RESOLUTION 2025-31

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 new sections are added per the attached exhibits as indicated below:

a.	Policy 7013	Personally Identifiable Information (PII)
b.	Policy 7014	Artificial Intelligence (AI)
c.	Policy 7015	Security Awareness and Training
d.	Policy 7016	Internet of Things (IoT)
e.	Policy 7017	Non-IT Approved Software Purchasing Policy

ADOPTED this 28 day of August, 2025, by the following vote:

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

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

Attachments: Exhibits A - E

EXHIBIT A

POLICY TITLE: PERSONALLY IDENTIFIABLE INFORMATION (PII)
POLICY NUMBER: 7013

7013.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) is committed to safeguarding the Personally Identifiable Information (PII) of its employees, customers, vendors, and other stakeholders. As a public utility and California Special District, BCVWD recognizes its responsibility to protect sensitive information in alignment with the National Institute of Standards and Technology (NIST) guidance (particularly NIST SP 800-122) and the California Public Records Act (CPRA), while maintaining operational transparency and accountability.

7013.2 Purpose. The purpose of this policy is to establish clear roles, responsibilities, and safeguards for collecting, storing, processing, accessing, and disposing of PII. This policy ensures BCVWD protects PII from unauthorized disclosure, use, or loss while maintaining compliance with applicable federal and state privacy laws.

7013.3 Scope. This policy applies to all BCVWD personnel, contractors, consultants, and third-party vendors who have access to systems, documents, or platforms that contain PII. It covers PII in physical or electronic form, including but not limited to:

- Full names (when combined with other data)
- Social Security Numbers (SSNs)
- Driver's license or state ID numbers
- Passport or visa numbers
- Financial account or credit/debit card information
- Medical or health-related data
- Employee ID numbers or HR records
- Utility customer account information (e.g., usage history, billing data)

7013.4 Policy Details

7013.4.1 Collection and Minimization

a. PII collection must be limited to what is legally required or operationally essential.
b. Departments must justify any new collection of PII through a business case approved by the organization and the Information Technology and Cybersecurity Department.
c. Data minimization principles must be followed, collecting the least amount of PII necessary to perform a task.

7013.4.2 Storage and Classification

a. PII must be classified and protected accordingly to prevent unauthorized access.
b. Electronic PII must be stored on secure, access-controlled systems managed by the Information Technology and Cybersecurity Department.
c. Physical PII must be secured in locked cabinets or restricted areas with controlled access.

7013.4.3 Access and Use

a. Access to PII is limited to employees with a demonstrated business need, governed by Role-Based Access Control (RBAC).
a. PII may not be transmitted via unencrypted email, portable media, or unsecured networks.
b. PII must never be entered into unauthorized applications, websites, or artificial intelligence tools (see Policy 7014 – AI Policy).
c. Use of PII for training, testing, or demonstration purposes is prohibited unless it has been properly anonymized or masked.

7013.4.4 Disclosure and Third Parties

a. PII may only be shared externally when required by law, approved by District counsel, or governed by a data sharing agreement.
b. All vendors and third-party service providers handling PII must sign agreements requiring compliance with this policy and applicable laws, including CPRA.
c. Public records requests involving PII must be reviewed in accordance with CPRA exemptions and handled by designated staff.

7013.4.5 Retention and Disposal

a. PII must be retained only as long as necessary for operational, legal, or regulatory purposes.
b. Disposal of PII must be performed using approved secure methods (e.g., digital wiping, document shredding, etc.).
c. Logs of disposal activities must be retained for audit purposes.

7013.4.6 Training and Awareness

a. All employees must complete annual privacy and security training that includes the handling of PII.
b. Departments must provide targeted guidance to employees who handle PII in high-risk areas such as Human Resources, Finance, and Information Technology and Cybersecurity.
c. Any suspected PII breach or exposure must be reported immediately to the Information Technology and Cybersecurity Department for appropriate response.

