COLORADO WATER RESOURCES & POWER DEVELOPMENT AUTHORITY

BOARD PROGRAM WORK SESSION (BPWS) AGENDA

March 5, 2026
3:00 pm

Board Members: Mike Fabbre (Chair), Steve Vandiver, Eric Wilkinson, Chris Treese, Patti Wells, Matt Shuler, Karen Wogsland, Roy Heald, and Bruce Whitehead.

Authority Staff: Keith McLaughlin, Jim Griffiths, Justin Noll, Wesley Williams, Ian Loffert, Gio Gazashvili and Kevin Carpenter.

Others present: Desi Santerre (DOLA), Alex Hawley (WQCD).

AGENDA

1. DWRF and WPCRF loan capacity – For discussion only. (Gio, Wes)

2. Wastewater Maximum and Per Entity Loan Limits – Discussion and possible action. (Wes)

3. Information Systems policy review – Discussion and possible action. (Jim)

4. Interim Loan Program – Discussion and possible action. (Jim)

5. April retreat and BPWS topics – For discussion only. (Keith)

6. RFP for Auditors - For discussion and if time allows. (Keith, Justin)

BACK TO AGENDA

COLORADO WATER RESOURCES &
POWER DEVELOPMENT AUTHORITY
The Amp - Suite 820, 1580 N. Logan Street, Denver, Colorado 80203-1942
303/830-1550 · Fax 303/832-8205 · info@cwrpda.com

MEMORANDUM

March 6, 2026

TO: **Board of Directors and Karl Ohlsen**

FROM: **Wesley Williams, Finance Director**
Ian Loffert, Assistant Finance Director

RE: **Water Pollution Control Revolving Fund ("WPCRF")**
WPCRF Loan Limit Recommendation

The Authority Board of Directors establishes loan limits for both base program and Infrastructure Investment and Jobs Act/Bipartisan Infrastructure Law ("IIJA/BIL") funding as needed to manage program capacity and demand.

At its December 2, 2022, meeting, the Board established a WPCRF loan limit per entity of $18 million. At that time, available WPCRF funding was constrained, and the limit was implemented to ensure funds could be distributed across a greater number of entities.

Over the last few years, the WPCRF program has experienced a decline in loan demand resulting in increased available program capacity. Given current demand levels, the $18 million cap is no longer necessary to preserve program capacity. Additionally, larger WPCRF projects have had to seek out other funding sources due to the current loan limit.

Staff recommends that the Board increase the WPCRF loan limit per entity from $18 million to $25 million.

This proposed increase would:

- Provide additional flexibility to finance larger wastewater projects
- Allow larger entities to meet more of their capital needs through the WPCRF program
- Maintain overall program capacity given current application levels

The proposed limit would apply to all WPCRF loans:

Loan Program & Type	Limit Per Entity
All WPCRF Loans (individual base and IIJA/BIL loans as well as combined base + IIJA/BIL loans)	$25 million

Board Action: Staff recommends that the Board approve increasing the WPCRF loan limit per entity from $18 million to $25 million at the March 6, 2026, Board meeting.

BACK TO AGENDA

BACK TO AGENDA

COLORADO WATER RESOURCES
POWER DEVELOPMENT AUTHORITY
The Amp - Suite 820, 1580 N. Logan Street, Denver, Colorado 80203-1942
303/830-1550 · Fax 303/832-8205 · info@cwrpda.com

MEMORANDUM

March 6, 2026

TO: **Board of Directors and Karl Ohlsen**

FROM: **Jim Griffiths, Deputy Director**

RE: **Information Systems Policy 2026 – Annual Review and Approval**

The Information Systems (IS) Policy follows this memo. Staff and the Authority's IS consultant (MyTech) reviewed the IS Policy and made several changes that are shown in "redline".

Staff recommends approval of this policy with the changes for another year.

BACK TO AGENDA

Information Systems Policy, version 4.0.0

Status: ☒ Working ☐ Draft ☐ Approved ☐ Adopted

Last Review Date: April 25, 2025

Information Systems Policy

Purpose

T~~he purpose of t~~he CWRPDA Information Systems Policy ~~is to~~ establishes acceptable practices ~~regarding~~for the use of CWRPDA **Information Resources ("Information Resources" is defined as but not limited to the storing, processing and transmitting of any data, verbally, virtually, paper, digitally)** in order to protect the confidentiality, integrity and availability of information created, collected, and maintained by the CWRPDA.

