



**Special Meeting
Of the Board of Directors of
YUIMA MUNICIPAL WATER DISTRICT
Monday, June 3, 2024 at 2:00 p.m.
34928 Valley Center Road, Pauma Valley, California**

Roland Simpson, President
Don Broomell, Secretary / Treasurer
Bruce Knox, Director

Steve Wehr, Vice-President
Laurie Kariya, Director

I. CALL TO ORDER

II. ROLL CALL – DETERMINATION OF QUORUM

III. APPROVAL OF AGENDA

At its option, the Board may approve the agenda, delete an item, reorder items, and add an item to the agenda per the provisions of Government Code §54954.2.

IV. PUBLIC COMMENT

This is an opportunity for members of the public to address the Board on matters of interest within the Board's jurisdiction that are not listed on the agenda. The Brown Act does not allow any discussions by the Board or staff on matters raised during public comment except; 1) to briefly respond to statements made or questions posed; 2) ask questions for clarification; 3) receive and file the matter; 4) if it is within staff's authority, refer it to them for a reply; or 5) direct that it be placed on a future Board agenda for a report or action. Inquiries pertaining to an item on the agenda will be received during deliberation on that agenda item. No action can be taken unless specifically listed on the agenda. (Government Code §54954.3).

V. CONSENT CALENDAR

- a) Approve minutes of the Regular Meeting of April 22, 2024
- b) Approve Accounts Paid and Payables & Reporting under Government Code §53065.5 for April 2024
- c) Acceptance of Monthly Financial Reports, Treasurer's Report and Cash Statements – April 2024

VI. ACTION DISCUSSION

a) Budget Workshop: First Review of the 2024/25 Preliminary Budget

Background: The preliminary 2024-2025 Operating Budget will be presented.

Recommendation: That the Board review and direct staff to modify as necessary for final adoption at the Regular Board meeting on June 24, 2024.

b) Proposed Resolution Awarding Audit Services for Fiscal Years 2023/24, 2024/25, and 2025/26 to Nigro & Nigro, PC.

Background: On April 10, 2024 the District released a Request for Proposal (RFP) for Audit Services for Fiscal Years 2023/24 through 2025/26 with a two-year extension option. The RFP's were due to the District by May 15, 2024. The District received one RFP for consideration. Nigro & Nigro, PC has submitted a RFP that meets the necessary

requirements of the District at a cost of \$18,500 per year for a total of \$55,500 over the three-year period. For budgeting purposes, each year will be budgeted separately and issued a separate purchase order, but Staff is requesting the Board to award the full 3-year contract for audit services to Nigro and Nigro.

Recommendation: That the Board accept the Staff recommendation and award the audit services preparation to Nigro & Nigro.

c) Proposed Resolution Adopting a Cybersecurity Policy

Background: As a condition of the insurance policy covering cyber attacks JPIA has required that the District adopt a Cyber Security Policy. The District's IT consultant developed the included policy taking into consideration the Cyber security protocols already in place and the logical response needed in the event of a cyber security breach.

Recommendation: That should the Board agree, the Board approve the Resolution as presented and direct the General Manager to in-service staff on the policy.

d) Proposed Resolution adopting a Workplace Violence Prevention Plan

Background: Senate Bill 553, requiring the District to create and adopt a Workplace Violence Prevention Plan, was signed into law on September 20, 2023 and becomes effective July 1, 2024.

Recommendation: That should the Board agree, the Board approve the Resolution as presented.

VII. INFORMATION /REPORTS

a) Board Reports / Meetings

- i) JPIA
- ii) San Diego County Water Authority / Metropolitan Water District
- iii) Other Meetings (USLRGMA)

b) Administrative

- i) General Information

c) Capital Improvements

d) Operations

- i) General Information
- ii) Rainfall
- iii) Production / Consumption Report
- iv) Well Levels
- v) District Water Purchased

e) **Counsel**

f) **Finance**

i) General Information

ii) Delinquent Accounts

VIII. OTHER BUSINESS

a) June 24, 2024 at 2:00 p.m. Regular Meeting 2nd Budget Review

IX. ADJOURNMENT

NOTE: In compliance with the Americans with Disabilities Act, if special assistance is needed to participate in the Board meeting, please contact the General Manager at (760) 742-3704 at least 48 hours before the meeting to enable the District to make reasonable accommodations. Any writings or documents provided to a majority of the members of the Yuima Municipal Water District Board of Directors regarding any item on this agenda will be made available for public inspection during normal business hours in the office of the General Manager located at 34928 Valley Center Rd., Pauma Valley.

CONSENT CALENDAR

MINUTES OF THE REGULAR MEETING OF THE BOARD OF DIRECTORS OF YUIMA MUNICIPAL WATER DISTRICT

Date: April 22, 2024

Time: 2:03 p.m.

I. CALL TO ORDER

The Regular Meeting of the Board of Directors of the Yuima Municipal Water District was held at the office of the district located at 34928 Valley Center Rd., Pauma Valley, California on Monday, the 22nd day of April 2024. The meeting was called to order at 2:03 p.m. and the Pledge of Allegiance was performed.

II. ROLL CALL – DETERMINATION OF QUORUM

General Manager Reeh conducted role call and declared that a quorum of the Board was present.

Directors In Attendance

Roland Simpson
Steve Wehr
Laurie Kariya
Bruce Knox
Don Broomell

Directors Absent

Others In Attendance

Amy Reeh, General Manager, YMWD
Jeremy Jungreis, District Counsel
Lynette Brewer, Finance and Admin Manager, YMWD
Mark Quinn, Operations Manager, YMWD
Breona Easley, Accounting Technician, YMWD
Allen Simon, Lead Systems Technician, YMWD
Matt Munaco, Water Systems Tech. II, YMWD
Noel Ruiz, Distribution Water Quality Tech, YMWD
Rosbelth Valenzuela, Utility Worker I, YMWD

Carson Drown, Water Systems Tech I, YMWD
Kristina Daily, Administrative Clerk, YMWD
La Vonne Peck, member of the public

III. APPROVAL OF THE AGENDA

Staff requested to add item **VI. f)** to the agenda, as well as move item **VI. e)** to the beginning of the Action Items. Upon motion by Director Kariya and seconded by Director Wehr, the revised agenda was approved by the following roll-call vote, to wit:

AYES: Simpson, Wehr, Broomell, Kariya, Knox
NOES: None
ABSTAIN: None
ABSENT: None

IV. PUBLIC COMMENT

There were no public comments.

V. CONSENT CALENDAR

- a) Approve Minutes of the Regular Meeting of March 25, 2024**
- b) Approve of Accounts Paid and Payables & Reporting under Government Code §53065.5 for March 2024**
- c) Acceptance of Monthly Financial Reports – March 2024, Treasurer’s Report and Cash Statements**

Upon motion by Director Knox and seconded by Director Kariya, the ***Approval of Minutes of the Regular Meeting of March 25, 2024, Approval of Accounts Paid and Payables & Reporting under Government Code §53065.5 for March 2024, Acceptance of Monthly Financial Reports – March 2024, Treasurer’s Report and Cash Statements***, was approved and carried unanimously by the following roll-call vote, to wit:

AYES: Simpson, Wehr, Broomell, Kariya, Knox
NOES: None
ABSTAIN: None
ABSENT: None

VI. ACTION / DISCUSSION

a) Proposed Resolution Showing Appreciation to Mark Quinn for 34 Years for Outstanding Public Service to the People of Yuima Municipal Water District

Operations Manager Quinn was presented with a Resolution of appreciation and gift from the Board for his dedicated service to Yuima Municipal Water District. Upon motion by Director Kariya and seconded by Director Broomell, **Resolution No. 1958-24 Showing Appreciation to Mark Quinn for 34 Years for Outstanding Public Service to the People of Yuima Municipal Water District** was approved and carried unanimously by the following roll-call vote, to wit:

AYES: Simpson, Wehr, Broomell, Kariya, Knox
NOES: None
ABSTAIN: None
ABSENT: None

b) Public Hearing to Receive Comments and Consider Adoption of the Proposed Ordinance Fixing a Water Availability Charge for the District (2024/2025)

President Simpson called the public hearing to order. General Manager Reeh reported the Notice of Public Hearing was given no less than fifteen (15) days prior to the hearing via the local paper and a copy is on file with the District. Secretary Broomell reported that there were zero (0) written letters of protest received. There being no members of the public wishing to speak, President Simpson declared the hearing closed.

1-A. Ordinance 143-24 Fixing a Water Availability Charge for the District (2024/2025)

Upon motion offered by Director Kariya, seconded by Director Broomell, **Ordinance 143-24 Fixing a Water Availability Charge for the District (2024/2025)** was approved and carried unanimously by the following roll-call vote, to wit:

AYES: Simpson, Wehr, Broomell, Kariya, Knox
NOES: None
ABSTAIN: None
ABSENT: None

c) [Resolution 1956-24 Setting Forth the Time and Place of Hearing and Giving Notice of Hearing for a Water Rate Increase](#)

Following discussion and upon motion offered by Director Knox, seconded by Director Wehr, ***Resolution 1956-24 Setting Forth the Time and Place of Hearing and Giving Notice of Hearing for a Water Rate Increase*** was approved and carried unanimously by the following roll-call vote, to wit:

AYES: Simpson, Wehr, Broomell, Kariya, Knox
NOES: None
ABSTAIN: None
ABSENT: None

d) [Resolution 1957-24 Adopting an Annual Statement of Investment Policy and Rescinding Resolution 1951-23](#)

Upon motion offered by Director Broomell, seconded by Director Knox, ***Resolution 1957-24 Adopting an Annual Statement of Investment Policy and Rescinding Resolution 1951-23*** was approved and carried unanimously by the following roll-call vote, to wit:

AYES: Simpson, Wehr, Broomell, Kariya, Knox
NOES: None
ABSTAIN: None
ABSENT: None

e) [Discussion: Forthcoming Groundwater Management Authority Pumping Fees and Additional Budget Rate Drivers](#)

General Manager Reeh discussed additional rate drivers for the 2024/2025 fiscal year including new pumping fees expected to be assessed by the Upper San Luis Rey Groundwater Management Authority. No fees have been adopted to date but are expected to be adopted and assessed on July 1st, 2024. General Manager Reeh also discussed the expected rate increase from the San Diego County Water Authority, which could be as high as 22%. Jeremy Jungreis gave further explanation of fees in comparison to other Groundwater Sustainability Agencies.

f) [Discussion and Possible Approval of Addendum No. 1 to the Memorandum of Understanding for the Regional Crop SWAP Program](#)

General Manager Reeh discussed the opportunity to participate in the newly expanded Rancho California Crop SWAP Program. An MOU was developed between Rancho, Valley Center, Rainbow, Fallbrook, and City of Oceanside. Further discussions between Rancho, the City of Escondido, and Yuima has resulted in an Amendment to the MOU to include Yuima and the City of Escondido.

Following discussion, the Board decided not to bring the item to a vote.

VII. INFORMATION / REPORTS

a) Board Reports / Meetings

Administrator Reeh updated the Board on the SDCWA's rate structure change.

b) Administrative

The General Manager's Report was available in the Board Packet.

c) Capital Improvements

The Capital Improvements Report was available in the Board Packet.

d) Operations

The Operations Report was available in the Board Packet.

e) Counsel

Counsel was in attendance and had nothing to report.

f) Finance & Administrative Services

General Manager Reeh briefly discussed the lack of water sales for the current year causing a revenue shortfall. The District is entering warmer months and water sales are expected to increase, however staff cannot predict if the District will meet its budgeted sales estimates for the fiscal year.

VII. CLOSED SESSION

Conference with Legal Counsel – Potential Litigation – 1 Case – Pursuant to Government Code Section 54956.9.

The Board entered closed session at 3:50 p.m. and returned to open session at 4:09 p.m. with nothing to report.