7013.5 Review and Revision Policy. The Information Technology and Cybersecurity Department will review the “Personally Identifiable Information (PII) Policy” annually, or as needed in response to changes in law or technology. This review ensures ongoing compliance with NIST, CPRA, and other applicable federal and state privacy regulations. Revisions will be made to ensure continuous improvement of PII handling practices and to address emerging privacy risks.

EXHIBIT B

POLICY TITLE: ARTIFICIAL INTELLIGENCE (AI)
POLICY NUMBER: 7014

7014.1 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) Cybersecurity Framework and Artificial Intelligence Risk Management Framework (AI RMF 1.0). 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 recognizes the rapid growth and integration of artificial intelligence (AI) in modern IT environments and establishes foundational principles for the responsible use of AI across the District.

7014.2 Purpose. The purpose of this policy is to provide guidance for the ethical, secure, and authorized use of artificial intelligence technologies by BCVWD employees, contractors, and vendors. It aims to protect District data, maintain public trust, and establish governance over AI use that aligns with state law, cybersecurity best practices, and evolving industry standards.

7014.3 Scope. This policy applies to all forms of AI technologies, including but not limited to: Generative AI tools (e.g., ChatGPT, Claude, Gemini), Predictive analytics and machine learning models, AI embedded within third-party applications and services, Image recognition, document summarization, or automated decision support tools. The policy governs use by employees, contractors, and vendors in any capacity involving District data, systems, communications, or services.

7014.4 Policy Details

7014.4.1 Governance Oversight

a. Use of any AI tool for official District business must be approved by the Information Technology Department.
b. Unauthorized use of AI tools on District systems or with District data is prohibited.
c. AI systems must be evaluated for data privacy risks, output reliability, and compliance with security policies prior to use.
d. The District may prohibit use of certain AI tools deemed insecure, untrustworthy, or misaligned with regulatory requirements.

7014.4.2 Data Protection and Input Restrictions

d. No personally identifiable information (PII), personnel records, customer data, infrastructure details, or confidential internal documents may be entered into AI systems, whether public or private, without prior approval.
e. Only de-identified, publicly available, or non-sensitive data may be used with AI tools, and only for legitimate business functions.
f. AI tools must not be used to generate, analyze, or infer sensitive characteristics about individuals or groups without a documented business case and prior written approval.

7014.4.3 Output Validation and Records

a. AI-generated content used for any external communication, decision-making, or record-keeping must be reviewed and validated by a human to ensure accuracy.
d. Employees must ensure all AI-generated outputs meet BCVWD standards for accuracy, professionalism, and compliance with legal obligations.

7014.4.4 Procurement and Vendor Controls

a. Any vendor solution incorporating AI functionality must undergo review and risk assessment by the Information Technology Department.
b. AI components in vendor platforms must comply with the same security, privacy, and data protection requirements as other IT services.
c. Contracts must address data ownership, model transparency, and vendor accountability for misuse or incorrect outputs.

7014.4.5 Employee Responsibilities

a. Employees must use AI in a manner that upholds BCVWD values, avoids bias or discrimination, and ensures public trust.
b. Any suspected misuse of AI, violation of this policy, or output that could impact public records or operations must be reported to the Information Technology Department.
c. Training on safe and appropriate AI use will be provided as part of the District's ongoing cybersecurity awareness training efforts.

7014.4.6 Compliance and Oversight

a. The Information Technology Department will maintain oversight over the use of AI and emerging technologies and may periodically audit use cases for compliance.
b. This policy will be updated regularly to reflect changes in technology, regulations, and risk environments.
c. Violations of this policy may result in disciplinary action, up to and including loss of system access or employment consequences, as outlined in the Acceptable Use Policy policy.

7014.5 Review and Revision Policy. The Information Technology Department will review the "Artificial Intelligence Policy" at least annually or as needed based on technological advancements, regulatory updates, and risk assessments. The review will ensure continued alignment with the National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (AI RMF), applicable state and federal laws, and BCVWD's mission to deliver secure and ethical digital services.