Audience

The CWRPDA Information Systems Policy applies to any individual, entity, or process that interacts with any CWRPDA **Information Resource**.

Contents

Acceptable Use	Asset Management
Access Management	Mobile Devices and Bring Your Own Device (BYOD)
Authentication/Passwords	Physical Security
Clear Desk/Clear Screen	Privacy
Data Security	Removable Media
Email and Electronic Communication	Security Training and Awareness
Hardware and Software	Social Media
Internet	Voice Mail
Malware Defense	Incidental Use

Policy

Acceptable Use

- Personnel are responsible for complying with CWRPDA policies when using CWRPDA **information resources** at all times.
- Personnel must promptly report the theft, loss, or unauthorized disclosure of CWRPDA **confidential** or **internal information** to your department manager.

Personnel must not purposely engage in activity using CWRPDA Information Resources or on CWRPDA time that may

- harass, threaten, or abuse others;
- degrade the performance of CWRPDA **Information Resources**;
- deprive authorized CWRPDA personnel access to a CWRPDA **Information Resource;**
- obtain additional Information Technology (IT) resources beyond those approved by CWRPDA management ("CWRPDA Management" is defined as Executive Director, Deputy Director, Finance Director, Office Manager, Controller);
- Circumvent CWRPDA computer measures.

- Personnel must not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, CWRPDA personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any CWRPDA **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blue prints, software codes, computer programs, data, writings, and technical information, developed on CWRPDA time and/or using CWRPDA **Information Resources** are the property of CWRPDA.
- Use of encryption must be managed in a manner that allows designated CWRPDA personnel to promptly access all data.
- CWRPDA **Information Resources** are provided to facilitate company business and must not be used for personal financial gain.
- Personnel must cooperate with incident investigations, including any federal or state investigations.
- Personnel must respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using CWRPDA **Information Resources**.
- Personnel must not intentionally access, create, store or transmit material that CWRPDA deems to be offensive, indecent, or obscene.

Access Management

- Personnel are permitted to use only those network and host addresses issued to them and must not attempt to access any data or programs contained on CWRPDA systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal CWRPDA networks and/or environments must be made through approved and CWRPDA-provided virtual private networks (VPNs), and remote desktop server.
- Multi-factor authentication (MFA) must be used to access the network remotely and any other necessary applications.
- Personnel must not divulge any access information to anyone not specifically authorized to receive such information.
- Personnel must not share their CWRPDA authentication information unless such sharing is expressly approved in advance by management, including:
    - Account passwords,

  - Personal Identification Numbers (PINs),
  - Access cards, keys and door codes,
  - Digital certificates,
  - Similar information or devices used for identification and authentication purposes.
- Lost or stolen access cards, door codes, and keys must be reported to your department manager as soon as practical.
- A service charge may be assessed for access cards and/or keys that are lost, stolen, or are not returned.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- CWRPDA Management encourages the use of password management software (Lastpass as one example) for password management.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following CWRPDA rules:
  - Must not be easily tied back to the account owner by including readily-identifiable information, such as: user name, social security number, nickname, relative's names, birth date, etc.
  - Shall not include only common words, such as dictionary words or acronyms.
  - Shall not be the same passwords as used for non-business purposes.
  - Use of numbers and special characters is recommended (*&^%$#).
  - Use of upper and lower case recommended.
- Password history must be kept to prevent the reuse of passwords.
- Unique passwords shall be used for each system.
- User account passwords must not be divulged to anyone outside CWRPDA staff and IT contractors.
- ~~Passwords must be provided to authorized CWRPDA management on demand or upon termination of the relationship with CWRPDA, if issued.~~Management will use administrative access and other procedures to manage account users and user privileges within our systems and will not require employees to provide passwords to management.
- If the security of a password is in doubt, the password shall be changed immediately.

Clear Desk/Clear Screen

- Personnel must log off from applications or network services when they are no longer needed.
- Personnel must log off or lock their workstations and laptops when their workspace is unattended.

- Confidential or internal information must be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- ~~Personal items, such as phones, wallets, purses and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.~~
- File cabinets containing **confidential information** must be locked when not in use or when unattended.
- Physical and/or electronic keys used to access **confidential information** must not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Copies of documents containing **confidential information** must be removed immediately from printers and fax machines.

