RESOLUTION NO. 2024-24

A RESOLUTION TO THE BOARD OF DIRECTORS OF MISSION SPRINGS WATER DISTRICT AMENDING CERTAIN PROVISIONS OF TITLES 1, 2 AND 3 OF THE ADMINISTRATIVE CODE

WHEREAS, pursuant to its authority granted by County Water District Law (California Water Code §§ 30000, et seq.), the Board of Directors adopted its Administrative Code on July 15, 2024; and

WHEREAS, the Board of Directors wishes to amend certain portions of that Code.

NOW THEREFORE, BE IT RESOLVED, DETERMINED AND ORDERED by the Board of Directors of Mission Springs Water District as follows:

SECTION 1. On July 15, 2024, the Board of Directors adopted Resolution No. 2024-20, rescinding Resolution 2022-19 and amending the Mission Springs Water District Conflict of Interest Code, Codified at Administrative Code Section 1.02. Pursuant thereto, Administrative Code section 1.02 is amended to read as follows:

Section 1.02.010 – Adoption of Code by Reference

The Political Reform Act ("Act") (Government Code Section 81000 et seq.) requires state and local government agencies to adopt and promulgate conflict of interest codes. The Fair Political Practices Commission ("Commission") has adopted a regulation (California Code of Regulations Section 18730 "Conflicts Code Regulation") which contains the terms of a standard conflict of interest code which can be incorporated by reference in an agency's code. After public notice and hearing, the standard code may be amended by the Commission to conform to amendments in the Act.

The terms of the Conflicts Code Regulation and any amendments to it duly adopted by the Commission are hereby incorporated by reference. This regulation and the attached Appendices "A" and "B" designating officials and employees and establishing disclosure categories, shall constitute the Conflict of Interest Code ("Code") for the Mission Springs Water District ("District")

Section 1.02.020 – Place of Filing

Designated employees shall file a statement of economic interests with the Secretary to the Board of Directors of the District ("Board"). Upon receipt of the statements of the Board, the Secretary to the Board shall make and retain a copy of the statements and forward the original statements to the County of Riverside. Statements for all other designated employees shall be delivered to the Secretary to the Board and retained by the District.

Section 1.02.030 – Violations

This Code has the force and effect of law. Designated employees violating any provision of this Code are subject to the administrative, criminal and civil sanctions provided in the Act, as it may be amended from time to time.

Section 1.02.040 – Designated Filers and Disclosure Categories

A. Director of Operations	All (1-3)
B. Assistant General Manager	All (1-3)
C. Engineering Manager	All (1-3)
D. Human Resources Manager	All (1-3)
E. Legal Counsel	All (1-3)
F. Consultants	See below

Section 1.02.050 – Officials Who Manage Public Investments

A. It has been determined that the positions listed below manage public investments and shall file a Statement of Economic Interests pursuant to Government Code Section 87200:
   1. Board of Directors
   2. General Manager
   3. Director of Finance

B. Consultants shall be included in the list of designated employees and shall disclose pursuant to the broadest disclosure category in this Code subject to the following limitations:
   1. The General Manager may determine in writing that a particular consultant, although a “designated position”, is hired to perform a range of duties that are limited in scope and thus is not required to fully comply with the disclosure requirements described in this section. Such written determinations shall include a description of the consultant’s duties and, based upon that description, a statement of the extent of disclosure requirements. The General Manager’s determination is a public record and shall be retained for public inspection in the same manner and location as this Conflict of Interest Code.
   2. The designated position of Consultants includes special legal counsel retained by the District as a position subject to the foregoing specialized disclosure category.

Section 1.02.060 – Disclosure Categories

A. This Code does not establish any disclosure obligation for those designated employees who are also specified in Government Code Section 87200. Such persons are covered by this Code for disqualification purposes only. With respect to all other designated employees, the disclosure categories set forth in Sections 1.02.040 and 1.02.050 specify which kinds of financial interests he or she has which are of the kind described in the disclosure categories to which he or she is assigned in Sections 1.02.040 and 1.02.050. It has been determined that the

financial interests set forth in a designated employee's disclosure categories are the kinds of financial interests which he or she foreseeably can affect materially through the conduct of his or her office.

