RESOLUTION 2025-26

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 recommendation by the Director of Information Technology and Cybersecurity and review and discussion by the Personnel Committee of the Board of Directors, the Committee recommended additions to the Policy and Procedures Manual; and

WHEREAS, the Board of Directors has reviewed and considered the addition of 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 is updated to include the attached exhibits as indicated below:

	New Policy:
A	7009 Drone Usage
B	7010 Electronic Signature
C	7012 Accessibility

ADOPTED this 9TH day of JULY, 2025, by the following vote:

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

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

ATTEST:

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

Attached Exhibits

A 7009 Drone Usage
B 7010 Electronic Signature
C 7012 Accessibility

EXHIBIT A

POLICY TITLE: DRONE USAGE
POLICY NUMBER: 7009

7009.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) employs drone technologies, including aerial and submersible (underwater) platforms, to enhance operational efficiency, safety, and infrastructure monitoring. This policy ensures that the use of drone technology complies with federal and state regulations, aligns with National Institute of Standards and Technology (NIST) security principles, and supports the District's mission in a secure, responsible, and ethical manner.

7009.2 Purpose . The purpose of this policy is to establish guidelines for the safe, authorized, and compliant operation of drones used for District business. It applies to all forms of drone technology, including aerial and underwater drones, used for imaging, inspection, or data collection.

7009.3 Scope. This policy applies to all BCVWD departments, employees, contractors, and third-party service providers involved in the procurement, operation, or management of drones used on behalf of the District.

7009.4 Policy Details

7009.4.1 Authorization and Registration

a. Only drones explicitly approved by the Information Technology Department may be used for District purposes.
b. All drones must be registered with the appropriate regulatory authority, such as the Federal Aviation Administration (FAA), where applicable.
c. A designated inventory of drones, including serial numbers and authorized users, will be maintained by the IT Department.
d. All District-owned drones must be covered under a current insurance policy that includes appropriate liability, damage, and equipment loss coverage.
e. Third-party operators must provide proof of insurance with sufficient coverage limits, naming BCVWD as an additional insured when required by contract or project scope.

7009.4.2 Operator Qualifications

a. Drone operators must hold a valid Certificate (for aerial drones) or equivalent qualification as applicable.
b. Only personnel who have completed District-approved training on drone safety and operational procedures may operate drones.
c. A record of training and certification must be maintained and verified by the Information Technology Department and stored in the personnel file located with the Human Resources Department.

7009.4.3 Operational Restrictions and Safety

a. Drones must not be flown over private property, individuals, or restricted areas without proper clearance or consent.
b. Flights must comply with FAA altitude restrictions, no-fly zones, and airspace classification rules.
c. Underwater drones must not be deployed without prior approval and an appropriate safety and recovery plan.
d. Drone operations must be suspended immediately in unsafe conditions (e.g., high winds, electrical storms, poor visibility).

7009.4.4 Data Collection and Privacy

a. Drone footage, images, or sensor data are considered District property and must be stored in District-approved systems.

b. Data must not be distributed externally without prior authorization.
c. All drone operations must respect individual privacy rights and comply with CPRA and applicable data protection regulations.

7009.4.5 Security and Cyber Risk

a. Drones with data storage or wireless communication capabilities must be configured in accordance with NIST security standards.
b. Only firmware and software approved by the IT Department may be installed on drone systems.
c. Unauthorized network-connected drones or non-secure remote access capabilities are prohibited.
d. If a drone is lost, damaged, or suspected to have been compromised, the incident must be reported immediately to the IT Department for risk assessment and response.
e. Flight logs, operational records, and mission data must be retained for at least one year and stored in a District-approved system.

7009.4.6 Third-Party Contractors

a. Contractors operating drones on behalf of BCVWD must sign an agreement confirming adherence to this policy.
b. Third-party operators must provide proof of current FAA licensing, insurance coverage, and cybersecurity safeguards.
c. All collected data must be transferred to BCVWD at project completion and may not be retained without explicit written permission.