Data Security

- Confidential information is information disclosed to an individual employee or known to that employee as a consequence of the employee's employment at the Authority, not generally known outside the Authority, or is protected by law. Examples of confidential information include but are not limited to social security numbers, payroll and personnel records, health information, credit card information, bank account information, passwords and other IT-related information. Individual departments or programs may have additional types or kinds of information that are considered confidential information and are covered by this policy. Confidential information includes information in any form, such as written documents or records, or electronic data.
- During employment, an employee must hold all confidential information in trust and confidence, and must only use, access, store, or disclose confidential information, directly or indirectly, as appropriate in the performance of the employee's duties for the Authority. An employee must comply with all applicable state and federal laws and Authority policies relating to access, use and disclosure of confidential information.
- An employee must not remove materials or property containing confidential information from the employee's department or program area unless it is necessary in the performance of the person's job duties. If materials or property containing confidential information are removed from the Authority, the employee must safeguard the materials/property and control access as necessary. The responsibility to safeguard and control access to materials and property similarly applies to any telework/remote access situation. Upon termination, the employee must secure all such materials/property and copies thereof or return all such materials/property and copies to the employee's supervisor or supervisor's designee.
- An employee must not seek to obtain any confidential information involving any matter which does not involve or relate to the person's job duties.

- If an employee has any question relating to the appropriate use or disclosure of confidential information, the employee shall consult with the employee's supervisor or other appropriate personnel.
- **Confidential information** transmitted via USPS or other mail service must be secured. Packages that are delivered outside of the office, when the office is closed, will be secured as soon as practical.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring **confidential** or **internal information**. Confidential or internal information must only be shared with, or transferred to, other individuals or entities which are authorized by CWRPDA Management to receive such information.
- Information must be shared, handled, transferred, saved, and destroyed appropriately, based on the information sensitivity.
- **Confidential information** must be transported either by a CWRPDA employee or a courier approved by Management.
- All electronic media containing **confidential information** must be securely disposed. Please contact Management for guidance or assistance.

Email and Electronic Communication

- Forwarding of electronic messages containing **confidential information** outside the CWRPDA internal systems is prohibited.
- Electronic communications must not misrepresent the originator or CWRPDA.
- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- CWRPDA Employees must not use personal email accounts to send or receive CWRPDA **confidential information**.
- Any personal use of CWRPDA provided email must not:
  - Involve solicitation.
  - Be associated with any political entity.
  - Have the potential to harm the reputation of CWRPDA.
  - Forward chain emails.
  - Contain or promote anti-social or unethical behavior.
  - Violate local, state, federal, or international laws or regulations.
  - Result in unauthorized disclosure of CWRPDA **confidential information**.
  - Attack, hack or limit service on any other systems on the internet.
- Personnel must send **confidential information** using secure electronic messaging solutions only. Secure electronic messaging includes CWRPDA's standard email provider encryption, and may include certain secure file transfer services and other management approved methods (confidential information includes but is not limited to account information, bank information, certain personnel information and other information as communicated by management).
- Personnel must use caution when responding to, clicking on links within, or opening attachments included in electronic communications.

- Personnel must use discretion in disclosing **confidential** or **internal information** in Out of Office or other automated responses, such as employment data or other sensitive data.

Hardware and Software

- All hardware must be approved by Management before being connected to CWRPDA networks.
- Software installed on CWRPDA equipment must be approved by Management.
- All CWRPDA assets taken off-site should be physically secured at all times.
- Employees must not allow family members or other non-employees to access CWRPDA **Information Resources** unless otherwise approved by the Executive Director.

Malware Defense

Purpose

Malware defense includes the configuration, maintenance, detection, reporting, and remediation of anti-malware software and the malware it identifies. This *Malware Defense Policy* provides the processes and procedures to accomplish those tasks. This policy section applies to all departments and all assets connected to the CWRPDA's network.

Responsibility

- The Information Systems (IS) consultant is primarily responsible for malware defense. Specifically, the IS consultant is responsible for configuring the correct devices to generate, store, and transmit logs. The IS consultant and CWRPDA management are responsible for informing all users of their responsibilities in the use of any assets assigned to them. All CWRPDA assets are required to comply with the malware defense policy and procedures.
- Users are responsible for connecting their devices to the CWRPDA's network and restarting their devices as appropriate.

Exceptions

Exceptions to this policy may occur. Exception requests must be made in writing and must contain:

- The reason for the request,
- Risk to the CWRPDA of not following the written policy,
- Specific mitigations that will be implemented,
- Technical and other difficulties, and
- Date of review.

Exceptions must be made to management and management will inquire with the IS consultant on whether the exception is acceptable or not.