B. The disclosure categories listed below identify the types of investments, business entities, sources of income, or real property, which the designated employee must disclose for each disclosure category to which he or she is assigned.
   1. Category 1: Interest in real property.
   2. Category 2: All investments and business positions in any business entity and income from any sources which are (1) a private water company; or (2) an entity or person engaged in farming or real estate development or an owner of real property.
   3. Category 3: Investment and business positions in business entities, and sources of income, which provide services, supplies, materials, machinery, or equipment of the type utilized by the District.

SECTION 2. Resolution No. 86-3, codified at Administrative Code section 2.01.030 is hereby amended to read as follows:

Section 2.01.030 – Smoking/Vaping Prohibited

Smoking or vaping of any kind (including but not limited to tobacco and/or cannabis products) on District property, and within twenty (20) feet of any District building/structure is prohibited, including within the Boardroom or in any District building.

SECTION 3. Resolution No. 88-20, codified at Administrative Code § 2.01.040 is hereby amended to read as follows:

Section 2.01.040 – Appeal of Certain Administrative Decisions

It is hereby found and determined that the application of Section 1094.6 of the Code of Civil Procedure to administrative decisions of this District will provide an orderly and reasonable procedure for the review of certain decisions of the District.

The provisions of Section 1094.6 of the Code of Civil Procedure shall apply to decisions of the District which are subject to review pursuant to Section 1094.5, and the provisions of Section 1094.6 of the Code of Civil Procedure shall prevail over any conflicting provision in any other applicable law relating to the subject matter, unless the conflicting provision is a state or federal law which provides a shorter statute of limitations, in which case the shorter statute of limitations shall apply.

SECTION 4. Resolution No. 37-1971, codified at Administrative Code section 2.03.020, is hereby amended to read as follows:

Section 2.03.020 – Manner of Calling Special Meetings

A special meeting may be called at any time by the presiding officer of the Board of Directors, or by a majority of the members of the Board of Directors, by providing notice in accordance with the provisions of the Ralph M. Brown Act (the "Brown Act") for such special meetings, as may be amended from time to time. Such notice must be delivered at least twenty-four (24) hours before the time of such meeting as specified in the notice. The call and notice shall specify the time and place of the special meeting and the

business to be transacted. No other business shall be considered at such meeting by the Board of Directors.

Written notice may be dispensed with as to any director who at or prior to the time the meeting convenes, files with the Secretary of the Board of Directors a written Waiver of Notice in accordance with the Brown Act. Such written notice may also be dispensed with as to any director who is actually present at the meeting at the time it convenes.

SECTION 5. Resolution No. 2024-09, the Board of Directors Handbook "Executive Summary," codified at Administrative Code section 2.04.020 is hereby amended to read as follows:

Section 2.04.020 – Executive Summary

The District's core values of Accountability, Leadership, Professionalism and Service are the foundation for this Handbook. These core values, along with specific criteria related to the performance of public officials, were used in identifying the appropriate Best Practices for members of the Board and the General Manager. An annual review of the approved and adopted best practices outlined in the Board Handbook would serve as a continual reminder of the Board's role in policy governance and principles of behavior as a "Best of Class" water agency. The document will also serve as a valuable tool in the orientation and education of new Board members and staff in the future.

A. Board Best Practices
    1. Ethical standards and accountable leadership
    2. Public confidence and integrity
    3. Compliance with the letter and spirit of existing laws and policies
    4. Dedication to superior service
    5. Personalized standards of conduct

SECTION 6. The Mission Springs Personnel Rules and Regulations, Rule 8 "No Smoking Policy," codified as Administrative Code section 3.01.080 is hereby amended to read as follows:

Section 3.01.050 – Use of Electronic Media: District Right of Access and No Expectation of Privacy (Rule 5)

The District provides various Technology Resources to authorized employees to assist them in performing their job duties for the District. Each employee has a responsibility to use the District's Technology Resources in a manner that increases productivity, enhances the District's public image, and is respectful of other employees. Failure to follow the District's policies regarding Technology Resources may lead to disciplinary measures, up to and including termination of employment. Moreover, the District reserves the right to advise appropriate legal authorities of any violation of the law by an employee.