VIII. OTHER BUSINESS

- a) June 3, 2024 at 2:00 p.m. Special Meeting 1st Budget Review (this meeting is in lieu of the Regular Meeting originally scheduled for May 20, 2024).
- b) June 24, 2024 at 2:00 p.m. Regular Meeting 2nd Budget Review and possible adoption.

IX. ADJOURNMENT

The meeting of the Board of Directors of the Yuima Municipal Water District was adjourned at 4:09 p.m. until the next special meeting on June 3rd, 2024 at 2:00 p.m.

Roland Simpson, President

Don Broomell, Secretary/Treasurer



Yuima Municipal Water District

Bank Transaction Report

Transaction Detail

Issued Date Range: 04/01/2024 - 04/30/2024

Cleared Date Range: -

Issued Date	Cleared Date	Number	Description	Module	Status	Type	Amount
Bank Account: 57-955468-36 - *General Checking							
04/01/2024		DFT0001806	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-308.03
04/01/2024		DFT0001807	EFTPS - Federal Payroll Tax	Accounts Payable	Outstanding	Bank Draft	-812.08
04/01/2024		EFT0000097	Payroll EFT	Payroll	Outstanding	EFT	-27,288.80
04/02/2024		72158	VALIC GA#24515	Accounts Payable	Outstanding	Check	-800.00
04/02/2024		72159	A-1 IRRIGATION, INC.	Accounts Payable	Outstanding	Check	-68.44
04/02/2024		72160	CONTROLLED ENTRANCES INC	Accounts Payable	Outstanding	Check	-260.00
04/02/2024		72161	Copeland Transmission and Automotive Repair	Accounts Payable	Outstanding	Check	-4,866.74
04/02/2024		72162	EDCO Waste and Recycling Services, Inc.	Accounts Payable	Outstanding	Check	-306.07
04/02/2024		72163	FALLBROOK OIL COMPANY	Accounts Payable	Outstanding	Check	-1,123.93
04/02/2024		72164	HACH COMPANY	Accounts Payable	Outstanding	Check	-2,010.00
04/02/2024		72165	OFFICE DEPOT	Accounts Payable	Outstanding	Check	-101.24
04/02/2024		72166	OPTIMIZED INVESTMENT PARTNERS	Accounts Payable	Outstanding	Check	-693.41
04/02/2024		72167	Protelesis	Accounts Payable	Outstanding	Check	-1,810.27
04/02/2024		72168	PRUDENTIAL OVERALL SUPPLY	Accounts Payable	Outstanding	Check	-33.33
04/02/2024		72169	TRAVIS W. PARKER	Accounts Payable	Outstanding	Check	-367.11
04/02/2024		72170	T-Y Nursery	Accounts Payable	Outstanding	Check	-10,791.08
04/02/2024		72171	Upper San Luis Rey Groundwater Management Authority	Accounts Payable	Outstanding	Check	-11,694.12
04/02/2024		72172	WATERLINE TECHNOLOGIES	Accounts Payable	Outstanding	Check	-1,103.13
04/02/2024		72173	XEROX FINANCIAL SERVICES LLC	Accounts Payable	Outstanding	Check	-459.18
04/02/2024		DFT0001808	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-691.61
04/02/2024		DFT0001809	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-685.37
04/02/2024		DFT0001810	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-1,720.74
04/02/2024		DFT0001811	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-3,712.51
04/02/2024		DFT0001812	CALPERS 457 PLAN	Accounts Payable	Outstanding	Bank Draft	-37.50
04/02/2024		DFT0001813	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-8.37
04/02/2024		DFT0001814	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-1,291.78
04/02/2024		DFT0001815	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-359.41
04/02/2024		DFT0001816	EFTPS - Federal Payroll Tax	Accounts Payable	Outstanding	Bank Draft	-4,410.06
04/02/2024		DFT0001817	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-88.83
04/02/2024		DFT0001818	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-79.38
04/02/2024		DFT0001819	EFTPS - Federal Payroll Tax	Accounts Payable	Outstanding	Bank Draft	-552.37
04/02/2024		EFT0000098	Payroll EFT	Payroll	Outstanding	EFT	-24,152.78
04/02/2024		EFT0000099	Payroll EFT	Payroll	Outstanding	EFT	-6,599.04
04/10/2024		72174	A-1 IRRIGATION, INC.	Accounts Payable	Outstanding	Check	-50.09
04/10/2024		72175	ALPHA ANALYTICAL LABORATORIES, INC.	Accounts Payable	Outstanding	Check	-100.00
04/10/2024		72176	AMERICA'S JANITORIAL SERVICE	Accounts Payable	Outstanding	Check	-215.00

Bank Transaction Report

Issued Date Range: -

Issued Date	Cleared Date	Number	Description	Module	Status	Type	Amount
04/10/2024		72177	BABCOCK LABORATORIES, INC	Accounts Payable	Outstanding	Check	-1,482.26
04/10/2024		72178	POWERS ELECTRIC PRODUCTS	Accounts Payable	Outstanding	Check	-505.92
04/10/2024		72179	Protelesis	Accounts Payable	Outstanding	Check	-168.20
04/10/2024		72180	PRUDENTIAL OVERALL SUPPLY	Accounts Payable	Outstanding	Check	-22.94
04/10/2024		72181	ROADRUNNER PUBLICATIONS, INC	Accounts Payable	Outstanding	Check	-173.25
04/10/2024		72182	T-Y Nursery	Accounts Payable	Outstanding	Check	-52,319.79
04/10/2024		72183	UNDERGROUND SERV. ALERT	Accounts Payable	Outstanding	Check	-17.50
04/10/2024		72184	Visual Edge IT, Inc	Accounts Payable	Outstanding	Check	-268.41
04/10/2024		72185	WATERLINE TECHNOLOGIES	Accounts Payable	Outstanding	Check	-2,504.93
04/10/2024		DFT0001820	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-1,260.01
04/10/2024		DFT0001821	SAN DIEGO COUNTY WATER AUTHORITY	Accounts Payable	Outstanding	Bank Draft	-95,079.00
04/16/2024		72186	VALIC GA#24515	Accounts Payable	Outstanding	Check	-800.00
04/16/2024		DFT0001822	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-691.61
04/16/2024		DFT0001823	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-685.37
04/16/2024		DFT0001824	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-1,728.39
04/16/2024		DFT0001825	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-3,729.01
04/16/2024		DFT0001826	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-8.37
04/16/2024		DFT0001827	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-1,220.99
04/16/2024		DFT0001828	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-350.70
04/16/2024		DFT0001829	EFTPS - Federal Payroll Tax	Accounts Payable	Outstanding	Bank Draft	-4,203.00
04/16/2024		EFT0000100	Payroll EFT	Payroll	Outstanding	EFT	-23,156.71
04/17/2024		72187	ACWA JPIA	Accounts Payable	Outstanding	Check	-17,396.16
04/17/2024		72188	ACWA/JPIA	Accounts Payable	Outstanding	Check	-3,476.81
04/17/2024		72189	AFLAC	Accounts Payable	Outstanding	Check	-35.88
04/17/2024		72190	AT & T MOBILITY	Accounts Payable	Outstanding	Check	-520.40
04/17/2024		72191	AT&T	Accounts Payable	Outstanding	Check	-182.66
04/17/2024		72192	CONTROLLED ENVIRONMENTS LLC	Accounts Payable	Outstanding	Check	-953.00
04/17/2024		72193	HACH COMPANY	Accounts Payable	Outstanding	Check	-1,092.00
04/17/2024		72194	KWC ENGINEERS	Accounts Payable	Outstanding	Check	-1,900.00
04/17/2024		72195	OPTIMIZED INVESTMENT PARTNERS	Accounts Payable	Outstanding	Check	-672.87
04/17/2024		72196	PRUDENTIAL OVERALL SUPPLY	Accounts Payable	Outstanding	Check	-63.62
04/17/2024		72197	RUTAN & TUCKER, LLP	Accounts Payable	Outstanding	Check	-714.78
04/17/2024		72198	WATERLINE TECHNOLOGIES	Accounts Payable	Outstanding	Check	-1,168.26
04/23/2024		72040	KWC ENGINEERS Reversal	Accounts Payable	Outstanding	Check Reversal	450.00
04/24/2024		72199	KWC ENGINEERS	Accounts Payable	Outstanding	Check	-2,200.00
04/30/2024		72200	VALIC GA#24515	Accounts Payable	Outstanding	Check	-800.00
04/30/2024		DFT0001830	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-692.70
04/30/2024		DFT0001831	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-686.45
04/30/2024		DFT0001832	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-1,724.57
04/30/2024		DFT0001833	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-3,720.76
04/30/2024		DFT0001834	CALPERS -FISCAL SERVICES DIV.	Accounts Payable	Outstanding	Bank Draft	-8.37
04/30/2024		DFT0001835	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-1,273.06
04/30/2024		DFT0001836	EFTPS - Federal Payroll Tax	Accounts Payable	Outstanding	Bank Draft	-166.66

Bank Transaction Report

Issued Date Range: -

Issued Date	Cleared Date	Number	Description	Module	Status	Type	Amount
04/30/2024		DFT0001837	EMPLOYMENT DEVELOPMENT DEPARTMENT	Accounts Payable	Outstanding	Bank Draft	-366.50
04/30/2024		DFT0001838	EFTPS - Federal Payroll Tax	Accounts Payable	Outstanding	Bank Draft	-4,431.13
04/30/2024		EFT0000101	Payroll EFT	Payroll	Outstanding	EFT	-24,238.27
Bank Account 57-955468-36 Total: (82)							-368,063.07
Report Total: (82)							-368,063.07

Government Code 53065.5 Reporting - Fiscal Year 2023/2024

No.	Name	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	2023/2024
1040	A. Simon								90.00	188.55				\$ 278.55
0900	M. Quinn				200.00				90.00					\$ 290.00
1349	M. Munaco				60.00									\$ 60.00
1772	A. Reeh													\$ -
1827	N. Ruiz													\$ -
1858	L. Brewer				183.91									\$ 183.91
1946	B. Easley			53.38		62.88		53.05		65.12				\$ 234.43
1997	R. Valenzuela		125.00					70.03						\$ 195.03
2068	J. Hudson									66.61				\$ 66.61
2070	C. Drown									256.47				\$ 256.47
	Totals	\$ -	\$ 125.00	\$ 53.38	\$ 443.91	\$ 62.88	\$ -	\$ 123.08	\$ 180.00	\$ 253.67	\$ -	\$ -	\$ -	\$ 1,241.92

California Government Code Section 53065.5

Each special district, as defined by subdivision (a) of Section 53036, shall, at least annually, disclose any reimbursement paid by the district within the immediately preceding fiscal year of at least one hundred (\$100) for each individual charge for services or products received. "Individual charge" includes, but is not limited to, one meal, lodging for one day, transportation, or a registration fee paid to any employee or member of the governing body of the district. The disclosure requirement shall be fulfilled by including the reimbursement information in a document published or printed at least annually by a date determined by that district and shall be made available for public inspection.