Configuration

- The IS consultant must install anti-malware software on all CWRPDA assets where appropriate.
    - Users must not disable anti-malware software on their CWRPDA assets.
    - Users must not modify the update frequency specified by the IS consultant.

Update

- Anti-malware software must be configured to automatically update.
- The IS consultant must ensure that anti-malware signatures are kept up to date as they become available via an automatic update process.
- Operating systems must be configured to automatically update unless an alternative approved patching process is used.

Detection

- The IS consultant must ensure that anti-malware software is properly functioning on all applicable CWRPDA assets.

Reporting

- All confirmed high severity alerts must be reported to CWRPDA management.
- The presence of unauthorized software must be properly investigated.

Remediation

- Identified malware must be removed from CWRPDA assets.
    - Unauthorized software must be removed from use on CWRPDA assets or receive a documented exception.
    - All exceptions must be documented.

Asset Management

Purpose

CWRPDA asset management is the process of procuring, identifying, tracking, maintaining, and disposing of an asset owned by the CWRPDA. This *Asset Management Policy* provides the processes and procedures for governing the CWRPDA asset lifecycle while the CWRPDA is using an asset. An inventory must be created and maintained to support the CWRPDA's mission. This inventory must be current and reflect the current assets owned and operated by the CWRPDA.

Responsibility

The IS consultant is responsible for all CWRPDA asset management functions. This information is relayed to other departments within the CWRPDA such as finance and accounting as required or needed. The IS consultant and CWRPDA management are responsible for informing all users of their responsibilities in the use of any CWRPDA assets assigned to them.

Acquisition

- The IS consultant shall assign unique identifiers to all existing and newly acquired CWRPDA assets they manage.
- Each managed CWRPDA asset (e.g., desktops, laptops, servers, tablets), where applicable, must have an CWRPDA asset tag affixed to the device with this identifier.

- Record the CWRPDA asset identifier alongside other relevant information within the IS inventory. This is to include:
    - CWRPDA asset identifier
    - Date of purchase
    - Purchase price
    - Item description
    - Manufacturer
    - Model number
    - Serial number
    - Warranty expiration date
- IS consultant must verify the CWRPDA asset inventory every year.

Discovery

- CWRPDA assets not managed by the IS consultant must be investigated, as these assets may be unauthorized.
- Assets owned by the CWRPDA but not managed by IS consultant and not kept within the CWRPDA asset inventory must be added to the inventory.
- Users are required to connect their CWRPDA assets to the CWRPDA network on a weekly basis, where practical.
- The IS consultant must choose to remove the unauthorized asset from the network, deny the asset from connecting remotely to the network, quarantine the asset, or add it if needed.

Usage

- Users must handle all CWRPDA assets with care.
- It is the responsibility of the CWRPDA asset owner to:
    - Maintain control over the CWRPDA asset.
    - Contact the IS consultant with any problems such as malfunctions, needed repairs, and underutilized equipment or in the event of equipment loss.

Controlled Disposal

- CWRPDA assets to be decommissioned or retired must be returned to IS consultant.
- IS consultant must make a copy of the user data, as needed.
- IS consultant will be responsible for the secure erasure of the primary memory storage device within the CWRPDA asset, where applicable.
- IS consultant will be responsible for updating the status of the CWRPDA asset within all CWRPDA management systems.
    - IS consultant must ensure that relevant records are retained.

- Document the removal of the CWRPDA asset from the CWRPDA within the asset inventory.

Uncontrolled Disposal

- All lost or stolen CWRPDA assets must be immediately reported to management and IS consultant.
- Lost and stolen CWRPDA assets must have their access to CWRPDA data revoked as soon as possible.
    - The CWRPDA assets must also be removed from the inventory.

Internet

- The Internet must not be used to communicate CWRPDA **confidential** or **internal information**, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with CWRPDA networking or computing resources shall be for business-related activities. However, incidental use of the internet or CWRPDA information systems is allowed while on personal time. Incidental use is acceptable as long as it does not consume more than a trivial amount of resources, does not interfere with productivity, and does not preempt any business activity. Unapproved activities include, but are not limited to:
    - Recreational games,
    - Accessing or distributing pornographic or sexually oriented materials,
    - Accessing or distributing racists, violent or other potentially offensive material,
    - Broadcasting unsolicited personal views on social, political or religious issues,
    - Attacking, hacking or limiting service on any other systems on the internet,
    - Attempting or making unauthorized entry to any network or computer accessible from the Internet.
- Streaming media or audio will be limited or eliminated if it is impairing or impacting the CWRPDA network.
- Access to the Internet from outside the CWRPDA network using a CWRPDA owned computer, laptop or tablet must adhere to all of the same policies that apply to use from within CWRPDA facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- The use of a personally-owned mobile device to connect to the CWRPDA network is a revocable privilege granted to employees upon approval of Management.
- All personally-owned laptops and/or workstations must have approved virus and spyware detection/protection software along with personal firewall protection active and updated in a frequency consistent with the developers' recommendations.
- CWRPDA confidential information should not be stored on any personally-owned mobile device.

