

RESOLUTION 2025-09

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 of the Board of Directors recommended revisions to the Policy and Procedures Manual based on advice given by the Director of Information Technology and the District's legal counsel; and

WHEREAS, the Board of Directors has reviewed and considered the revisions to the subject policies attached hereto and listed below, finds the new 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 established per the attached exhibits as indicated below:

	New Policy:
A	7001 Acceptable Use Policy
B	7002 Bring Your Own Device

ADOPTED this 27TH day of MARCH, 2025, by the following vote:

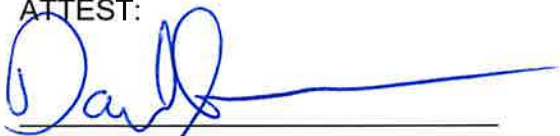
AYES: COVINGTON, HOFFMAN, RAMIREZ, SLAWSON, WILLIAMS

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

POLICY TITLE: ACCEPTABLE USE POLICY
POLICY NUMBER: 7001

7001.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) relies on Information Technology (IT) resources as essential tools for conducting business efficiently and securely. This policy ensures these resources are used responsibly, ethically, and in alignment with the National Institute of Standards and Technology (NIST) principles, which provide a framework for cybersecurity and data protection. As a California Special District, BCVWD adheres to state regulations, including compliance with the California Public Records Act (CPRA) to ensure transparency and accountability in public records management.

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

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

7001.4 Policy Details

7001.4.1 General Use

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

7001.4.2 Security and Confidentiality

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

7001.4.3 Prohibited Activities

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

7001.4.4 Internet and Email Use

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

7001.4.5 Monitoring Privacy

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

7001.4.6 Compliance with Local and State Laws

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

7001.4.7 Remote Work Guidelines

- a. Employees must adhere to all acceptable use standards when accessing District IT resources from remote locations.
- b. Employees are responsible for ensuring secure access to District systems, including using authorized devices and maintaining a secure home network.
- c. Failed login attempts will be logged and reviewed periodically by the IT Department to identify patterns of potential unauthorized access or brute-force attack attempts.

7001.4.8 Third-Party Compliance

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

7001.4.9 Policy Acknowledgement

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

7001.4.10 Enforcement

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

7001.5 Review and Revision Policy. BCVWD will review Policy 7001 Acceptable Use Policy annually to ensure it remains current and effective in addressing the needs of the organization and any changes in the regulatory or technological landscape. During the review process, the policy will be evaluated for its effectiveness, compliance with relevant regulations, alignment with the National Institute of Standards and Technology (NIST), and adherence to applicable local and state laws governing IT resource usage. Necessary updates or revisions will be made to ensure the policy continues to meet the District's requirements and supports its mission.

POLICY TITLE: BRING YOUR OWN DEVICE
POLICY NUMBER: 7002

7002.1 Introduction.

Beaumont-Cherry Valley Water District (BCVWD) relies on Information Technology (IT) resources as essential tools for conducting business efficiently and securely. This policy ensures these resources are used responsibly, ethically, and in alignment with the National Institute of Standards and Technology (NIST) principles, which provide a framework for cybersecurity and data protection. As a California Special District, BCVWD adheres to state regulations, including compliance with the California Public Records Act (CPRA) to ensure transparency and accountability in public records management.

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

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

7002.4 Policy Details

7002.4.1 General Use on Personal Devices

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

7002.4.2 Limited Wireless Internet Use

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

7002.4.3 Public Records Act Compliance

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

7002.4.4 Encouragement of District-Provided Resources

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

7002.4.5 Security and Confidentiality

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

7002.4.6 Enforcement

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

7002.5 Review and Revision Policy. BCVWD will review Policy 7002 Bring Your Own Device annually to ensure it remains current and effective in addressing the needs of the organization and any changes in the regulatory or technological landscape. During the review process, the policy will be evaluated for its effectiveness, compliance with relevant regulations, alignment with the National Institute of Standards and Technology (NIST), and adherence to applicable local and state laws governing the use of personal devices. Necessary updates or revisions will be made to ensure the policy continues to meet the District's requirements and supports its mission.