Government Code 53065.5 reporting
Breakdown available in the Finance Department



Pooled Cash Report

Yuima Municipal Water District

For the Period Ending 4/30/2024

ACCOUNT #	ACCOUNT NAME	BEGINNING BALANCE	CURRENT ACTIVITY	CURRENT BALANCE	
CLAIM ON CASH					
01-1001-000	Claim on Cash - Yuima General District	2,384,655.48	219,848.40	2,604,503.88	
02-1001-000	Claim on Cash - IDA	74,607.27	(123,981.35)	(49,374.08)	
10-1001-000	Claim on Cash - Yuima General District Capital	926,824.16	21,562.82	948,386.98	
20-1001-000	Claim on Cash - IDA Capital	333,310.89	6,983.64	340,294.53	
TOTAL CLAIM ON CASH		<u>3,719,397.80</u>	<u>124,413.51</u>	<u>3,843,811.31</u>	
CASH IN BANK					
Cash in Bank					
99-1000-000	Petty Cash	500.00	0.00	500.00	
99-1000-011	General Checking	119,218.76	157,442.12	276,660.88	
99-1100-015	General Savings	10,123.46	4.87	10,128.33	
99-1100-017	Official Pay	21,219.75	(11,258.80)	9,960.95	
99-1200-020	LAIF State Treasury	5,299.10	5,609.33	10,908.43	
99-1200-021	California CLASS	947,642.27	84,195.38	1,031,837.65	
99-1300-030	UBS Financial Services - Clearing	5,368.50	(2,933.46)	2,435.04	
99-1300-035	Higgins Capital Management - Clearing	2,343.34	7,657.06	10,000.40	
99-1400-041	Valley Strong CD - CUSIP 920133AN5	244,889.75	(147.00)	244,742.75	
99-1400-046	BMO Harris Bank - 05600XCG3	92,221.00	83.00	92,304.00	
99-1400-051	BMW Bank - 05580AH64	194,004.00	644.00	194,648.00	
99-1400-053	Sallie Mae - 795451AN3	231,352.50	(142.50)	231,210.00	
99-1400-054	State Bank of India - 856285VD0	230,697.50	182.50	230,880.00	
99-1400-057	BMO Harris Bank - 05600XGP9	240,244.55	56.35	240,300.90	
99-1400-062	Flagstar Bank - 33847E4D6	97,564.00	361.00	97,925.00	
99-1450-042	US Treasury Note - 91282CDP3	123,771.21	(2,528.13)	121,243.08	
99-1450-043	US Treasury Note - 91282CGT2	121,918.75	(2,162.50)	119,756.25	
99-1450-045	US Treasury Note - 91282CHK0	123,676.25	(2,367.50)	121,308.75	
99-1450-056	FHLB BOND CUSIP 3130AVNE8	248,900.00	(75.00)	248,825.00	
99-1450-061	FHLB Bond - 3130AJZ36	94,142.00	0.00	94,142.00	
99-1450-063	FHLB Step-Up Bond - 3130AR2X8	99,477.00	(24.00)	99,453.00	
99-1450-064	US Treasury Note 912828CCY5	122,904.60	(2,356.20)	120,548.40	
99-1450-068	FHLB Step-Up Bond - 3130AMAW2	235,442.50	(1,350.00)	234,092.50	
TOTAL: Cash in Bank		<u>3,719,397.80</u>	<u>124,413.51</u>	<u>3,843,811.31</u>	
TOTAL CASH IN BANK		<u>3,719,397.80</u>	<u>124,413.51</u>	<u>3,843,811.31</u>	
DUE TO OTHER FUNDS					
99-2601-000	Due to Other Funds	3,719,397.80	124,413.51	3,843,811.31	
TOTAL DUE TO OTHER FUNDS		<u>3,719,397.80</u>	<u>124,413.51</u>	<u>3,843,811.31</u>	
Claim on Cash	3,843,811.31	Claim on Cash	3,843,811.31	Cash in Bank	3,843,811.31
Cash in Bank	3,843,811.31	Due To Other Funds	3,843,811.31	Due To Other Funds	3,843,811.31
Difference	<u>0.00</u>	Difference	<u>0.00</u>	Difference	<u>0.00</u>

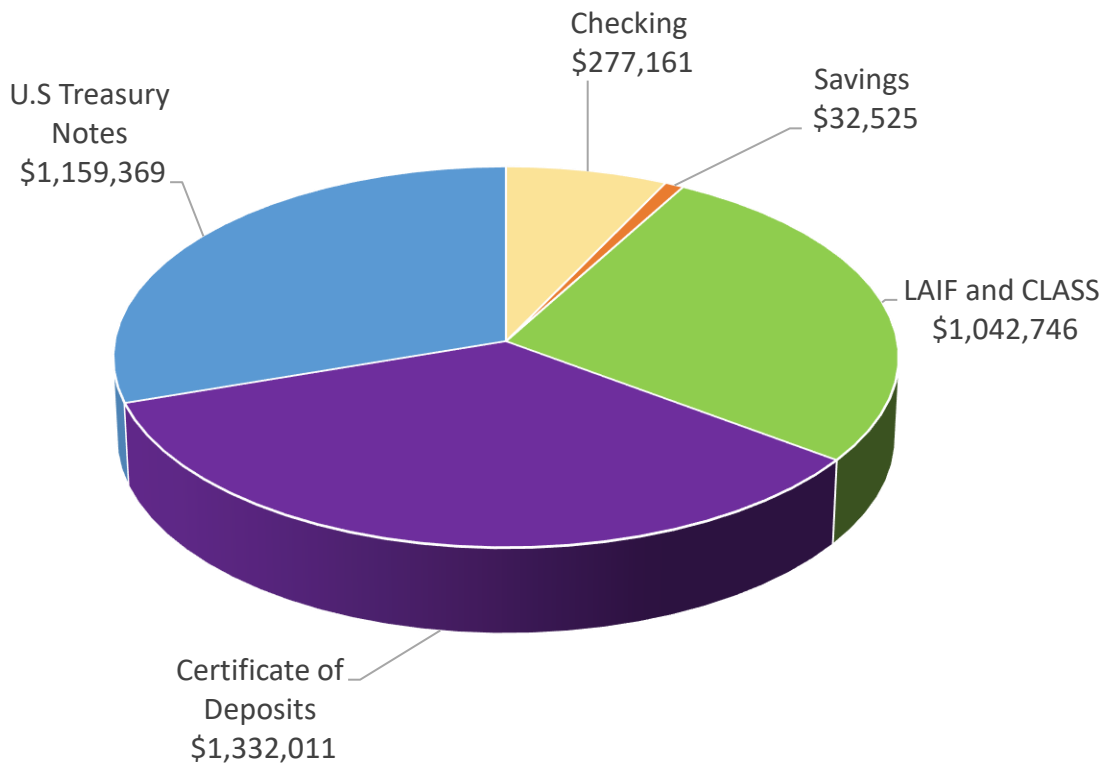
ACCOUNT #	ACCOUNT NAME	BEGINNING BALANCE	CURRENT ACTIVITY	CURRENT BALANCE	
ACCOUNTS PAYABLE PENDING					
01-2555-000	AP Pending - General District	289,761.84	151,357.68	441,119.52	
02-2555-000	AP Pending - IDA	3,890.26	72,807.73	76,697.99	
TOTAL ACCOUNTS PAYABLE PENDING		<u>295,662.10</u>	<u>222,155.41</u>	<u>517,817.51</u>	
DUE FROM OTHER FUNDS					
99-1501-000	Due From General District	(289,761.84)	(151,357.68)	(441,119.52)	
99-1502-000	Due From IDA	(3,890.26)	(72,807.73)	(76,697.99)	
TOTAL DUE FROM OTHER FUNDS		<u>(295,662.10)</u>	<u>(222,155.41)</u>	<u>(517,817.51)</u>	
ACCOUNTS PAYABLE					
99-2555-000	Accounts Payable	295,662.10	222,155.41	517,817.51	
TOTAL ACCOUNTS PAYABLE		<u>295,662.10</u>	<u>222,155.41</u>	<u>517,817.51</u>	
AP Pending	517,817.51	AP Pending	517,817.51	Due From Other Funds	517,817.51
Due From Other Funds	517,817.51	Accounts Payable	517,817.51	Accounts Payable	517,817.51
Difference	<u>0.00</u>	Difference	<u>0.00</u>	Difference	<u>0.00</u>

Yuima Municipal Water District

Cash & Investments Data

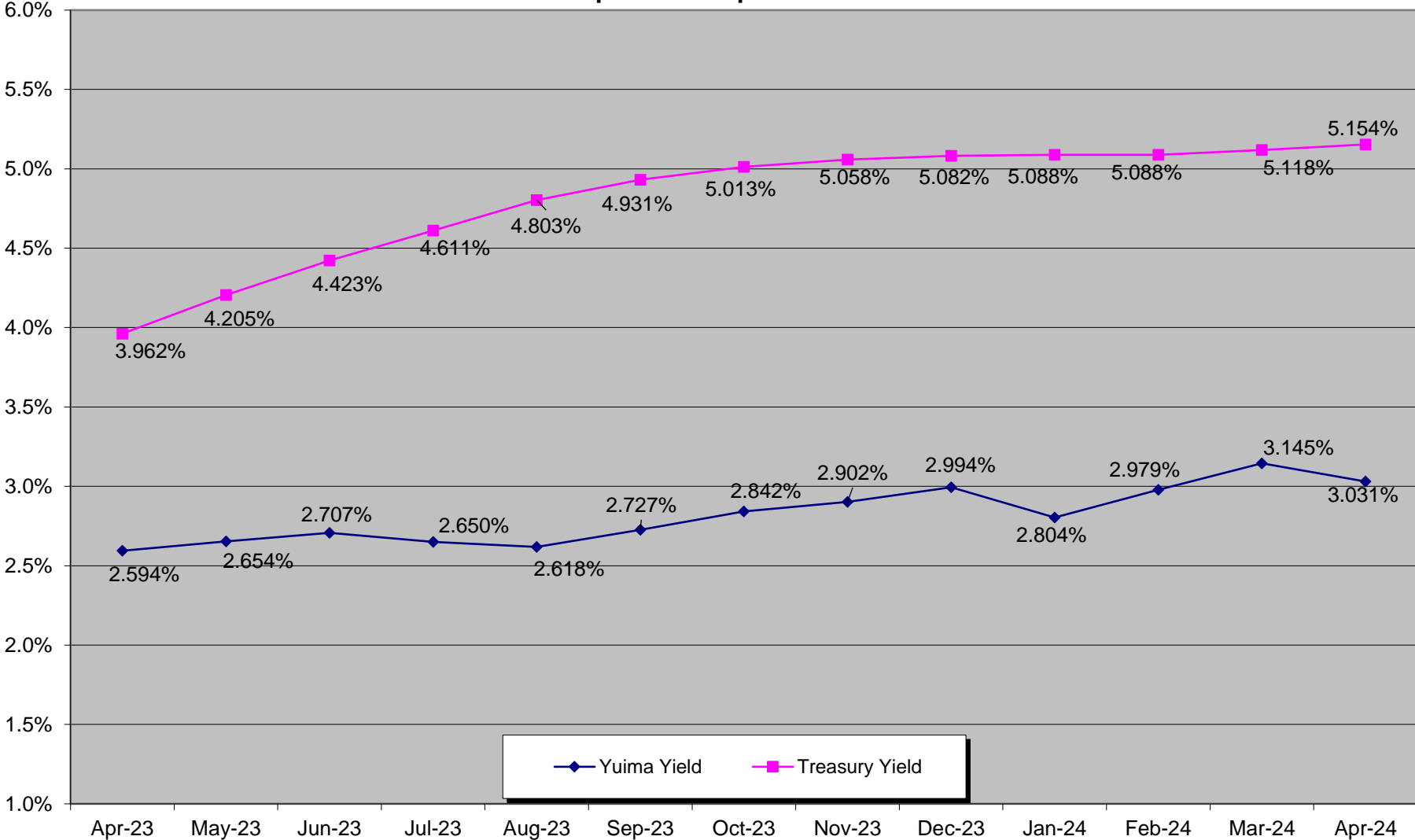
April 2024

\$3,843,811.31



Aggregate Yuima Portfolio Yield

April 2023 - April 2024





State of California Pooled Money Investment Account Market Valuation 4/30/2024

Description	Carrying Cost Plus Accrued Interest Purch.	Fair Value	Accrued Interest
United States Treasury:			
Bills	\$ 35,373,771,328.36	\$ 35,812,925,867.50	NA
Notes	\$ 64,807,714,652.49	\$ 63,983,688,682.50	\$ 372,328,906.00
Federal Agency:			
SBA	\$ 257,148,292.59	\$ 251,439,956.55	\$ 1,245,990.70
MBS-REMICs	\$ 1,969,219.55	\$ 1,913,742.70	\$ 8,590.56
Debentures	\$ 8,032,854,727.68	\$ 7,929,641,345.00	\$ 48,426,221.95
Debentures FR	\$ -	\$ -	\$ -
Debentures CL	\$ 1,600,000,000.00	\$ 1,585,020,400.00	\$ 12,312,291.00
Discount Notes	\$ 25,938,670,854.06	\$ 26,205,125,600.00	NA
Supranational Debentures	\$ 2,919,839,134.05	\$ 2,874,057,240.00	\$ 15,976,237.00
Supranational Debentures FR	\$ -	\$ -	\$ -
CDs and YCDs FR	\$ -	\$ -	\$ -
Bank Notes			
CDs and YCDs	\$ 15,150,015,000.00	\$ 15,144,578,111.20	\$ 218,884,486.12
Commercial Paper	\$ 11,212,045,541.69	\$ 11,315,194,958.32	NA
Corporate:			
Bonds FR	\$ -	\$ -	\$ -
Bonds	\$ 699,090,069.71	\$ 679,642,499.00	\$ 6,191,909.65
Repurchase Agreements	\$ -	\$ -	\$ -
Reverse Repurchase	\$ -	\$ -	\$ -
Time Deposits	\$ 5,125,000,000.00	\$ 5,125,000,000.00	NA
PMIA & GF Loans	\$ 349,834,000.00	\$ 349,834,000.00	NA
TOTAL	\$ 171,467,952,820.18	\$ 171,258,062,402.77	\$ 675,374,632.98

Fair Value Including Accrued Interest \$ 171,933,437,035.75

Repurchase Agreements, Time Deposits, PMIA & General Fund loans, and Reverse Repurchase agreements are carried at portfolio book value (carrying cost).