7009.4.7 Prohibited Activities

a. Personal drone use on District property is prohibited.
b. Drones may not be used for surveillance, monitoring employees, or capturing unauthorized footage.
c. Use of drones for recreational, non-operational, or commercial purposes unrelated to District business is not permitted.

7009.5 Review and Revision Policy. The Information Technology Department will review the "Drone Usage Policy" annually to ensure it remains aligned with evolving regulations, technologies, and District needs. During this review, the policy will be evaluated for compliance with FAA Part 107 rules, cybersecurity standards (e.g., NIST), CPRA, and California law. Any necessary revisions will be made to maintain legal compliance, operational safety, and data security.

EXHIBIT B

POLICY TITLE: ELECTRONIC SIGNATURE
POLICY NUMBER: 7010

7010.1 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. This policy also aligns with legal requirements for the use of electronic signatures in governmental operations.

7010.2 Purpose . The purpose of this policy is to define the standards, procedures, and controls for the use of electronic signatures in official District business. The policy ensures that electronic signatures are legally binding, secure, and compliant with federal and California state laws, including the Uniform Electronic Transactions Act (UETA), the California Government Code §16.5, and other applicable legal frameworks.

7010.3 Scope. This policy applies to all BCVWD employees, contractors, vendors, and third parties who generate, sign, approve, or process official District documents using electronic signatures. It covers internal workflows and external communications where signatures are required.

7010.4 Policy Details

7010.4.1 Approved Signature Platforms

A. Only electronic signature solutions approved by the Information Technology Department may be used.
B. Approved platforms must support identity verification, audit trails, access control, and cryptographic protection.
C. Unauthorized platforms or tools are prohibited for signing District-related documents.

7010.4.2 Legal and Regulatory Compliance

A. All electronic signatures must comply with:
   - California Government Code §16.5
   - California Uniform Electronic Transactions Act (UETA)
   - Federal Electronic Signatures in Global and National Commerce (E-SIGN) Act
B. Electronic signatures must only be used where legally permissible and not for documents that require notarization unless specifically authorized by law.

7010.4.3 Identity Verification and Security

A. Digital certificates issued and managed by the Information Technology Department must be used to authenticate signer identity and secure signatures.
B. Employees must coordinate with the Information Technology Department for certificate issuance, renewal, and secure storage.
C. All electronic signature events must be logged and include the signer's identity, date/time, and document hash or audit trail.
D. Digital certificates must be revoked immediately upon employee separation, role change, or suspected compromise. The Information Technology Department shall maintain a certificate revocation list and ensure deprovisioning occurs within 24 hours of notification.

7010.4.4 Document Control and Records Retention

A. Electronically signed documents must be retained in accordance with BCVWD's Electronic Data Retention and Records Management Policy.

B. Signed documents must be stored in secure District-managed file systems..
C. Platforms used must ensure document integrity through cryptographic validation or signature locking.

7010.4.5 Roles and Responsibilities

A. The Information Technology Department is responsible for approving platforms, issuing digital certificates, and maintaining audit logs.
B. Employees must report any suspected misuse or loss of certificate credentials to the IT Department immediately.

7010.4.6 Prohibited Activities

A. Electronic signatures must not be applied by anyone other than the authorized signer.
B. Use of another employee's digital certificate or login credentials is strictly prohibited.
C. Electronic signatures must not be used for non-District business.

7010.5 Review and Revision Policy. The Information Technology Department will review the "Electronic Signature Policy" annually to ensure it remains current and effective in addressing the needs of the organization and any changes in legal, 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, state, and federal laws. 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: ACCESSIBILITY
POLICY NUMBER: 7012

7012.1 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. This policy also supports the District's obligation to provide accessible digital services to all individuals, including those with disabilities.