- Theft or loss of any mobile device that has been used to create, store, or access **confidential** or **internal information** must be reported to the CWRPDA management immediately.
- All mobile devices must maintain up-to-date versions of all software and applications.
- All personnel are expected to use mobile devices in an ethical manner.
- Jail-broken or rooted devices should not be used to connect to CWRPDA **Information Resources**.
- In the event that there is a suspected incident or breach associated with a CWRPDA device, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to CWRPDA **Information Resources** may be monitored at the discretion of CWRPDA Management.
- CWRPDA IT support for personally-owned mobile devices is limited to assistance in complying with this policy.
- Use of personally-owned devices must be in compliance with all other CWRPDA policies.
- CWRPDA reserves the right to revoke the privilege of using personally-owned mobile devices for CWRPDA purposes in the event that personnel do not abide by the requirements set forth in this policy.
- Texting or emailing while driving is not permitted while on company time or using CWRPDA resources. Only hands-free talking while driving is permitted while on company time or when using CWRPDA resources.

Physical Security

- Visitors must be accompanied by authorized personnel.
- Eating or drinking are not allowed in the server room. Caution must be used when eating or drinking near workstations or information processing facilities.

Privacy

- Information created, sent, received, or stored on CWRPDA **Information Resources** is not private and may be accessed by CWRPDA management at any time, under the direction of CWRPDA executive management, without knowledge of the user or resource owner.
- CWRPDA may log, review, and otherwise utilize any information stored on or passing through its **Information Resource** systems.
- Systems Administrators, CWRPDA management, and other authorized CWRPDA personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment-related task.
- The Executive Director may grant limited Information System access to CWRPDA vendors such as auditors. Access will be limited to what is needed to perform specific work.

BACK TO AGENDA

Removable Media

- The use of removable media for storage of CWRPDA information must be supported by a reasonable business case.
- All removable media use must be approved by CWRPDA management prior to use.
- Personally-owned removable media use is not permitted for storage of CWRPDA information.
- Personnel are not permitted to connect removable media, without prior approval from CWRPDA management.
- Confidential and internal CWRPDA information should not be stored on removable media without the use of encryption.
- The loss or theft of a removable media device that may have contained CWRPDA information must be reported to the CWRPDA management.

Security Training and Awareness

- All new personnel must complete an approved security awareness training class prior to, or at least within 10 days of, being granted access to any CWRPDA **Information Resources**.
- All personnel must be provided with and acknowledge they have received and agree to adhere to the CWRPDA Information Security Policies before they are granted access to CWRPDA **Information Resources**.
- All personnel must complete security awareness training no less than four times a year.

Social Media

- Communications using social media should be made in compliance with all applicable CWRPDA policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent CWRPDA, including accounts that could reasonably be assumed to be an official CWRPDA account, requires the permission of the CWRPDA Executive Director.
- When discussing CWRPDA or CWRPDA -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an CWRPDA representative, and
    - Make it clear that you are speaking for yourself and not on behalf of CWRPDA, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at CWRPDA.
- When publishing CWRPDA -relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer is: “The opinions and content are my own and do not necessarily represent CWRPDA’s position or opinion. The mere appearance or participation by CWRPDA personnel, in any capacity, does not constitute an endorsement of the opinions and content by the CWRPDA, and the CWRPDA cannot be held liable for the opinions and content contained herein.”
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).

BACK TO AGENDA

- The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with CWRPDA will not be tolerated and is prohibited.
- Confidential information, internal communications and non-public financial or operational information may not be published online in any form.

CWRPDA Voice Mail

- Personnel must use discretion in disclosing **confidential** or **internal information** in voice mail greetings, such as employment data or other sensitive data.
- Personnel must not access another user's voicemail account unless it has been explicitly authorized by CWRPDA Management or voicemails user.