PMIA/LAIF Performance Report as of 5/15/24



Quarterly Performance Quarter Ended 03/31/24

LAIF Apportionment Rate ⁽²⁾ :	4.30
LAIF Earnings Ratio ⁽²⁾ :	0.00011755619077389
LAIF Administrative Cost ^{(1)*} :	0.27
LAIF Fair Value Factor ⁽¹⁾ :	0.994191267
PMIA Daily ⁽¹⁾ :	4.22
PMIA Quarter to Date ⁽¹⁾ :	4.12
PMIA Average Life ⁽¹⁾ :	226

PMIA Average Monthly Effective Yields⁽¹⁾

April	4.272
March	4.232
February	4.122
January	4.012
December	3.929
November	3.843

Pooled Money Investment Account Monthly Portfolio Composition ⁽¹⁾ 4/30/24 \$171.5 billion

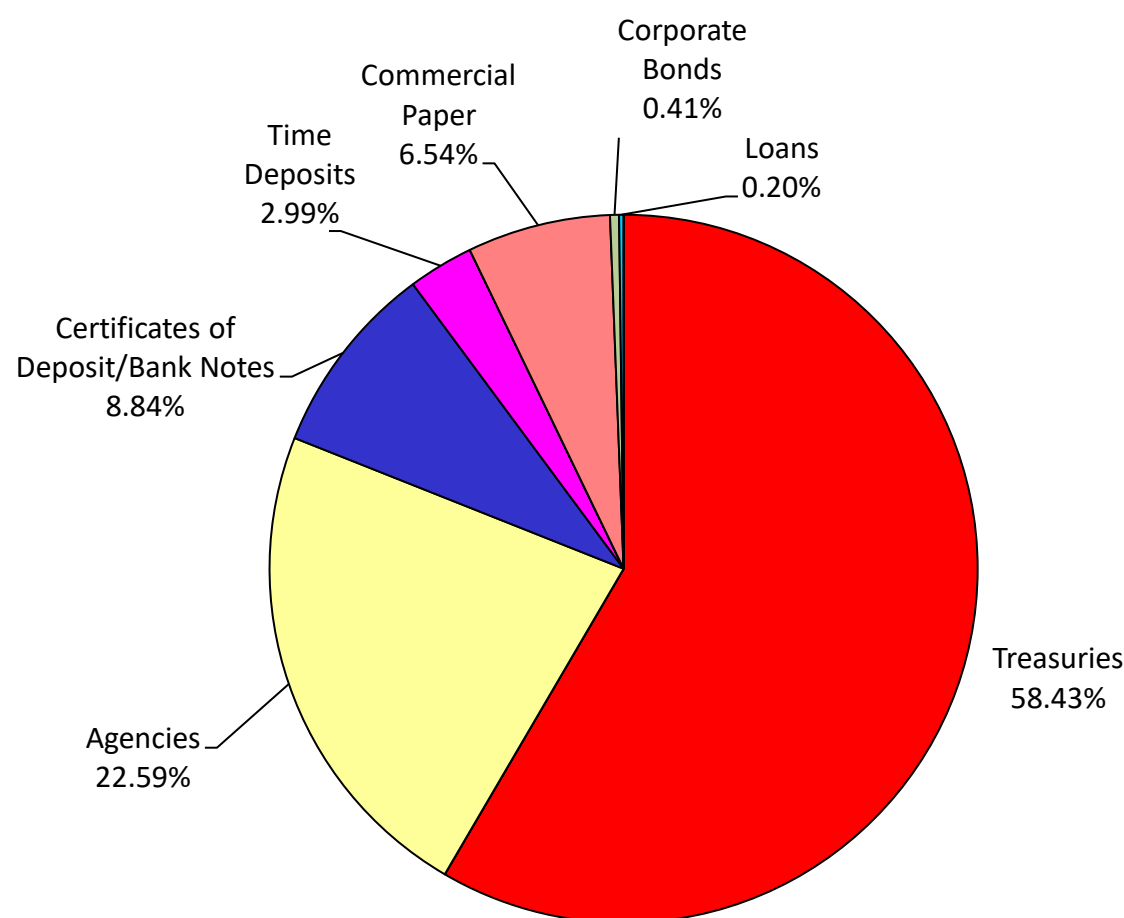


Chart does not include \$1,969,000.00 in mortgages, which equates to 0.001%. Percentages may not total 100% due to rounding.

Daily rates are now available here. [View PMIA Daily Rates](#)

Notes: The apportionment rate includes interest earned on the CalPERS Supplemental Pension Payment pursuant to Government Code 20825 (c)(1) and interest earned on the Wildfire Fund loan pursuant to Public Utility Code 3288 (a).

*The percentage of administrative cost equals the total administrative cost divided by the quarterly interest earnings. The law provides that administrative costs are not to exceed 5% of quarterly EARNINGS of the fund. However, if the 13-week Daily Treasury Bill Rate on the last day of the fiscal year is below 1%, then administrative costs shall not exceed 8% of quarterly EARNINGS of the fund for the subsequent fiscal year.

Source:

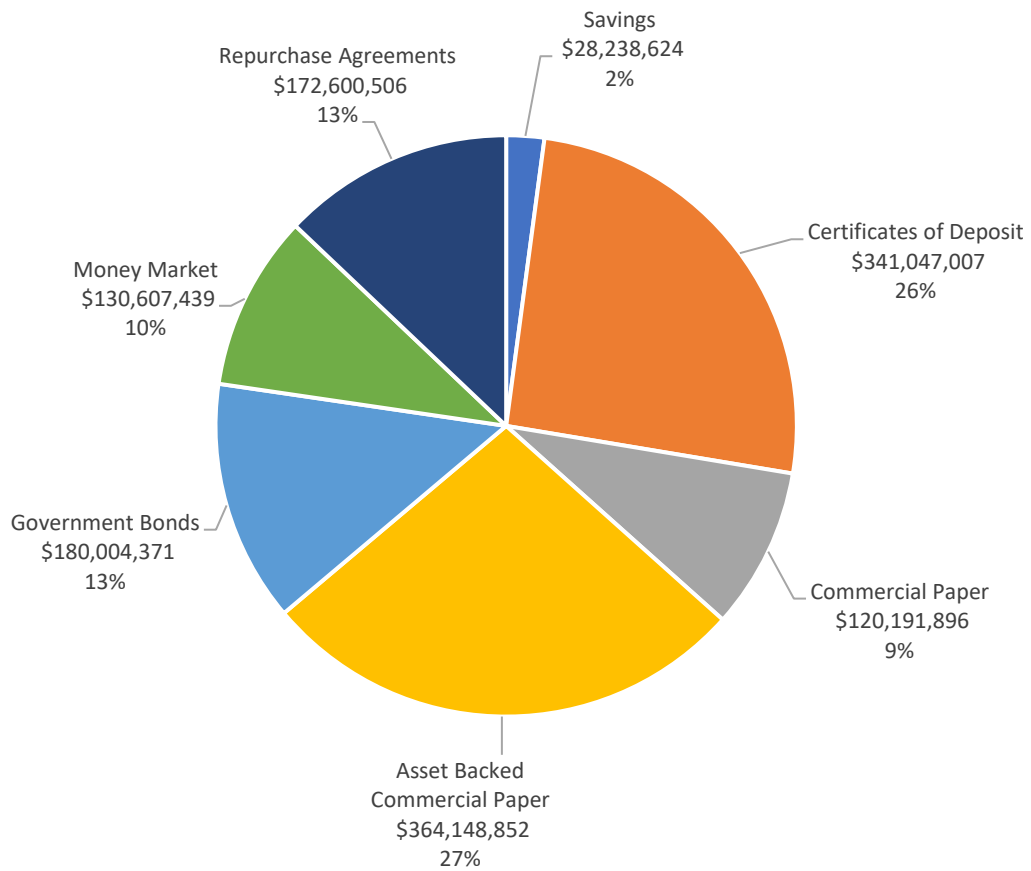
⁽¹⁾ State of California, Office of the Treasurer

⁽²⁾ State of California, Office of the Controller

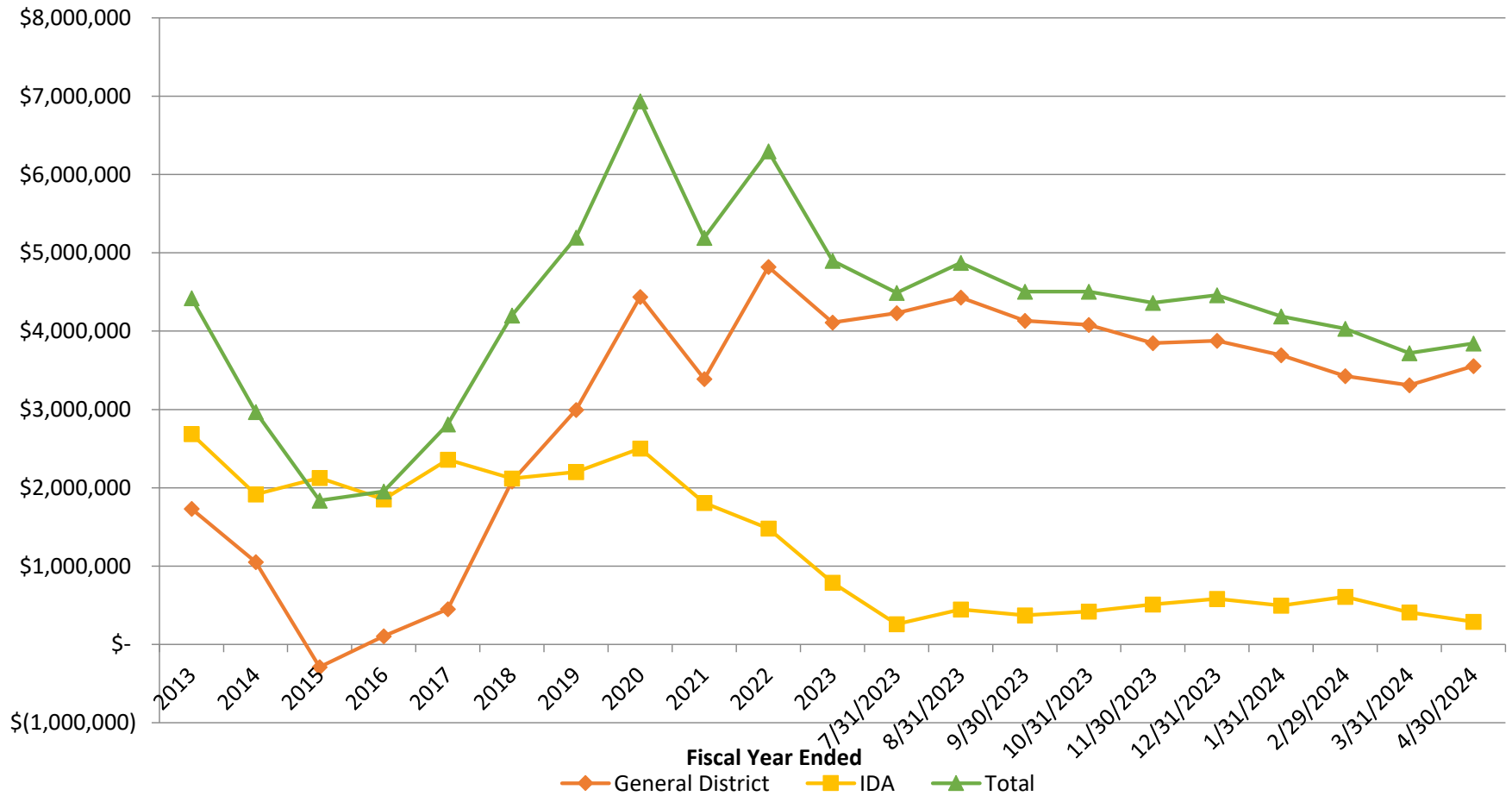
California CLASS Schedule of Investments