EXHIBIT C

POLICY TITLE: SECURITY AWARENESS AND TRAINING
POLICY NUMBER: 7015

7015.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) relies on Information Technology (IT) resources as essential tools for conducting business efficiently and securely. To mitigate human risk and ensure effective cybersecurity, BCVWD maintains a proactive Security Awareness and Training Program. This policy aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST Special Publication 800-50 to promote awareness, accountability, and readiness among employees, contractors, and leadership. As a California Special District, BCVWD also complies with relevant state laws, including the California Public Records Act (CPRA), and embraces its role in protecting public trust and information systems.

7015.2 Purpose. The purpose of this policy is to establish standards for delivering security awareness and training to all individuals who access BCVWD information systems. The goal is to ensure users understand their cybersecurity responsibilities and are equipped to recognize and respond appropriately to cyber threats.

7015.3 Scope. This policy applies to all BCVWD employees, contractors, and third parties who are granted access to the District's technology infrastructure, including computers, mobile devices, applications, cloud services, and sensitive data. It covers onboarding, continuous training, and role-specific education related to information security risks and responsibilities.

7015.4 Policy Details

7015.4.1 Security Awareness and Training Program Structure

e. All users must complete mandatory cybersecurity training annually as a condition of continued access to District systems.

b. Refresher training will be delivered mid-year (at six-month intervals) to reinforce key concepts and address emerging threats.

c. Micro-training and situational updates will be provided throughout the year, customized by department or function (e.g., Information Technology, Finance, Human Resources, Customer Service, Accounts Payable/Receivable, Executives).

d. Training content will cover core threat topics, including but not limited to:
   - Phishing and social engineering
   - Password and credential protection
   - Safe use of mobile and remote access
   - Insider threats and data misuse
   - Ransomware and malware prevention
   - Public sector-specific risks

7015.4.2 Training Delivery and Tracking

a. Training will be administered by the Information Technology and Cybersecurity Department utilizing an easy-to-access learning management or secure training platform.

b. Participation in training is mandatory and will be logged, tracked, and audited by the Information Technology and Cybersecurity Department.

c. Failure to complete required training within designated timeframes may result in temporary suspension of system access or additional corrective action.

7015.4.3 Role Based and Specialized Training

a. Additional role-specific training will be provided to personnel in positions with elevated security responsibilities or access to sensitive information, such as:

- Information Technology administrators
- Finance and payroll personnel
- Human Resources and confidential records custodians
- Customer-facing staff managing account data
- Executives with decision-making or incident response authority

b. These training courses will be updated as job roles evolve, threat vectors change, or regulations are revised.

7015.4.4 Reinforcement and Continuous Awareness

a. The Information Technology and Cybersecurity Department will distribute periodic security bulletins, tips, or alerts to reinforce a security-first culture.
b. Posters, email campaigns, and desktop notices may also be used to promote ongoing awareness.
c. Users are encouraged to report suspicious activities or questions to the IT Department without fear of reprisal.

7015.4.5 Compliance Monitoring and Oversight

a. The Information Technology and Cybersecurity Department will regularly monitor compliance with this policy, review training metrics, and assess the effectiveness of training content.
b. Periodic audits may be conducted to verify participation and measure employee readiness.
c. Lessons learned from incident response activities will be used to refine the training program.

7015.4.6 Responsibilities

a. The Information Technology and Cybersecurity Department is responsible for designing, updating, and delivering the training curriculum.
b. Human Resources and Department supervisors are responsible for ensuring their teams complete assigned training and meeting all deadlines assigned by the Information Technology and Cybersecurity Department.
c. All users are responsible for completing required training and following secure practices in daily operations.

7015.5 Review and Revision Policy. The Information Technology and Cybersecurity Department will review the "Security Awareness and Training Policy" annually to ensure it remains current and responsive to emerging threats, evolving technologies, and regulatory changes. During the review process, the policy will be evaluated for alignment with the NIST Cybersecurity Framework and NIST SP 800-50. Necessary updates or revisions will be made to ensure the policy continues to meet the District's risk management and compliance requirements.