A. Technology Resources Definition – Technology Resources consist of all electronic media and storage devices, software, and means of electronic communication

including any of the following: personal computers and workstations; laptop computers; mini and mainframe computers; tablets; computer hardware such as disk drives, tape drives, external hard drives and flash/thumb drives; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet or cloud storage accounts; electronic mail; telephones; mobile phones; personal organizers and other handheld devices; pagers; voicemail systems; and instant messaging systems.

B. Authorization – Access to the District's Technology Resources is within the sole discretion of the District. Generally, employees are given access to the District's various technologies based on their job functions. Only employees whose job performance will benefit from the use of the District's Technology Resources are authorized to access and use the necessary technology. Additionally, employees must successfully complete District-approved training before they are authorized to access and use the District's Technology Resources.

   The District's Technology Resources are to be used by employees during working time only for the purpose of conducting District business. Employees may, however, use the District's Technology Resources for the following incidental non-work-related uses during nonworking time as long as such use does not interfere with the employee's duties, is not done for pecuniary gain, and does not violate any District policy:

   1. To use the telephone system for brief and necessary calls;
   2. To send and receive necessary and occasional communications;
   3. To prepare and store incidental data (such as personal calendars, personal address lists, and similar incidental data) in a reasonable manner; and
   4. To access the Internet and personal social media sites for brief personal searches and inquiries during meals, breaks, or other nonworking time, provided that employees adhere to all other usage policies.

   The District assumes no liability for loss, damage, destruction, alteration, receipt, transmission, disclosure, or misuse of any personal data or communications transmitted over or stored on the District's Technology Resources. The District accepts no responsibility or liability for the loss or non-delivery of any personal electronic mail or voicemail communications or any personal data stored on any District property. The District strongly discourages employees from storing any personal data on any of the District's Technology Resources.

C. District Access to Technology Resources – All messages sent and received, including personal messages, and all data and information stored on the District's Technology Resources (including on its electronic mail system, voicemail system, or computer systems) are District property regardless of the content. As such, the District reserves the right to access all of its Technology Resources including its

computers, voicemail, and electronic mail systems, at any time, in its sole discretion. No employee, other than the General Manager, has authority to waive, vary or amend the District's right to access its Technology Resources.

D. No Reasonable Expectation of Privacy – Although the District does not wish to examine personal information of its employees, on occasion, the District may need to access its Technology Resources including computer files, electronic mail messages, and voicemail messages. Employees should understand, therefore, that they have no right of privacy with respect to any messages or information created, collected, or maintained on the District's Technology Resources, including personal information or messages. The District may, at its discretion, inspect all files or messages on its Technology Resources at any time for any reason. The District may also monitor its Technology Resources at any time in order to confirm compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

E. Passwords – Certain of the District's Technology Resources can be accessed only by entering a password or using login credentials. Passwords and login credentials are intended to prevent unauthorized access to information. Passwords and login credentials do not confer any right of privacy upon any employee of the District. Thus, even though employees may maintain passwords or be provided with login credentials for accessing Technology Resources, employees must not expect that any information maintained on Technology Resources, including electronic mail and voicemail messages, are private. Employees are expected to maintain their passwords and login credentials as confidential. Employees must not share passwords, or forward login credentials unless authorized by the Innovation and Technology Manager and must not access coworkers' systems without express authorization.

F. Data Collection – The best way for employees to ensure the privacy of personal information is not to store or transmit it on the District's Technology Resources. So that employees understand the extent to which information is collected and stored, examples of information currently maintained by the District are provided below. The District may, however, in its sole discretion, and at any time, alter the amount and type of information that it retains.
    1. Telephone Use and Voicemail: Records are kept of all calls made to and from a given telephone extension. Although voicemail is password-protected, an authorized administrator can listen to voicemail messages and also reset the password.
    2. Electronic Mail: Electronic mail is backed up and archived. Although electronic mail is password-protected, an authorized administrator can read electronic mail and also reset the password.