April 2024

Average Daily Yield
5.403%



Cash Position



ACTION DISCUSSION

The background features a light blue gradient with several realistic water droplets of various sizes scattered across the surface. The droplets have highlights and shadows, giving them a three-dimensional appearance. A large, faint, red-outlined watermark with the word "DRAFT" is oriented diagonally across the center of the page.

YUIMA MUNICIPAL WATER DISTRICT

2024-25 PRELIMINARY BUDGET

BUDGET AND RATE DEVELOPMENT PROCESS

Operational
Needs
Assessment

DISCUSSION, ASSESSMENT AND DETERMINATION OF DISTRICT NEEDS FOR OPERATIONS, CAPITAL PROJECTS, OTHER OPERATING RECOMMENDATIONS.

Water Sales
&
Production

ESTIMATE WATER SALES AND LOCAL PRODUCTION TO DETERMINE ESTIMATED CWA PURCHASES.

Imported
Water Costs
SDCWA Rates

DETERMINE COSTS OF IMPORTED WATER ONCE SDCWA HAS ADOPTED THEIR RATES FOR THE NEW FISCAL YEAR.

Revenue
Requirement
Analysis

DETERMINE TOTAL REVENUES NEEDED TO FUND OPERATIONS, CAPITAL, DEBT SERVICE, AND OTHER OPERATING REQUIREMENTS.

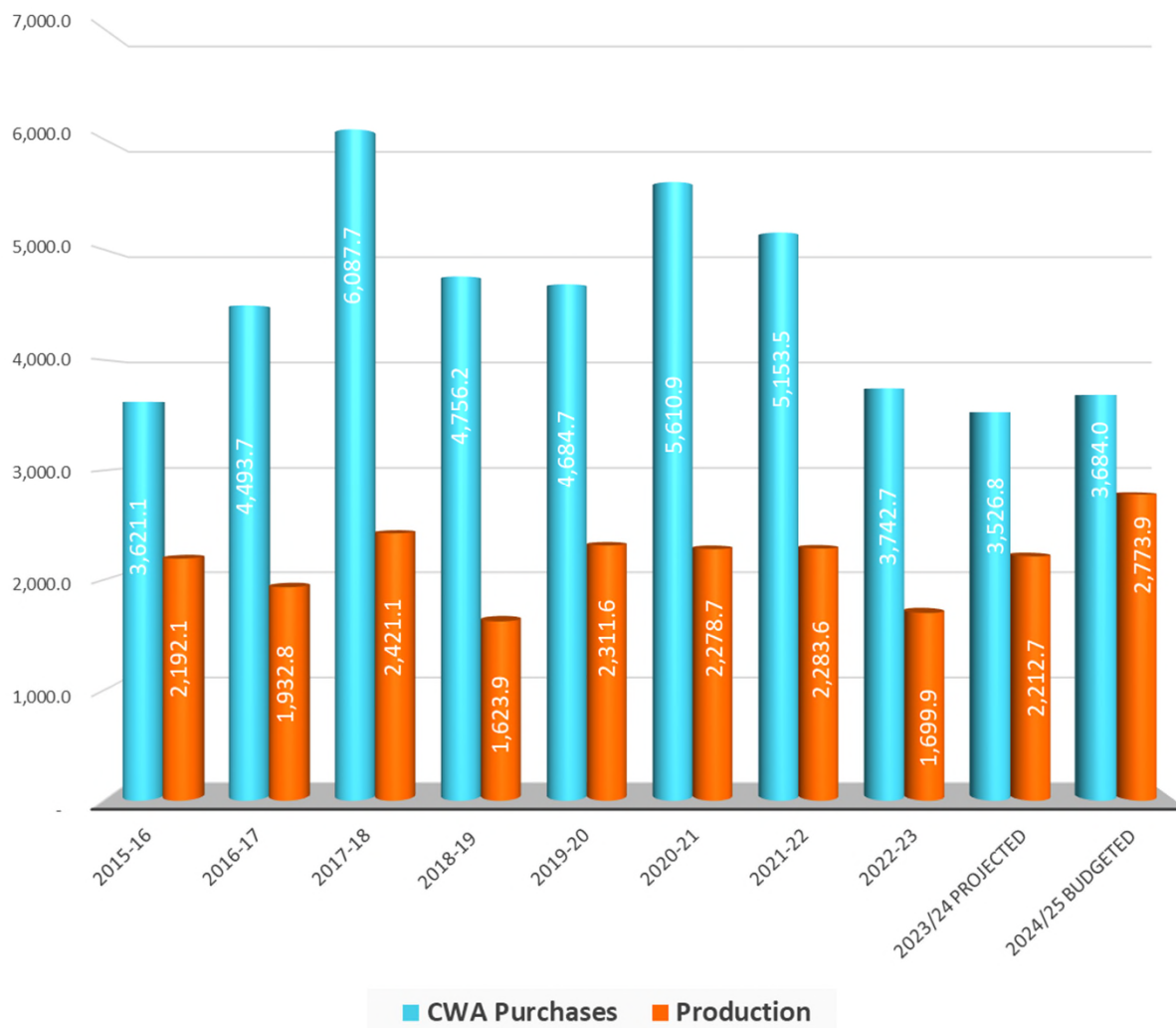
Water Rates
&
Charges

SET RATES TO RECOVER ALL COSTS OF OPERATIONS, CAPITAL, ETC.

NEEDS ASSESSMENT

- ADMINISTRATIVE & OPERATIONS DEPARTMENT RECOMMENDATIONS – 2023/24
 - COST CURTAIL TO REDUCE RATE INCREASE
- 2024/25 ASSESSMENT
 - STAFFING NEEDS
 - NEW GSA PUMPING FEES
 - CURTAIL SIGNIFICANT RATE INCREASE FROM SDCWA
 - DELAYED CAPITAL ASSETS MAINTENANCE
 - CONTINUAL INCREASE IN EVERYDAY COSTS
 - WATER TREATMENT
 - ELECTRICITY

CWA Purchases vs. Production Comparison

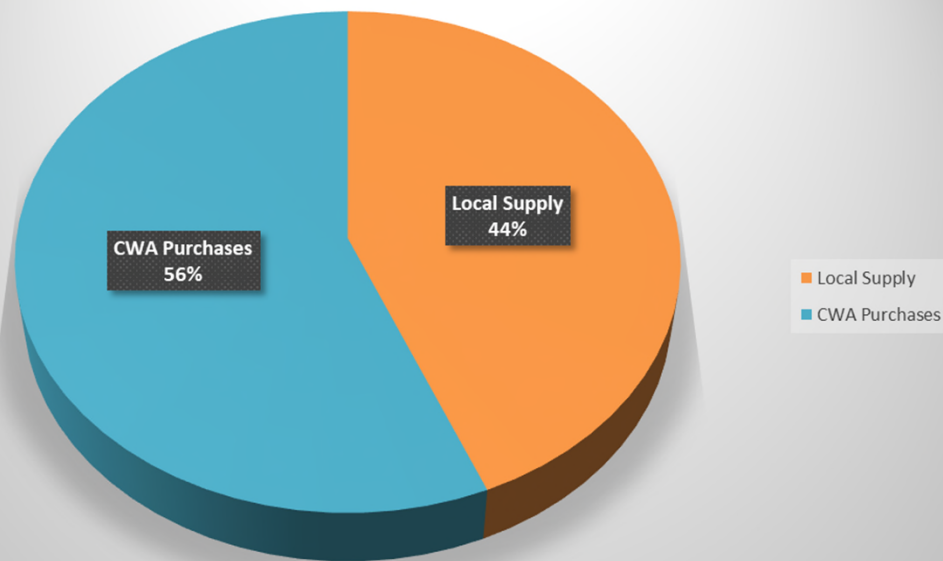


LOCAL PRODUCTION & CWA WATER PURCHASES

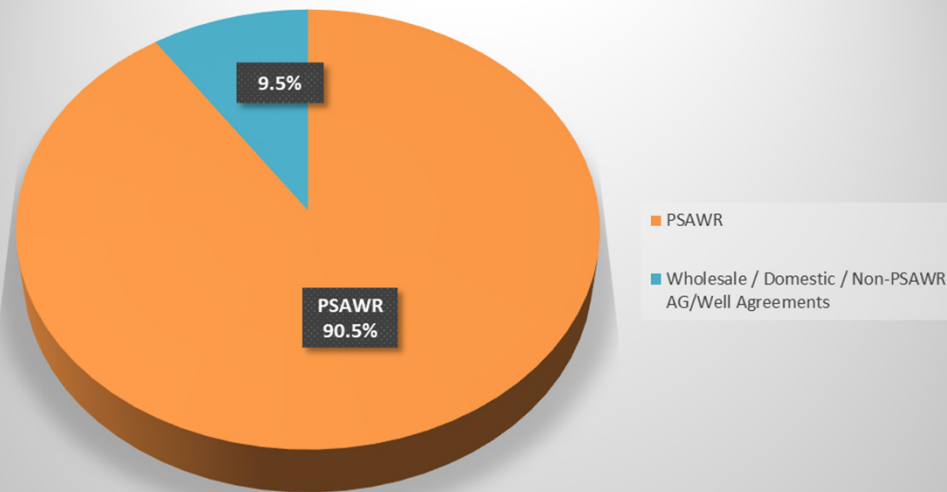
- BASED ON 10-YEAR AVERAGE
- LOCAL PRODUCTION – ESTIMATES A 25.3% INCREASE FROM 23/24 PROJECTIONS.
- CWA PURCHASED WATER, ESTIMATES A 4.4% INCREASE IN CWA PURCHASED WATER FROM 23/24 PROJECTIONS.
 - ALTHOUGH LOCAL PRODUCTION HAS INCREASED AT TIMES THE CWA PURCHASE AVERAGE INCREASED SLIGHTLY DUE TO PURCHASING BLEND WATER AND SUPPLEMENTING WHEN WELLS ARE DOWN.