EXHIBIT D

POLICY TITLE: INTERNET OF THINGS (IoT) SECURITY
POLICY NUMBER: 7016

7016.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) recognizes the growing integration of Internet of Things (IoT) technologies across critical infrastructure and operations, including sensors, smart meters, wireless devices, and environmental monitoring systems. This policy establishes a security framework for the management and control of IoT devices in alignment with the National Institute of Standards and Technology (NIST) standards, including NIST SP 800-213 and the NIST Cybersecurity Framework (CSF). As a California Special District, BCVWD also adheres to the California Public Records Act (CPRA) to ensure transparency and accountability in data management and public trust.

7016.2 Purpose. The purpose of this policy is to define security requirements for the deployment, management, and operation of all IoT devices used by BCVWD. The policy is designed to mitigate the risk of unauthorized access, data breaches, and cyber-physical system vulnerabilities resulting from improperly configured or unmanaged IoT assets.

7016.3 Scope. This policy applies to all IoT devices connected to BCVWD's networks or systems, including, but not limited to:

- Smart meters and pressure sensors
- Surveillance and security cameras
- Building automation and HVAC systems
- Water treatment instrumentation and telemetry
- Remote monitoring systems (e.g., SCADA components)
- Embedded systems and field-deployed hardware
- Industrial IoT devices
- Voice assistants or smart displays, if ever deployed
- Mobile-connected devices such as GPS trackers
- Any network-connected or Bluetooth-enabled physical device
- Any third-party IoT systems integrated into BCVWD infrastructure

7016.4 Policy Details

7016.4.1 Governance and Ownership

a. All IoT devices must be owned, approved, configured, and maintained by the Information Technology and Cybersecurity Department.

b. Personal or employee-owned IoT devices (e.g., smartwatches, fitness trackers, home assistants, or IP cameras) are prohibited from connecting to BCVWD's secure network infrastructure.

c. In cases where personal devices are authorized under the Bring Your Own Device (BYOD) Policy, they may only connect to designated guest wireless networks, which are logically segmented and isolated from BCVWD's operational networks.

7016.4.2 Procurement and Authorization

a. All IoT device acquisitions must be reviewed and approved by the Information Technology and Cybersecurity Department.

b. Devices must meet baseline security and interoperability standards, including:
   - Support for firmware upgrades and patching
   - Device authentication mechanisms
   - Secure transmission protocols (e.g., TLS)
   - Minimal attack surface by default

c. Vendors must provide documentation regarding firmware lifecycle, known vulnerabilities, and any embedded third-party code.

7016.4.3 Network Segmentation and Access Control

a. All IoT devices must be deployed in logically segmented network zones to minimize lateral movement and reduce potential impact from device compromise.
b. Role-based access controls (RBAC) must be applied to limit device access to essential personnel.
c. Default credentials must be changed prior to deployment; multi-factor authentication (MFA) must be enforced where supported.

7016.4.4 Monitoring and Maintenance

a. IoT devices must be registered in the District's Asset Inventory and managed by the Information Technology and Cybersecurity Department.
b. All IoT devices must be monitored for unusual behavior, unauthorized access attempts, or connectivity issues using automated alerting and logging systems.
c. Firmware and software must be updated promptly in response to security advisories or patches issued by manufacturers.

7016.4.5 Data Handling and Security

a. IoT devices must not collect, transmit, or store personally identifiable information (PII), customer account data, or employee records unless expressly authorized and protected through encryption and role-based access.
b. Where anonymized data is collected (e.g., environmental readings), it must be verified to contain no indirectly identifying information.

7016.4.6 Risk Management and Resilience

a. IoT deployment must undergo cybersecurity risk assessment prior to installation, including evaluation of physical risks and cybersecurity exposure.
b. Devices that are deemed obsolete, unsupported, or vulnerable must be decommissioned by the Information Technology and Cybersecurity Department.
c. IoT-related incidents will be managed under the Incident Response Policy and must be reported immediately to the Information Technology and Cybersecurity Department.

