RESOLUTION 2025-07

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, and the Finance and Audit Committee of the Board of Directors recommended revisions to the Policy and Procedures Manual based on advice given by 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 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 I, Section 45, Internet, Email, and Electronic Communication Ethics, Usage and Security	Policy 7004 Email and Communication
B	Part I, Section 45, Internet, Email, and Electronic Communication Ethics, Usage and Security	Policy 7006 Password
C	Part I, Section 46, Cellular Telephone Usage	Policy 7011 Cellular Telephone Usage

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

AYES: Hoffman, Williams, Slawson, Covington
NOES:
ABSTAIN:
ABSENT: Ramirez

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

Exhibit A

POLICY TITLE: EMAIL AND COMMUNICATION
POLICY NUMBER: 7004

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

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

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

7004.4 Policy Details

7004.4.1 General Use and Ownership

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

7004.4.2 Security Measures

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

7004.4.3 Retention and Transparency

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

7004.4.4 Prohibited Activities

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

7004.4.5 Best Practices

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

7004.4.6 Monitoring

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

7004.4.7 Reporting Incidents

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

7004.4.8 California Compliance

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

7004.4.9 Water Sector Guidelines

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

7004.4.10 Third-Party Communications

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

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

POLICY TITLE: PASSWORD
POLICY NUMBER: 7006

Exhibit B

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

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

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

7006.4 Policy Details

7006.4.1 Password Creation and Complexity

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

7006.4.2 Password Management

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

7006.4.3 Multi-Factor Authentication (MFA)

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

c. Passwords for remote access tools, such as VPN or remote desktop applications, must meet complexity requirements and be protected by multi-factor authentication (MFA) when possible, to ensure secure access from external networks.

7006.4.4 Password Protection

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

7006.4.5 Account Lockout

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

7006.4.6 Special Considerations for System Accounts

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

7006.4.7 Monitoring and Enforcement

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

7006.4.8 California Compliance

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

7006.4.9 Water Sector Guidelines

a. Passwords used to access water sector-specific systems (e.g., SCADA or water quality monitoring systems) must adhere to enhanced security requirements as directed by NIST and industry best practices.
b. Periodic penetration testing will be conducted at least annually to evaluate the strength of password controls, identify vulnerabilities, and address risks to both IT and operational technology systems.
c. Critical systems such as SCADA must use customized password policies that address their unique security and operational requirements.
d. High-risk accounts, such as administrative or SCADA accounts, may require periodic password changes based on risk assessments conducted by the IT Department.

7006.4.10 Emergency Situations

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

7006.4.11 Awareness and Training

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

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

Exhibit C

POLICY TITLE: CELLULAR TELEPHONE USAGE
POLICY NUMBER: 7011

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

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

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

7011.4 Policy Details

7011.4.1 General Use

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

7011.4.2 Security Requirements

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

7011.4.3 Data Ownership and Protection

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

7011.4.4 Prohibited Activities

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

7011.4.5 Monitoring and Privacy

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

7011.4.6 Responsibilities

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

7011.4.7 California Compliance

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

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