WATER PURCHASES

Imported to Local Supply Breakdown



PSAWR Agricultural to Domestic / Non-PSAWR Breakdown



CWA & MET RATES

THESE ARE ESTIMATES AS THE SDCWA RECOMMENDED RATES HAVE NOT BEEN APPROVED

- CWA RATE ESTIMATES
 - 19.2 % INCREASE SUPPLY RATE
 - 2.8-15.8% OVERALL
 - PSAWR CREDIT \$518
- FIXED COST PASS-THRU LARGELY UNKNOWN
 - PASSED THROUGH DIRECTLY TO CUSTOMER

Metropolitan (MET) & County Water Authority Treated Water Rate				
Acre Foot Charge	Rate	Rate	Change	% of
	1/1/2024	1/1/2025	per Ac. Ft.	Change
MET Supply Rate				
MET Supply Rate	\$332	\$290	-42	-12.7%
MET System Access Rate	389	463	74	19.0%
MET System Power Rate	182	159	-23	-12.6%
<i>Subtotal</i>	903	912	9	1.0%
MET Treatment Surcharge	353	483	130	36.8%
Total MET Supply Cost	\$1,256	\$1,395	139	11.1%
	Rate	Rate	Change	% of
	1/1/2024	1/1/2025	per Ac. Ft.	Change
CWA's "All-in" Rate				
Melded Supply Rate	\$1,200	\$1,430	230	19.2%
Melded Treatment Rate	400	500	100	25.0%
Transportation Rate	189	141	-48	-25.4%
Cost of Treated Water	\$1,789	\$2,071	282	15.8%
Cost for Treated M&I	\$1,789	\$2,071	\$282	15.8%
CWA's PSAWR Rate				
Melded Supply Rate	\$1,200	\$1,430	230	19.2%
Less: Agricultural Credit Programs				
(1) CWA/PSAWR Program (Supply Cost Benefit)	-297	-518	221	0.0%
Melded Treatment Rate	400	500	100	25.0%
Transportation Rate	189	141	-48	-25.4%
Net PSAWR Ag. Rate	\$1,492	\$1,553	61	2.8%

REVENUE REQUIREMENTS

• SOURCE OF SUPPLY	\$7,137,657
• PUMPING	2,441,846
• WATER TESTING	230,149
• TRANSMISSION & DISTRIBUTION	555,839
• CUSTOMER SERVICE	116,864
• GENERAL & ADMINISTRATIVE	1,867,341
• GENERAL PLANT	<u>788,210</u>
TOTAL REVENUE REQUIREMENT (EXPENSES)	\$13,179,431*

* DIFFERENCE DUE TO ROUNDING

SOURCE OF SUPPLY

Purchased Water - SDCWA	5,643,029
Purchased Water - Local	480,000
CWA/MET Fixed Costs	1,014,628
Total	7,137,657

- PURCHASED WATER IS 54.6% OF THE TOTAL OPERATING EXPENDITURES IN 2024/25
 - ESTIMATED TO SELL 6,342.9 ACRE FEET OF WATER
 - 56% OF OUR PROJECTED SALES IS EXPECTED TO BE PURCHASED FROM CWA (3,684.0AF)
 - THE BALANCE OF 2,773.9 ACRE FEET OF EXPECTED SALES WILL COME FROM LOCAL SUPPLIES (44%)
 - BASED ON A 10-YEAR AVERAGE PLUS 600AF OF NEW LOCAL SUPPLY
 - CERTIFIED AGRICULTURAL (PSAWR) USERS REPRESENT AN ESTIMATED 90.5 % OF PROJECTED SALES

OTHER REVENUE REQUIREMENT CATEGORIES

PUMPING:		2024/25 Budget	2023/24 Projection
Salaries & Wages		27,093	20,174
Power		2,372,108	2,221,545
Maintenance		42,645	20,819
Total		2,441,846	2,262,539
WATER TREATMENT:			
Salaries & Wages		108,440	72,317
Supplies/Chlorine		80,200	75,907
Maintenance & Wtr. Testing		38,209	27,845
Power		3,300	3,392
Total		230,149	179,461

Continued increases in electricity and water treatment (chlorine / water testing) are expected. While the cost of power has increased 76.8% since FY 2018/19, the pump fee has not been increased since that time. This is what is driving the significant increase in the pump fee.

OTHER REVENUE REQUIREMENT CATEGORIES

TRANSMISSION & DISTRIBUTION:		
Salaries & Wages		281,830
Materials & Supplies		2,500
Telemetry		25,817
Engineering		-
Maintenance		200,860
Signal Channel		321
Total		511,328

CUSTOMER EXPENSE:		
Salaries & Wages		114,214
Meter Repair & Maintenance		2,650
Total		116,864

OTHER REVENUE REQUIREMENT CATEGORIES

GENERAL & ADMINISTRATIVE:		
Salaries & Wages		462,510
Benefits		606,434
Professional Services-SGMA		36,000
Legal Fees		40,000
Accounting/Audit Fees		21,500
Insurance		96,650
Auto Expense		37,500
Telephone Expense		14,000
Uniform Expense		4,000
Office Expense		18,977
Postage Expense		4,500
Computer Expense		41,400
License/Permits/LAFCO/Fees		23,000
Utilities		5,500
Medical Exams/Physicals		670
Manager Expense		3,800
115% Debt Service Reserve		469,910
Education/Training Expense		2,500
Membership Fees		23,000
Total		1,911,851

OTHER REVENUE REQUIREMENT CATEGORIES

GENERAL PLANT:		
Salaries & Wages		88,276
Maintenance		32,894
Safety Programs/Equip.		2,800
Small Tools		4,500
Supplies		2,000
Radio Maintenance		550
Property Tax & Obsolete Inventory		847
Depreciation		656,343
Total		788,210

PERSONNEL

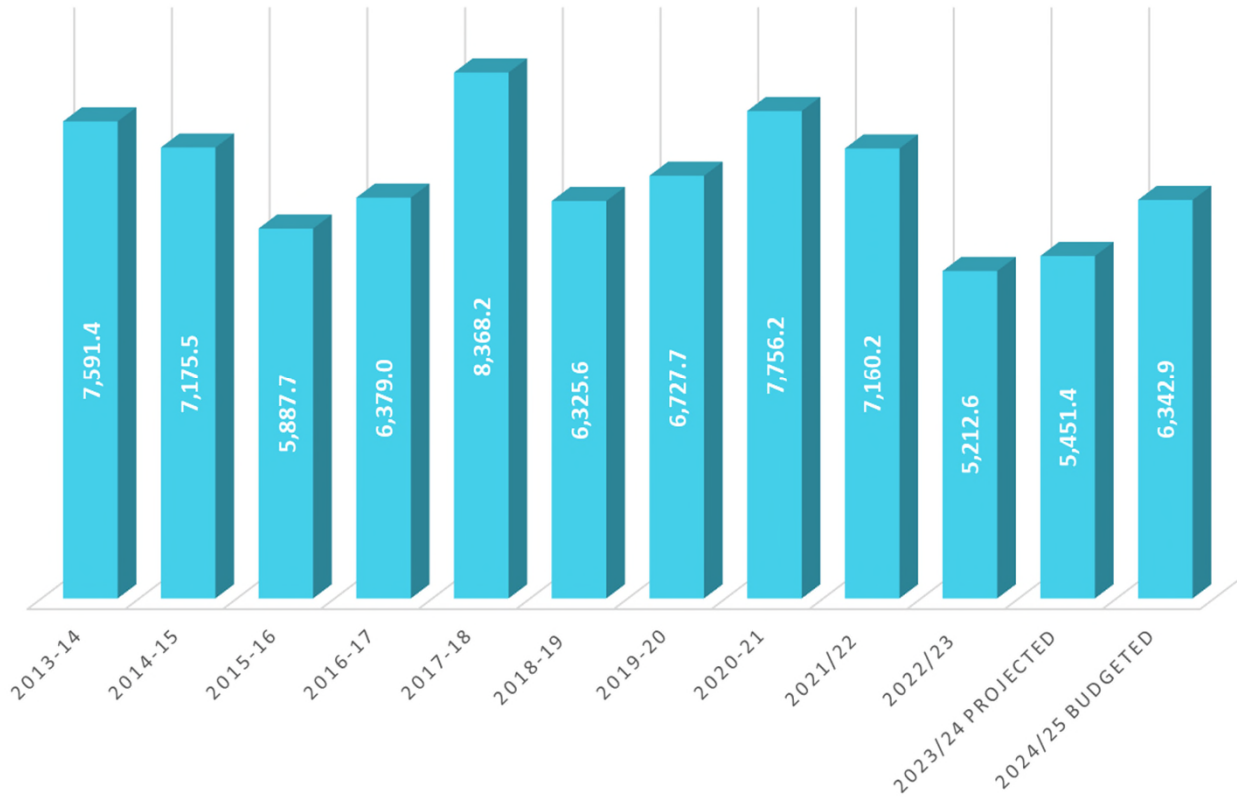
- SALARIES & BENEFITS OF \$1,688,466 MAKES UP 12.9% OF TOTAL BUDGET EXPENDITURES
 - TOTAL SALARIES \$1,082,032 – 66.0% OF TOTAL PERSONNEL COSTS
 - TOTAL BENEFITS \$606,434 – 34% OF TOTAL PERSONNEL COSTS
 - RETIREE ASSOCIATED COSTS \$6,600 – 1.0% OF TOTAL BENEFITS
 - PERS ACTIVE EMPLOYEES \$122,230 -20.2% OF TOTAL BENEFITS
 - PERS UNFUNDED LIABILITY \$217,758 – 35.9% OF TOTAL BENEFITS
 - MEDICAL, DENTAL, VISION, ETC. \$259,846. – 42.9% OF TOTAL BENEFITS
 - VACATION/SICK LEAVE ACCRUAL \$152,978 – 21.8% OF TOTAL BENEFITS

REVENUE RATES & CHARGES

- REVENUE GENERATION CATEGORIES

• WATER SALES & SERVICES	\$8,846,109
• CWA / MET FIXED COSTS	1,014,628
• MONTHLY METER FEES	876,155
• PUMP ZONE CHARGES	1,742,535
• SERVICE CONTRACTS MISC. NON-OPERATING REVENUE	<u>700,004</u>
TOTAL REVENUE	\$13,179,431*

WATER SALES - 10 YEAR AVERAGE



WATER SALES

- PROJECTED TO SELL 5,451.4 AF IN 2023/24
 - 4.5% INCREASE FROM 22/23
 - 17.8% LESS THAN THE BUDGETED AMOUNT
- ESTIMATED TO SELL 6,342.9 AF OF WATER IN 2024/25
 - ESTIMATED SALES ARE BASED ON A 10-YEAR AVERAGE
 - 16.3% INCREASE FROM 23/24 PROJECTIONS
 - 4.3% LESS THAN 23/24 BUDGETED

BASE WATER RATE

- THERE IS A PROPOSED INCREASE OF BETWEEN 6.2% AND 18.5% TO THE WATER COMMODITY RATE FOR THE 2024/25 FISCAL YEAR. THE LARGEST PART OF THIS INCREASE IS THE 19.2% INCREASE ON THE WATER RATE FROM THE SAN DIEGO COUNTY WATER AUTHORITY.