7012.2 Purpose . The purpose of this policy is to establish requirements and best practices that ensure BCVWD's digital resources, including websites, applications, and electronic documents, are accessible to all users regardless of disability. The policy aligns with applicable accessibility standards and legal requirements, including Section 508 of the Rehabilitation Act, the Americans with Disabilities Act (ADA), and Web Content Accessibility Guidelines (WCAG) 2.1.

7012.3 Scope. This policy applies to all digital platforms, services, systems, applications, and content developed, maintained, or procured by BCVWD, including internal and public-facing resources. It covers employees, contractors, third-party vendors, and consultants involved in creating, managing, or delivering digital content or IT systems.

7012.4 Policy Details

7012.4.1 Accessibility Standards and Compliance

A. All BCVWD digital resources must meet or exceed WCAG 2.1 Level AA conformance standards.
B. b. Procured digital services and products must be reviewed by the Information Technology Department for accessibility compliance prior to publishing on any district website or resource.
C. Electronic documents (e.g., PDFs, Word documents, presentations) shared internally or with the public must be designed for accessibility, including appropriate headings, alt text, readable fonts, and tagged structures.
D. All new web applications and content must be tested for accessibility using automated and manual tools prior to deployment.
E. Accessibility will be considered throughout the system lifecycle, from design and procurement to maintenance and decommissioning.
F. Mobile accessibility standards must be met when required by law, regulation, or contractual obligation.

7012.4.2 Employee Responsibilities

A. Employees who create or manage digital content are responsible for ensuring their work complies with accessibility standards.
B. Training on accessible content creation and inclusive design practices will be made available to relevant staff.
C. Any known accessibility issues must be reported to the Information Technology Department for review and resolution.

7012.4.3 Procurement and Vendor Requirements

A. All third-party vendors and contractors developing or hosting digital services for BCVWD must comply with accessibility requirements outlined in this policy and in procurement documents.
B. Contracts must include accessibility clauses that mandate WCAG 2.1 compliance, Section 508 compatibility, and remediation timelines.
C. Vendors must provide a Voluntary Product Accessibility Template (VPAT) upon request or when submitting solutions for approval.

7012.4.4 Remediation and Monitoring

A. The Information Technology Department will routinely audit BCVWD's digital properties for accessibility compliance.

B. Issues identified through audits, complaints, or user feedback must be documented and addressed with a corrective action plan.
C. Legacy systems and content must be prioritized for remediation based on frequency of use, criticality, and visibility to the public.

7012.4.5 Public Feedback and Accommodation Requests

A. BCVWD will provide clear mechanisms on its website and digital platforms for the public to report accessibility barriers or request accommodations.
B. Requests for alternative formats or accessible services will be responded to promptly and handled in coordination with relevant departments (e.g. IT, Administration or Human Resources).

7012.4.6 Legal and Regulatory Compliance

A. This policy supports compliance with the Americans with Disabilities Act (ADA), Section 508 of the Rehabilitation Act, California Government Code Sections 7405 and 11135, and other applicable federal and state mandates. In addition, in accordance with California Government Code Section 54954.2(a)(2)(A), BCVWD will make agendas and related public meeting materials available in alternative formats upon request to ensure persons with disabilities have equal access to public meetings.
B. Digital accessibility is considered a public service obligation under California law and BCVWD's transparency and equity commitments.
C. Any security controls implemented on public-facing websites or digital services must not create unnecessary barriers to accessibility. Such controls must align with NIST guidance on balancing cybersecurity with usability and public access requirements.

7012.5 Review and Revision Policy. The Information Technology Department will review the "Accessibility Policy" annually to ensure it remains current and effective in addressing the needs of the organization and any changes in legal, regulatory, or technological requirements. During the review process, the policy will be evaluated for its effectiveness, compliance with relevant accessibility standards, alignment with the National Institute of Standards and Technology (NIST), and adherence to applicable state and federal laws. Necessary updates or revisions will be made to ensure the policy continues to meet the District's mission and obligations.