7016.5 Review and Revision Policy. The Information Technology and Cybersecurity Department will review the "IoT Security Policy" annually to ensure alignment with evolving NIST guidance, industry best practices, regulatory mandates, and the expanding IoT threat landscape. Revisions will be made to ensure the policy remains effective in mitigating risk and securing BCVWD's infrastructure and public trust.

EXHIBIT E

POLICY TITLE: NON-IT APPROVED SOFTWARE PURCHASING POLICY
POLICY NUMBER: 7017

7017.1 Introduction. Beaumont-Cherry Valley Water District (BCVWD) prioritizes the secure, efficient, and compliant acquisition and use of software throughout the organization. In accordance with National Institute of Standards and Technology (NIST) best practices and the District's cybersecurity risk management framework, all software procurement and deployment must be carefully vetted to prevent data exposure, ensure interoperability, and reduce third-party risk. This policy ensures that no software is purchased, installed, or used without the involvement and explicit approval of the Information Technology and Cybersecurity Department.

7017.2 Purpose. The purpose of this policy is to:

- Prevent the introduction of unvetted or insecure software into BCVWD systems.
- Ensure data security, confidentiality, and privacy (including PII protection).
- Ensure compliance with NIST, CPRA, and internal cybersecurity requirements.
- Evaluate third-party software providers for risk related to data access, encryption, and storage.
- Maintain operational integrity, system compatibility, and centralized support.

7017.3 Scope. This policy applies to all BCVWD departments, employees, contractors, consultants, and third-party vendors who seek to acquire or utilize software, including desktop applications, mobile apps, SaaS platforms, cloud-based tools, and browser plugins, within the District's technology environment.

7017.4 Policy Details

7017.4.1 Software Procurement and Approval

a. All software purchases, subscriptions, or free installations must be submitted in advance for review and approval by the Information Technology and Cybersecurity Department.
b. No department or individual is authorized to purchase, download, or use software, regardless of cost, without prior authorization.
c. Procurement requests must include a description of business need, technical requirements, and intended users.
d. The IT Department will evaluate software for compatibility with District systems and cybersecurity standards.

7017.4.2 Third-Party Risk Assessments

a. All third-party software is subject to a risk assessment prior to approval. This includes review of:
    - Vendor reputation and history
    - Data handling practices
    - Access permissions and authentication methods
    - Where and how data is stored (e.g., domestic vs. international storage)
    - Encryption at rest and in transit
    - Security certifications (e.g., SOC 2 Type II, ISO 27001)
    - Vendors must complete cybersecurity and compliance questionnaires upon request.

7017.4.3 Data Protection and Privacy

a. Software solutions that process or store personally identifiable information (PII), employee records, customer data, or internal District files must meet CPRA and NIST security requirements.
b. The District prohibits the use of software that transmits unencrypted sensitive data over the internet.

c. The use of AI-enabled or analytics platforms that extract user behavior or confidential content must be approved under the District's AI Policy (7014).

7017.4.4 Integration and Compatibility

a. Approved software must integrate with existing systems, infrastructure, and cybersecurity protocols.
b. Solutions that conflict with current technologies or introduce vulnerabilities will be rejected.
c. Cloud-based tools must comply with the District's Cloud Computing Policy (7003).

7017.4.5 BYOD and Personal Software

a. As outlined in the BYOD Policy (7002), personal software or tools may not be used to process or store BCVWD data.
b. Use of any personal or department-purchased software on District-issued devices is prohibited without IT Department approval.

7017.4.6 Unauthorized Software Use

a. The Unauthorized or unapproved software discovered on District systems will be subject to removal without notice.
b. Employees found to be installing, using, or facilitating use of non-approved software may be subject to disciplinary action in accordance with District policy.

7017.5 Review and Revision Policy. The Information Technology and Cybersecurity Department will review the "Non-IT Approved Software Purchasing Policy" annually or upon the introduction of significant new threats, technologies, or regulatory requirements. This review ensures continued alignment with NIST cybersecurity standards, California laws such as the California Public Records Act (CPRA), and internal operational objectives. Updates will be made to preserve data integrity, prevent third-party risk, and maintain the security posture of the District.