Rate Category	Current		Proposed		% Increase	Per Unit Increase
	Per Unit	Acre Foot	Per Unit	Acre Foot		
Yuima PSAWR Agricultural Rate	\$ 3.5888	\$ 1,563.29	\$ 3.8935	\$1,696.02	8.5%	\$ 0.3047
Yuima Domestic and Non-PSAWR Agricultural Rate	\$ 4.0868	\$ 1,780.20	\$ 4.6183	\$2,011.73	13.0%	\$ 0.5315
IDA PSAWR Agricultural Rate	\$ 2.8466	\$ 1,239.97	\$ 3.3738	\$1,469.62	18.5%	\$ 0.5272
IDA Domestic and Non-PSAWR Agricultural Rate	\$ 3.9692	\$ 1,728.97	\$ 4.2167	\$1,836.79	6.2%	\$ 0.2475

METER AND PUMP ZONE CHARGE

Yuima Meter Charge		
Size	Current	10% Proposed Increase
	Monthly	
5/8"	\$36.81	\$40.49
1"	58.91	64.80
1 1/2"	110.50	121.55
2"	191.54	210.69
3"	353.59	388.95
4"	604.06	664.47
5"	854.51	939.96
6"	1,105.00	1,215.50
8"	1,915.30	2,106.83
10"	2,872.27	3,159.50
Add'l Unit	59.06	64.97

Yuima Pump Zone Charge					
Pump Zone	Current		Proposed		% Increase
	Per Unit	Acre Foot	Per Unit	Acre Foot	
Zone 1	\$ 0.16900	\$ 73.62	\$ 0.21130	\$ 92.04	25.0%
Zone 2	\$ 0.37914	\$ 165.15	\$ 0.47390	\$ 206.43	25.0%
Zone 3	\$ 0.64249	\$ 279.87	\$ 0.80310	\$ 349.83	25.0%
Zone 4	\$ 0.81402	\$ 354.59	\$ 1.01750	\$ 443.22	25.0%
Zone 5	\$ 0.23755	\$ 103.48	\$ 0.29690	\$ 129.33	25.0%
Zone 6	\$ 0.23755	\$ 103.48	\$ 0.29690	\$ 129.33	25.0%
Zone 7	\$ 0.81402	\$ 354.59	\$ 1.01750	\$ 443.22	25.0%
Zone 11	\$ 0.23755	\$ 103.48	\$ 0.29690	\$ 129.33	25.0%

	PROPOSED BUDGET 2024/2025	-----COMBINED-----			-----GENERAL DISTRICT-----			-----IMPROVEMENT DISTRICT A-----		
		2023/24 BUDGET	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23	PROPOSED BUDGET 2024/2025	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23	PROPOSED BUDGET 2024/2025	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23
OPERATING REVENUES *	*6,342.9 ac. ft.	*6,931.3 ac. ft.	6,711.1 ac. ft.		4,283.7ac. ft.	5,099.2 ac. ft.		4,553.9 ac.ft.	5,026.8 ac. ft.	
Water Sales ¹	8,776,778 ⁽¹⁾	7,327,872	6,497,558	5,454,057	7,182,786	5,506,229	5,255,796	6,675,807	4,892,619	4,201,115
Water Services	69,331	5,200	88,029	81,037	69,331	87,849	81,037	-	180	-
Service Contracts	-	34,488	-	24,931	-	-	24,931	-	-	-
CWA/MET Fixed Costs	1,014,628	1,003,181	907,628	931,225	1,014,628	907,628	931,225	-	-	-
Meter Charges	876,155	796,414	784,764	778,203	358,371	320,767	321,727	517,784	463,997	456,476
Pump Zone Charges	1,742,535	1,429,250	1,141,886	1,187,269	536,828	362,938	384,676	1,205,707	778,948	802,593
Total Operating Revenues	12,479,427	10,596,405	9,419,866	8,456,722	9,161,944	7,185,411	6,999,394	8,399,298	6,135,744	5,460,183
OPERATING EXPENSES										
SOURCE OF SUPPLY:								* 2,495.0 ac.ft.		
Purchased Water - SDCWA	5,643,029	5,262,162	4,852,193	4,885,833	5,643,027	4,852,193	4,885,833	5,081,814	3,901,289	4,002,853
Purchased Water - Local	480,000	16,400	121,275	2,500	480,000	121,275	2,500	-	-	-
CWA/MET Fixed Costs	1,014,628	1,003,181	919,476	934,554	1,014,628	919,476	934,554	-	-	-
Total	7,137,657	6,281,743	5,892,943	5,822,887	7,137,655	5,892,943	5,822,887	5,081,814	3,901,289	4,002,853
PUMPING:										
Salaries & Wages	27,093	25,392	20,174	16,212	75	230	42	27,018	19,944	16,170
Power	2,372,108	1,540,100	2,221,545	1,885,769	743,347	632,820	559,001	1,628,761	1,588,725	1,326,767
Maintenance	42,645	78,000	20,819	76,411	12,645	9,027	6,343	30,000	11,792	70,068
Total	2,441,846	1,643,492	2,262,539	1,978,391	756,067	642,077	565,387	1,685,779	1,620,461	1,413,005
WATER TREATMENT:										
Salaries & Wages	108,440	52,727	72,317	63,829	48,358	12,667	9,431	60,082	59,649	54,398
Supplies/Chlorine	80,200	35,000	75,907	59,017	7,500	6,950	6,643	72,700	68,958	52,374
Maintenance & Wtr. Testing	38,209	33,200	27,845	9,883	16,527	4,298	1,958	21,682	23,547	7,925
Power	3,300	3,200	3,392	17,449	3,200	3,243	3,017	100	149	14,433
Total	230,149	124,127	179,461	150,178	75,585	27,159	21,049	154,564	152,303	129,129
TRANSMISSION & DISTRIBUTION:										
Salaries & Wages	281,830	228,402	195,046	167,595	129,676	84,055	100,032	152,154	110,991	67,563
Materials & Supplies	2,500	4,200	1,747	986	1,500	1,020	377	1,000	728	609
Telemetry	25,817	7,200	20,167	31,002	12,017	6,336	14,884	13,800	13,831	16,117
Engineering	-	-	-	-	-	-	-	-	-	-
Maintenance	200,860	161,747	18,945	71,852	43,631	5,022	28,031	157,229	13,924	43,821
Signal Channel	321	1,500	110	71	-	-	-	321	110	71
Total	511,328	403,049	236,015	271,503	186,824	96,432	143,325	324,504	139,583	128,179

¹ Combined Water Sales figures have been reduced by the amount allocated for IDA purchased water to eliminate duplication of inter-district exchange.

2024/25 PROPOSED BUDGET
2023/24 9 MONTH ACTUAL + 3 MONTH PROJECTED TO 6/30/2024
2022/23 ACTUAL YEAR END TOTALS

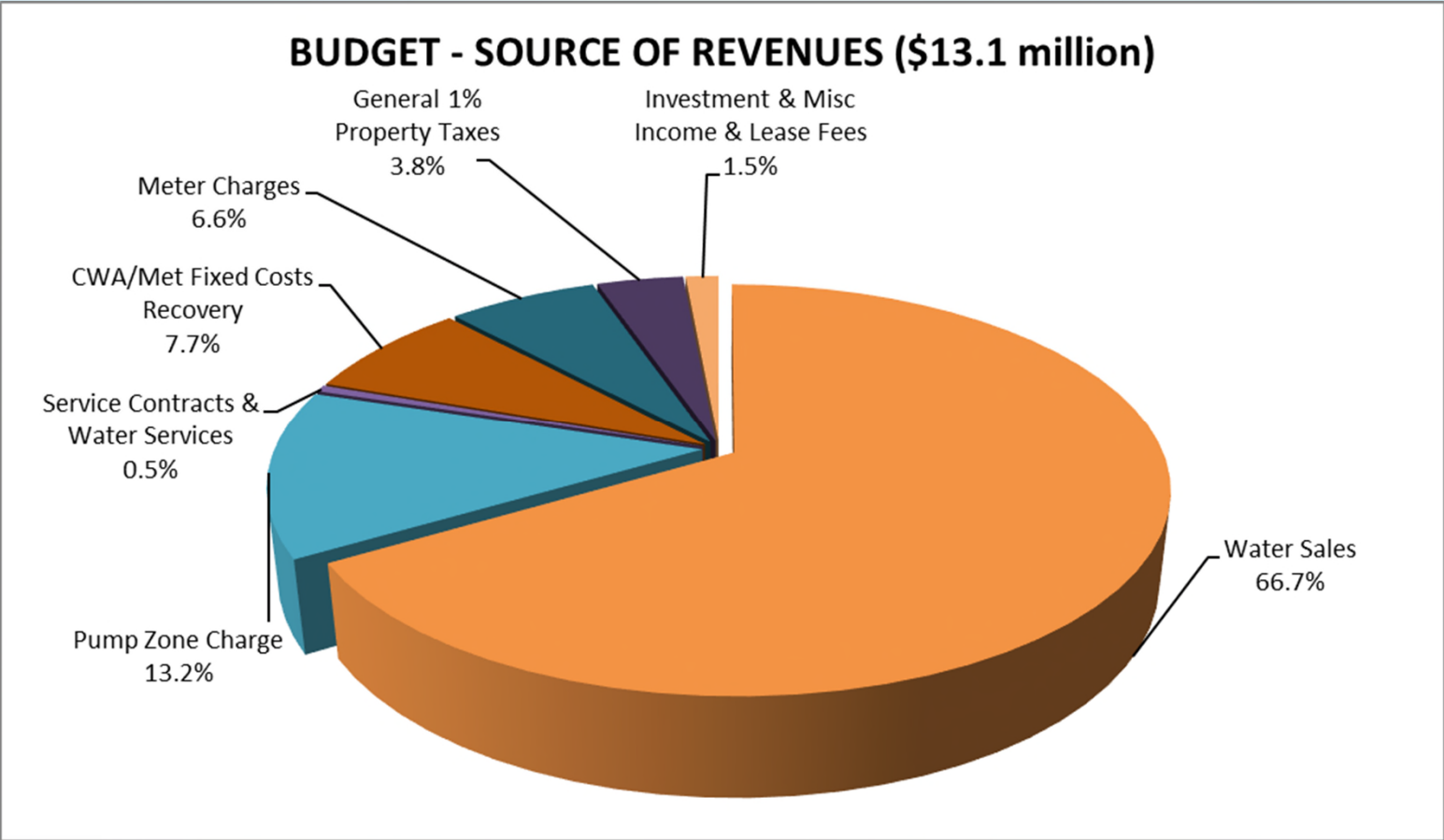
	PROPOSED BUDGET 2024/2025	-----COMBINED-----			-----GENERAL DISTRICT-----			-----IMPROVEMENT DISTRICT A-----		
		2023/24 BUDGET	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23	PROPOSED BUDGET 2024/2025	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23	PROPOSED BUDGET 2024/2025	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23
CUSTOMER EXPENSE:										
Salaries & Wages	113,883	97,174	105,876	105,072	56,807	49,238	49,119	57,076	56,638	55,953
Meter Repair & Maintenance	2,981	10,000	2,472	4,326	2,400	2,416	3,250	581	55	1,076
Total	116,864	107,174	108,348	109,396	59,207	51,655	52,367	57,657	56,693	57,029
GENERAL & ADMINISTRATIVE:										
Salaries & Wages	462,510	453,198	301,391	367,266	203,967	132,881	155,113	258,543	168,510	212,151
Benefits	606,434	474,045	592,802	704,961	267,437	247,372	312,221	338,997	345,429	392,740
Professional Services-SGMA	36,000	7,000	82,536	147,018	15,876	36,585	62,350	20,124	45,950	84,668
Legal Fees	40,000	55,000	31,550	59,207	17,640	14,357	29,789	22,360	17,192	29,417
Accounting/Audit Fees	21,500	16,500	-	21,960	9,482	-	9,293	12,019	-	12,667
Insurance	96,650	66,103	98,226	72,138	42,623	43,157	30,560	54,027	55,070	41,579
Auto Expense	37,500	23,500	40,378	27,901	16,538	17,969	12,061	20,963	22,409	15,840
Telephone Expense	14,000	14,215	12,327	13,130	6,174	5,448	5,565	7,826	6,878	7,565
Uniform Expense	4,000	3,510	3,664	3,621	1,764	1,614	1,532	2,236	2,050	2,089
Office Expense	18,977	15,265	20,139	26,746	8,369	8,933	11,293	10,608	11,206	15,453
Postage Expense	4,500	2,000	4,410	4,242	1,985	1,919	1,802	2,516	2,491	2,439
Computer Expense	41,400	29,710	60,989	37,886	18,257	27,025	16,045	23,143	33,964	21,841
License/Permits/LAFCO/Fees	23,000	16,600	26,287	22,258	10,143	10,006	11,443	12,857	16,281	10,815
Utilities	5,500	4,200	5,377	4,416	2,426	2,381	1,868	3,075	2,996	2,549
Medical Exams/Physicals	670	-	1,601	-	295	723	-	375	878	-
Manager Expense	3,800	500	3,755	4,759	1,676	1,673	2,040	2,124	2,081	2,719
115% Debt Service Reserve	469,910	540,725	-	-	385,000	-	-	84,910	-	-
Education/Training Expense	2,500	-	1,719	3,753	1,103	654	1,587	1,398	1,065	2,166
Membership Fees	23,000	16,000	21,687	16,107	10,143	9,666	6,738	12,857	12,021	9,367
Total	1,911,851	1,738,071	1,308,837	1,537,367	1,020,896	562,364	671,300	890,955	746,473	866,065
GENERAL PLANT:										
Salaries & Wages	88,276	79,631	34,290	57,711	38,930	15,350	24,371	49,346	18,939	33,340
Maintenance	32,894	13,500	21,005	31,503	14,685	8,862	13,332	18,209	12,142	18,172
Safety Programs/Equip.	2,800	1,500	2,776	2,902	1,235	1,506	1,148	1,565	1,269	1,756
Small Tools	4,500	1,200	2,252	3,823	1,985	1,009	1,606	2,516	1,243	2,218
Supplies	2,000	1,000	1,100	2,710	882	397	1,214	1,118	703	1,495
Radio Maintenance	550	550	251	1,158	243	110	503	307	141	655
Property Tax & Obsolete Inventory	847	850	368	21,727	500	368	355	347	-	21,371
Depreciation	656,343	778,514	665,479	666,276	302,174	300,941	302,174	354,169	364,538	364,101
Total	788,210	876,745	727,520	787,810	360,633	328,544	344,703	427,577	398,976	443,107
OTHER EXPENSE:										
Total Contract Services Expenses	41,526	-	47,070	-	41,526	47,070	-	-	-	-
TOTAL OPERATING EXPENSE	13,179,431	11,174,401	10,762,733	10,657,532	9,638,393	7,648,243	7,621,019	8,622,851	7,015,778	7,039,367
OPERATING MARGIN	(700,003)	(577,996)	(1,342,867)	(2,200,809)	(476,449)	(462,832)	(621,625)	(223,553)	(880,034)	(1,579,184)