3. Desktop Facsimile Use: Copies of all facsimile transmissions are maintained in the facsimile server.
4. Document Use: Each document stored on District computers has a history that shows which users have accessed the document for any purpose.
5. Internet Use: Internet sites visited, the number of times visited, and the total time connected to each site are recorded and periodically monitored.

G. Deleted Information – Deleting or erasing information, documents, or messages maintained on the District's Technology Resources is, in most cases, ineffective. All employees should understand that any information kept on the District's Technology Resources may be electronically recalled or recreated regardless of whether it may have been "deleted" or "erased" by an employee. Because the District periodically backs up all files and messages, and because of the way in which computers reuse file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information or messages are confidential or ever were confidential. If a legal dispute arises, or may arise in the future, it may be unlawful to attempt to delete or erase certain information. Employees shall fully comply with District policy regarding retention or destruction of information.

H. The Internet and On-Line Services – The District provides authorized employees access to online services such as the Internet. The District expects that employees will use these services in a responsible way and for business-related purposes only. Under no circumstances are employees permitted to use the District's Technology Resources to access, download, or contribute to Internet sites that contain inappropriate content such as that which is discriminatory, harassing, defamatory, obscene, indecent, threatening, or that otherwise could reasonably adversely affect any individual, group, or entity.

   Additionally, employees may not use the District's Technology Resources to post, comment, send, or otherwise upload any information to any Web sites or other online groups, including web logs (i.e., "blogs"), social networking Web sites, newsgroups, discussion groups, or non-District email groups, except in accordance with the District's Blogging Policy. These actions will likely generate junk electronic mail and may expose the District to liability or unwanted attention because of comments or other contributions that employees may make. The District strongly encourages employees who wish to access the Internet for non-work-related activities to obtain their own personal Internet access accounts that are unaffiliated with the District, and to use such accounts at home on their own personal computer, except as allowed by law.

I. Online Monitoring – The District monitors both the amount of time spent using online services and the sites visited by individual employees. The District reserves

the right to limit such access by any means available to it, including revoking access altogether. The District, through technological tools, may also prohibit or limit access to certain Web sites considered inappropriate by the District or its technology provider.

J. Confidential Information – The District is very sensitive to the issue of protecting confidential information of both the District, business partners, vendors, or customers (''Confidential Information''). Confidential Information includes all confidential and personal information covered by the District's guideline in Rule 3, Section B above regarding “Confidential Information.” Therefore, employees are expected to use good judgment and to adhere to the highest ethical standards when using or transmitting Confidential Information on the District's Technology Resources.

   Confidential Information should not be accessed through the District's Technology Resources in the presence of unauthorized individuals. Similarly, Confidential Information should not be left visible or unattended. Moreover, any Confidential Information transmitted via Technology Resources should be marked with the following confidentiality legend: ''This message contains confidential information. Unless you are the addressee (or authorized to receive for the addressee), you may not copy, use, or distribute this information. If you have received this message in error, please advise [employee's name] immediately at [employee's telephone number] or return it promptly by mail.''

   Employees should adhere to District's security policy with regard to Confidential Information and take all appropriate measures to safeguard the confidentiality and security of such information. Employees should avoid sending Confidential Information via the Internet, except when absolutely necessary. Employees should also verify electronic mail addresses before transmitting any messages containing Confidential Information.

K. Software Use
   1. License Restrictions – All software in use on the District's Technology Resources is officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No employee may load any software on the District's computers, by any means of transmission, unless authorized in writing in advance by the General Manager or designee (e.g., the Innovation and Technology Manager) and thoroughly scanned for viruses or other malware prior to installation.
   2. Software for Home Use – Before transferring or copying any software from a District Technology Resource to another computer or other device, employees must obtain written authorization from the General Manager or

designee. It is the employee's responsibility to adhere to applicable licensing requirements, including not making or distributing unauthorized copies of software to others. Upon departure from the District, it is the employee's responsibility to remove all District software from non-District computers and other devices on which District software has been installed. If an employee sells or otherwise transfers out of his or her own possession or controls his or her own personally owned computer, he or she must delete all District software prior to such sale or other transfer. Please ask the General Manager or designee (e.g., the Innovation and Technology Manager) for assistance if needed.

