POLICY NUMBER: 4045

4045. 1 Attendance. Members of the Board of Directors shall attend all regular and special meetings of the Board unless there is cause for absence.

4045. 2 Punctuality. Each member shall be in his or her respective seat at the hour set for each regular meeting and at the time set for any special or adjourned meeting. If a member arrives after a meeting convenes, the recording secretary shall note his or her arrival time in the minutes and the Board member shall be deemed present. A Board member not present for a minimum of 51 percent of the duration of the meeting shall be marked "absent."

4045.3 Absences. If any member of the Board is unable to attend a meeting, the Board member shall, if possible, notify the Board President or the Board Secretary prior to the meeting.

4045.4 Teleconferencing. A Board member may use audio or video teleconferencing to attend a regular or special meeting of the Board of Directors pursuant to the standard provisions of the Ralph M. Brown Act. At least a quorum of the Board members must participate from locations within the District's service area boundary.

A. A request for teleconferencing under the standard provisions of the Brown Act must be made by the Board member to the Board President, and the General Manager, or his/her designee or the Recording Secretary via email or telephone call no later than one business day prior to the 72-hour agenda posting deadline to allow compliance with legal noticing requirements. If the agenda is not updated with the teleconference location at least 72 hours prior to the meeting, such teleconferencing is not allowed under State law.
    a. Under the standard provisions of the Brown Act, a Board member must post the meeting agenda at his or her teleconference location and maintain said location accessible to the public.
B. Other requests for teleconferencing may be made pursuant to current law, i.e., AB 2449 or other currently applicable legislation, following the procedures set out therein.
C. A Board member not in compliance with the provisions set forth in the Brown Act may listen to a live meeting via teleconference but may not participate in discussion, offer comment, or vote. The Board member will be marked as absent, but will be listed as a member of the public in attendance.

4045.5 Business. Staff will, to the extent practicable, consider planned absences when scheduling matters for Board action if District business will not be hindered by any delay or advancement of schedule.

EXHIBIT B

POLICY TITLE: MINUTES OF BOARD MEETINGS
POLICY NUMBER: 4050

4050.1 Minutes. Staff acting in his/her capacity as "Recording Secretary" shall keep minutes of all regular and special meetings of the Board.

4050.2 Copies of a meeting's minutes shall be distributed to Directors as part of the information packet for the next regular meeting of the Board, at which time the Board will consider approving the minutes as presented or with modifications. Once approved by the Board, the official minutes shall be kept on archival paper in a fire resistant room.

4050.3 Unless directed otherwise, an audio recording of regular and special meetings of the Board of Directors will be made providing that no such recording shall be made of any closed session of the Board of Directors. The device upon which the recording is stored shall be kept for a minimum of 100 days in a fireproof vault or in fire-resistant room or locked cabinet. Members of the public may inspect recordings of Board meetings without charge on a playback device that will be made available by the District.

4050.4 Motions, resolutions or ordinances shall be recorded in the minutes as having passed or failed and individual votes will be recorded. (GC 54953(c)(2). All resolutions and ordinances adopted by the Board shall be numbered consecutively, starting new at the beginning of each year.

4050.5 In addition to other information that the Board may deem to be of importance, the following information (if relevant) shall be included in each meeting's minutes:

A. Date, place and type of each meeting;
B. Directors present and absent by name;
C. Administrative staff present by name;
D. Call to order;
E. Time and name of late arriving Directors;
F. Time and name of early departing Directors;
G. Names of Directors absent during any agenda item upon which action was taken;
H. Summary record of staff reports;
I. Summary record of public comment regarding matters not on the agenda, including names of commentators;
J. Approval of the minutes or modified minutes of preceding meetings;
K. Approval of financial reports;
L. Complete information as to each subject of the Board's deliberation;
M. Record of the vote of each Director on every action item
N. Resolutions and ordinances described as to their substantive content and sequential numbering;
O. Record of all contracts and agreements, and their amendment, approved by the Board;
P. Approval of the annual budget;
Q. Approval of all polices, rules and/or regulations;
R. Approval of all dispositions of District assets;
S. Approval of all purchases of District assets; and
T. Time of meeting's adjournment.