Incidental Use

- As a convenience to CWRPDA personnel, incidental use of **Information Resources** is permitted. The following restrictions apply:
    - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to CWRPDA approved personnel; it does not extend to family members or other acquaintances unless approved by the Executive Director.
    - Incidental use should not result in direct costs to CWRPDA.
    - Incidental use must not interfere with the normal performance of an employee's work duties.
    - No files or documents may be sent or received that may cause legal action against, or embarrassment to, CWRPDA or its customers.
    - Incidental use must adhere to all policies/ directives contained herein.
- Storage of personal email messages, voice messages, files and documents within CWRPDA **Information Resources** must be nominal.
- All information located on CWRPDA **Information Resources** is owned by CWRPDA, may be subject to open records requests, and may be accessed in accordance with this policy.

Waivers

Waivers from certain policy provisions may be approved by the CWRPDA Executive Director. All waivers approved by the Executive Director must be documented and saved. The Executive Director must determine the appropriate place to save the waivers.

Enforcement

Personnel found to have violated this policy are subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy is subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Review

The Acceptable Use Policy shall be formally approved and adopted by the Authority's Board of Directors and reviewed annually. Any modifications to the Acceptable Use Policy shall be reflected in the **Version History** of said document.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	N/A	Jan. 30, 2019	BOD	Original adoption
1.1.0	N/A	January 29, 2020	BOD	Annual Review
1.2.0	January 29, 2021	January 29, 2021	BOD	Clean up items and Annual Review
1.3.0	January 26, 2022	January 26, 2022	BOD	Clean up items and Annual Review
2.0.0	March 3, 2023	March 3, 2023	BOD	Changes and Annual Review
3.0.0	March 8, 2024	March 8, 2024	BOD	Added two new sections
3.1~~4.0.0~~	April 25, 2025	April 25, 2025	BOD	Added additional language
3.2~~5.0.0~~	March 6, 2026			Modified language. Cleanup items.

BACK TO AGENDA

COLORADO WATER RESOURCES
POWER DEVELOPMENT AUTHORITY
The Amp - Suite 820, 1580 N Logan Street, Denver, Colorado 80203-1942
303/830-1550 · Fax 303/832-8205 · info@cwrpda.com

MEMORANDUM

March 6, 2026

TO: **Board of Directors and Karl Ohlsen**

FROM: **Jim Griffiths, Deputy Director**
Wesley Williams, Finance Director

RE: **2026 Interim Loan Program Annual Review***
Continuing the Pause on Interim Loan Applications and Approvals

---

Authority staff recommends a continued pause of interim loan applications.

Currently, there are no interim loans outstanding and no entities have requested an interim loan over the last year. The Authority Board asked staff to review the previous pause (in March 2025) in one-year.

The Interim Loan Program provided bridge financing and has been lightly used, historically. Examples of bridge financing provided by the Interim Loan Program include the following:

- To bridge the gap between an Authority leveraged loan approval and a leveraged loan bond issue (bond issues previously occurred annually and not twice a year as is generally the case now).
- For construction financing of a USDA loan. USDA requires interim loan financing for all of its loans.
- To fund the design and engineering costs for larger projects that do not have the fund balances to complete the design and engineering that enables them to apply for SRF financing.

Recently, staff executed two State Revolving Fund ("SRF") design and engineering loans instead of utilizing the interim loan program. The SRF design and engineering direct loans provided the necessary up-front funding, and with less risk. The risk was reduced because the entity approved and entered into a fully amortizing term loan that did not have to be paid off by another source immediately upon construction completion.

Several historical interim loans posed risks to the Authority including:

- Uncertain timing for payoff of the interim loan resulting in re-approvals (extensions) often with no specific resolution in sight.
- Payoff source (including one USDA loan) was not accessible, resulting in a long period of interim loan accrued interest.
- One recent interim loan approval was never executed, resulting in reserving limited funds that could have been deployed for other purposes.

Staff therefore recommends that the Board approve another one-year pause of the Interim Loan Program.

*General Notes: On April 22, 2021, Authority Staff presented a historic look at the Interim Loan Program and policy. Then, on June 4, 2021, Staff proposed changes to the interim loan program. The Board adopted changes to the interim loan program including a shorter term and the accrual of interest on both the drawn and undrawn portions of the loan at different rates. The Board approved pausing the interim loan program on February 1, 2024, subject to an annual review of the program.

BACK TO AGENDA