3. Security – The District has installed a variety of programs and devices to ensure the safety and security of the District's Technology Resources. Any employee found tampering with or disabling any of the District's security devices will be subject to discipline up to and including termination.

   Moreover, the District reserves the right to advise appropriate legal authorities of any violation of law by an employee that results in the misappropriation, theft, or unlawful use of District's property or proprietary information.

   To maintain the effectiveness of the District's security measures, employees should use only secure networks established by the District to access or use Confidential Information. Such information may not be downloaded, stored, or copied onto any non-District equipment or media (including personally owned computer, handheld devices, external memory devices, or disks) without prior written approval from the General Manager or designee (e.g., the innovation and Technology Manager). If Confidential Information is downloaded, stored, or copied onto non-District equipment or media, employees must take all appropriate measures to safeguard against loss, theft, damage, or breach of such equipment or media. If Confidential Information is downloaded, stored, or copied onto non-District equipment or media, employees must permanently delete such information prior to selling or otherwise transferring out of their own possession or control such equipment or media. If Confidential Information is downloaded, stored, or copied onto non-District equipment or media and employee resigns, is terminated, or is requested to do so by management, employees must delete all Confidential Information they received, including any and all copies thereof. Similarly, employees may not send Confidential Information to their personal e-mail accounts, even for work-related purposes, without prior written approval of the General Manager or designee (e.g., the Innovation and Technology Manager).

Any loss or suspected loss of Confidential Information, or any suspicious activity such as external hacking attempts or unusual internal activity, should be reported immediately to District management.

4. Remote Access to Technology Resources – The District may, at its sole discretion, provide certain employees with remote access systems such as a laptop, smartphone, tablet, or other personal organizer to allow such employees to handle the tasks associated with their jobs while working away from the office. Employees must take care to ensure the security of all District-provided equipment. Employees must not share network passwords or other PINs with anyone. As soon as an employee believes District-provided equipment is lost or that the security and confidentiality of the data on that equipment has been compromised, he or she must notify the General Manager or designee (e.g., the Innovation and Technology Manager). If District-provided equipment is lost, or if it is damaged as a result of carelessness, employees may be responsible for replacement fees. The District-provided remote access system should only be used for District-related business. The District may decide that it is no longer necessary for certain employees to possess a remote access system and their ability to use such systems may be discontinued, in which case such employees are expected to return any District-issued remote access systems in accordance with District's "District Property" policy.

   The District does not expect or require employees to work on tasks (including e-mail, work product, etc.) during meal periods or after scheduled working times. Any and all use of remote access systems shall be made in compliance with District's "Hours of Work, Overtime, And Pay Day policy."

   Use of public or home networks, such as unencrypted Wi-Fi networks, can be a threat to the security and reliability of the District's Technology Resources. Accordingly, employees must only access District Technology Resources via means that are specifically approved by the General Manager or designee (IT Manager).

5. Use of AI – The General Manager or his designee may establish and implement staff guidance related to the use of Artificial Intelligence (AI), including but not limited to ChatGPT, to ensure the responsible use of AI technologies within the District. Employees are expected to understand and adhere to any such policies. Any staff actions or behaviors that may compromise the integrity, security, or reputation of the District or its assets are strictly prohibited. This includes but is not limited to, the misuse of AI technologies, unauthorized access to AI systems, and any activities that could potentially harm District operations or stakeholders. Employees are

expressly prohibited from inputting confidential or sensitive information into an AI platform, or from utilizing AI in any way that might compromise District information, property, and/or reputation.