EXHIBIT C

POLICY TITLE MEMBERSHIP IN ASSOCIATIONS
POLICY NUMBER 4080

4080.1 Policy. The District shall ordinarily hold membership in such national, state, and local associations as may exist which have applicability to the functions of the District, and which promote the interests of public water utilities or special districts.

4080.2 The Board of Directors may attend meetings and look upon such memberships as an opportunity for in-service training.

4080.3 The President-elect may appoint a representative and alternate, and/or a voting delegate during the annual Board reorganization meeting in December, or the first regular or special meeting in January each year, or as necessary.

4080.4 The Board may approve memberships in other organizations, such as the Chamber of Commerce, as it deems appropriate.

4080.5 Board members who vote or hold an appointed position in these associations are representing the District when attending those meetings and functions.

A. When Board members are attending association meetings on their own accord, and are not requested or appointed to attend by the President, Board members are not authorized to officially speak on behalf of the District at those meetings.

EXHIBIT D

POLICY TITLE: REMOTE ACCESS
POLICY NUMBER: 7007

7007.1 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.

7007.2 Purpose. The purpose of this policy is to define the requirements and responsibilities for securely accessing BCVWD systems and data from remote locations. The policy ensures that only authorized, District-issued devices are used, and that remote access is managed with strict security controls to protect the confidentiality, integrity, and availability of District information.

7007.3 Scope. This policy applies to all BCVWD employees, contractors, and authorized third parties who access District systems, data, or services remotely. It governs the use of District-issued laptops, tablets, and mobile devices and prohibits the use of personal devices for remote access.

7007.4 Policy Details

7007.4.1 Authorization and Access Control

A. Remote access must be explicitly approved by the Information Technology Department and will be granted only to users with a demonstrated business need
B. Access will be provisioned using District-issued and MDM-managed devices only.
C. BCVWD-issued device Remote access credentials must not be shared and must be unique to each user.
D. Access will be limited based on the principle of least privilege.

7007.4.2 Prohibited Use of Personal Devices

A. Personal devices, including personal computers, tablets, smartphones, printers, USB drives, and external storage, are strictly prohibited for use in accessing District systems.
B. Only devices issued or explicitly approved by the Information Technology Department may be used for any form of remote connectivity.
C. No blending of personal and professional use is permitted on District devices. This includes accessing personal email, browsing non-work-related websites, or installing unapproved applications.

7007.4.3 Device Configuration and Security

A. All remote access devices must be enrolled in BCVWD's Mobile Device Management (MDM) program.
B. Devices must use strong authentication methods, including multi-factor authentication (MFA).
C. Devices must be configured to auto-lock after a period of inactivity (maximum 10 minutes).
D. Endpoint protection (antivirus, firewall, and system updates) must be maintained by the IT Department.

7007.4.4 Data Handling and Storage

A. No District data shall be stored locally on devices unless explicitly authorized and encrypted.
B. All remote work must be conducted through District-approved platforms or systems.
C. Cloud services and document sharing tools must be approved by IT and covered under the Cloud Computing Policy.

D. Remote users must disconnect from District systems when not in use.

7007.4.5 Monitoring and Logging

A. All remote access sessions are subject to monitoring and logging by the Information Technology Department.
B. Logs will be reviewed regularly for unauthorized activity or anomalies.
C. Any attempt to circumvent security controls will result in immediate suspension of access.

7007.4.6 Incident Reporting

A. Users must immediately report lost or stolen District-issued devices to the Information Technology Department.
B. Any security incidents, including suspected unauthorized access, must be reported without delay.
C. The IT Department will respond in accordance with the District's Incident Response Policy.

7007.5 Review and Revision Policy. The Information Technology Department will review the "Remote Access 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.

EXHIBIT E

POLICY TITLE: WIRELESS NETWORK SECURITY
POLICY NUMBER: 7008

7008.1 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.

7008.2 Purpose . The purpose of this policy is to define standards and security controls for the use of wireless networks within BCVWD facilities. This includes management of secure internal wireless networks, guest wireless networks, and appropriate use of cellular wireless access, in order to prevent unauthorized access, data leakage, or policy violations.