L. Electronic Mail Guidelines – Employees are expected to use sound judgment with respect to the use of the District's electronic mail ("e-mail"). All employees should adhere to the following with respect to use of e-mail:
    1. Always ask before sending an e-mail if it is the appropriate medium of communication. When communicating about a sensitive subject, consider whether e-mail is the appropriate medium or whether using the phone rather than e-mail might be more appropriate (but keep in mind that voicemail is similar to e-mail; voicemail may be stored on a computer server and may be forwarded to third parties).
    2. Use the "front page" test. Assuming that e-mail is the appropriate medium of communication, each e-mail should be treated as a formal written document. Do not write anything in an e-mail that could not be printed on the front page of the newspaper. Off-the-cuff, sarcastic, or angry comments can come back to haunt the author.
    3. E-mail is part of the workplace environment. E-mail containing rude and insensitive comments is not only personally embarrassing, but also may serve as the basis for legal liability. Employees and managers should exercise the same care and sensitivity in communicating via e-mail as they would when communicating in person or in letters. Offensive e-mail received from others should not be forwarded, and the recipient should ask the sender to refrain from sending inappropriate e-mail.
    4. Provide context. As with other forms of communication, there is a risk that an e-mail message may be taken out of context. To reduce the risk that the message will be taken out of context, consider including the original message to which the reply e-mail relates.
    5. Know your audience. When sending an e-mail, always double-check to whom the e-mail is addressed, especially when using the "reply to all" button. Ask whether it is appropriate for each addressee to receive the e-mail and whether sending the e-mail to a particular addressee will result in the unauthorized disclosure of Confidential Information. If in doubt, remove the doubted addressee.
    6. Avoid using a home or personal computer for business purposes. If there is any concern that a legal dispute or litigation involving the District and a third party may require producing one's hard drive from a home or personal computer, the employee should not use the device for business-related purposes. E-mail relating to District business, even though stored on a home or personal computer, is recoverable and discoverable in litigation.

M. Audits – The District may perform auditing activity or monitoring to determine compliance with these policies. Audits of software and data stored on the District's Technology Resources may be conducted without warning at any time.

N. Improper Use

1. Prohibition Against Harassing, Discriminatory and Defamatory Use – The District is aware that employees use electronic mail for correspondence that is less formal than written memoranda. Employees must take care, however, not to let informality degenerate into improper use. As set forth more fully in the District's "Policy Against Harassment," the District does not tolerate discrimination or harassment based on gender, pregnancy, childbirth (or related medical conditions), race, color, religion, national origin, ancestry, age, physical disability, mental disability, medical condition, marital status, sexual orientation, family care or medical leave status, military status, veteran status, or any other status protected by state and federal laws. Under no circumstances shall employees use the District's Technology Resources to transmit, receive, or store any information that is discriminatory, harassing, defamatory, obscene, indecent, threatening, or that otherwise could adversely affect any individual, group, or entity (e.g., sexually explicit or racial messages, slurs, jokes, or cartoons).
2. Prohibition Against Violating Copyright Laws – Employees shall not use the District's Technology Resources to copy, retrieve, forward, or send copyrighted materials unless the employee has the author's permission or is accessing a single copy only for the employee's reference.
3. Other Prohibited Uses – Employees shall not use the District's Technology Resources for any illegal purpose, violation of any District policy, for pecuniary gain, or in any way that discloses trade secrets or other confidential or proprietary information of the District, business partners, vendors, or customers.

Section 3.01.080 – No Smoking Policy (Rule 8)

Smoking or vaping of any kind (including but not limited to tobacco and/or cannabis products) is prohibited in District vehicles, and within twenty (20) feet of any District building/structure. Employees shall be especially attentive to the sensitivities of the public and fellow employees who may object to smoking/vaping. Management reserves the right to limit employees from leaving their work area to smoke/vaping except at break and lunch time. However, employees should use reason and discretion in the frequency of leaving the work area to smoke/vape.

It is also a violation of California law for any person to smoke in a vehicle where minors are present. As such, any employee who smokes in a District vehicle while a minor is present may also be subject to criminal liability.

ADOPTED this _____ day of September 2024, by the following vote:

Ayes:
Noes:
Abstain:

_____

Ivan Sewell
President of Mission Springs Water District
and its Board of Directors

ATTEST:

_____

Brian Macy
Secretary of Mission Springs Water District
and its Board of Directors