7008.3 Scope. This policy applies to all BCVWD employees, contractors, vendors, and guests who access BCVWD wireless networks or connect wirelessly using cellular or mobile broadband services within District facilities. It covers secure and guest Wi-Fi, mobile hotspot usage, and wireless-capable devices.

7008.4 Policy Details

7008.4.1 Wireless Network Segmentation and Access Control

A. BCVWD maintains two distinct wireless environments:
    1. Secure Wireless Network (internal): Available only to BCVWD-issued and IT-approved devices
    2. Guest Wireless Network: Provided for visitors and employee-owned personal devices requiring basic internet access.
B. Each network operates on separate SSIDs and is logically segregated to prevent cross-network traffic or lateral movement.
C. BCVWD-issued devices are strictly prohibited from connecting to the Guest Wireless Network.
D. Access to the Secure Wireless Network must be explicitly approved and provisioned by the Information Technology Department.

7008.4.2 Security Standards and Configuration

A. All wireless networks must use industry-standard encryption (e.g., WPA3, or WPA2 with AES encryption) as defined by NIST.
B. Wireless access points (WAPs) must be configured to block peer-to-peer communication and isolate client devices.
C. Wireless networks must enforce complex passwords, automatic re-authentication after inactivity, and secure password rotation policies.
D. Wireless networks must be monitored for rogue access points, unauthorized SSIDs, and abnormal traffic. Regular security scans will be conducted
E. All wireless access logs will be retained and reviewed periodically to detect misuse or unauthorized activity.
F. Wireless access points (WAPs) must be regularly updated with the latest firmware and patches. Periodic vulnerability scans will be performed to identify misconfigurations, outdated software, or security gaps.
G. Devices connecting to the Secure Wireless Network must be registered and approved. MAC address filtering or network access control (NAC) systems may be used to limit access to authorized devices.

H. Wireless sessions must be configured to disconnect or reauthenticate after a defined period of inactivity, in accordance with session timeout thresholds set by the Information Technology Department

7008.4.3 Guest Wireless Network Use

A. Guest Wireless Network access is provided for limited internet browsing and communication use only. No access to BCVWD internal systems or data is permitted.
B. Guest access credentials may be restricted, time-limited, or revoked at the discretion of the IT Department.
C. Activity on the Guest Network may be logged and monitored to detect abuse, malicious behavior, or policy violations.

7008.4.4 Device and User Restrictions

A. No unauthorized personal routers, wireless repeaters, hotspots, or similar devices may be used within BCVWD facilities.
B. Employees must not share Secure Wireless Network credentials or connect personal devices to secure SSIDs without written IT authorization.
C. All devices connected to BCVWD wireless networks must comply with Acceptable Use, BYOD, and Mobile Device Management (MDM) policies.
D. Use of VPNs or other tunneling technologies over wireless connections requires prior IT Department approval

7008.4.5 Cellular Wireless Access and Tethering

A. Personal cellular hotspots, tethering, or mobile broadband connections may not be used to access BCVWD systems unless explicitly authorized by the Information Technology Department.
B. BCVWD-issued devices must not connect to personal cellular networks unless approved for specific business continuity or emergency response scenarios.
C. Any cellular access used for District purposes must comply with BCVWD's network security standards, including encryption, MFA, and MDM requirements.
D. The IT Department may audit, monitor, or restrict cellular use on District-managed devices as needed to enforce security compliance.

7008.4.6 Monitoring and Enforcement

A. The Information Technology Department reserves the right to monitor all wireless and cellular wireless activity for security purposes.
B. Devices found to be non-compliant, infected, or misused may be immediately disconnected or blocked.
C. In the event of wireless-related security incidents (e.g., rogue access points, signal jamming, impersonation attacks), the Information Technology Department will initiate a wireless incident response procedure in accordance with the District's Incident Response Policy.
D. Violations of this policy may result in disciplinary action, including revocation of access, device confiscation, or further corrective measures in accordance with BCVWD personnel policy.

7008.5 Review and Revision Policy. The Information Technology Department will review the "Wireless Network Security 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.