2024/25 PROPOSED BUDGET
2023/24 9 MONTH ACTUAL + 3 MONTH PROJECTED TO 6/30/2024
2022/23 ACTUAL YEAR END TOTALS

	PROPOSED BUDGET 2024/2025	-----COMBINED-----			-----GENERAL DISTRICT-----			-----IMPROVEMENT DISTRICT A-----		
		2023/24 BUDGET	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23	PROPOSED BUDGET 2024/2025	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23	PROPOSED BUDGET 2024/2025	2023/24 PROJECTED TO 06/30/24	2022/23 ACTUAL 06/30/23
		OPERATING MARGIN - from page 2	(700,003)	(577,996)	(1,342,867)	(2,200,809)	(476,449)	(462,832)	(621,625)	(223,553)
NON-OPERATING REVENUES										
Tax Revenue - General	507,212	384,832	510,066	560,031	428,949	431,363	474,691	78,263	78,703	85,340
Water Availability	92,936	68,935	93,370	94,689	64,882	65,210	65,589	28,054	28,160	29,099
MET Stand-by credit	-	107,731	-	-	-	-	-	-	-	-
MET Ready-to-Serve charge	-	-	-	-	-	-	-	-	-	-
Connection Fees/Debt Service Interest	(129,020)	(150,406)	(97,416)	(128,936)	(111,454)	(83,833)	(108,891)	(17,566)	(13,583)	(20,046)
SDCWA- Infrastructure Access Charge Collected	30,100	31,140	29,796	29,520	30,100	29,796	29,520	-	-	-
Misc. Income & Lease Fees	136,361	117,942	115,916	188,743	-	(29,784)	15,715	136,361	145,700	173,028
Interest on Investments & Deliq. Accts.	119,922	48,500	231,776	92,599	95,000	212,971	57,172	24,922	25,426	35,427
County Contribution to Fire Protection	-	-	-	6,421	-	-	6,421	-	-	-
	-	-	-	-	-	-	-	-	-	-
NON-OPERATING EXPENSES										
Water Availability to Capital Reserve	(92,936) ⁽²⁾	(68,935)	(93,370)	(93,898)	(64,882)	(65,210)	(64,913)	(28,054)	(28,160)	(28,984)
MET Stand-by charge to Capital	-	(107,730)	-	-	-	-	-	-	-	-
MET Ready-to-serve to Capital	-	-	-	-	-	-	-	-	-	-
Conn. Fees/Debt Int Exp. to Capital	129,020 ⁽³⁾	150,406	97,416	128,936	111,454	83,833	108,891	17,566	13,583	20,046
SDCWA-Infrastructure Access Charge	(39,944) ⁽⁴⁾	(41,286)	(39,550)	(39,338)	(30,100)	(29,922)	(29,874)	(9,844)	(9,628)	(9,464)
50% Invest Rev. to Capital Reserve	(53,650) ⁽⁵⁾	(32,250)	(59,644)	(46,235)	(47,500)	(53,252)	(35,853)	(6,150)	(6,392)	(10,382)
Transfer Fire Protection Funds to Fire	-	-	-	(4,271)	-	-	(4,271)	-	-	-
Trans. to Capital Reserves	- ⁽⁶⁾	(130,506)	-	-	-	-	-	-	-	-
Transfer from Rate Stabilization Fund	-	199,620	1,166,397	-	-	-	-	-	1,166,397	-
Total Non-Operating Revenues	700,004	577,993	1,954,757	788,260	476,449	561,173	514,196	223,553	1,400,205	274,064
NET MARGIN	(0)	-	611,890	(1,412,550)	0	98,341	(107,429)	(0)	520,171	(1,305,120)
RECAP										
TOTAL INCOME	13,179,431	11,174,398	11,374,623	9,244,982	9,638,393	7,746,584	7,513,590	8,622,851	7,535,949	5,734,247
TOTAL EXPENSE	13,179,431	11,174,398	10,762,732	10,657,532	9,638,393	7,648,243	7,621,019	8,622,851	7,015,778	7,039,367
NET MARGIN	(0)	0	611,891	(1,412,550)	0	98,341	(107,429)	(0)	520,171	(1,305,120)

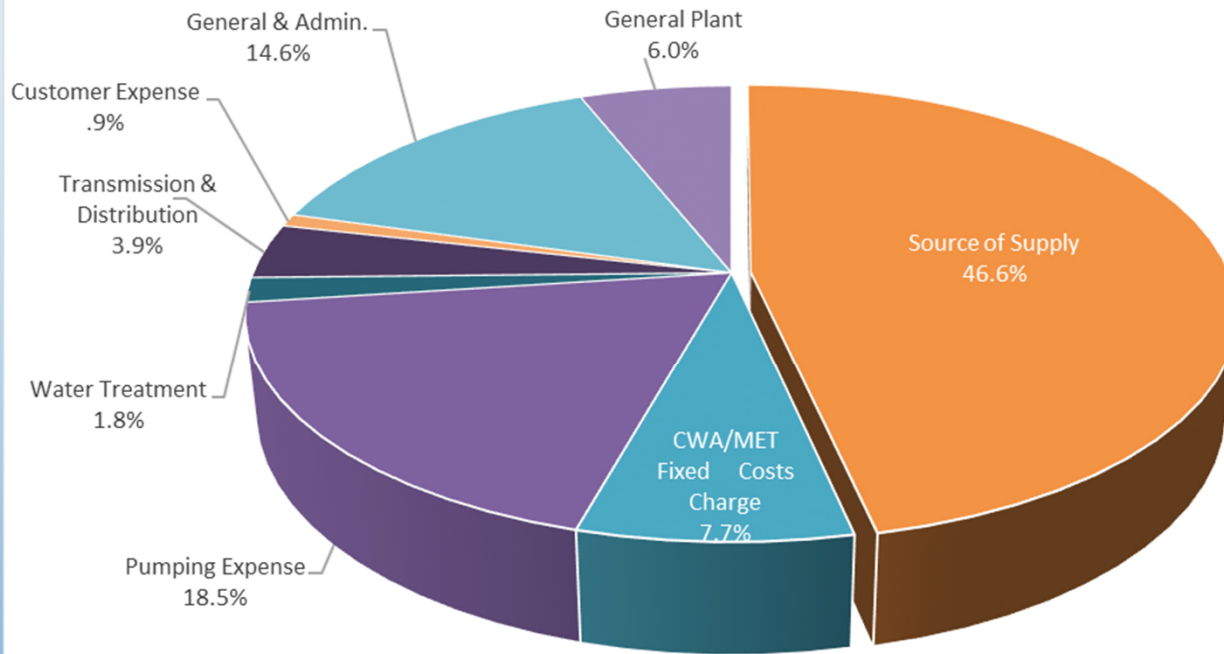
**BUDGET RECAP - SOURCE OF REVENUES
2024-25**

BUDGET - SOURCE OF REVENUES (\$13.1 million)



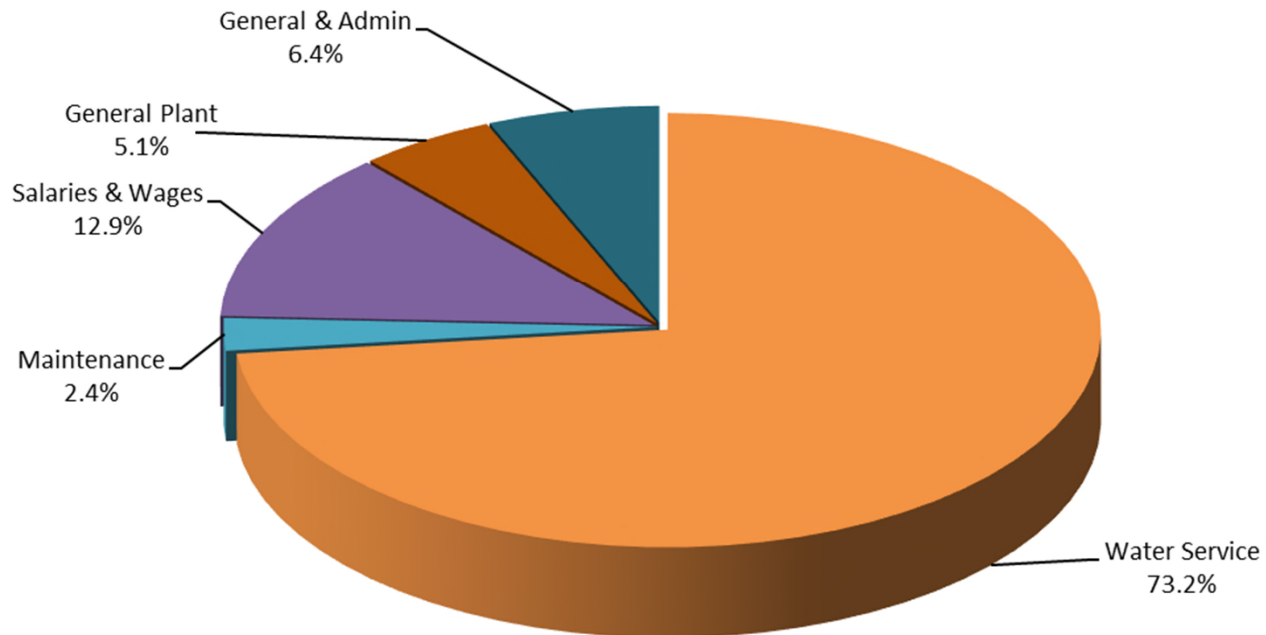
BUDGET RECAP - EXPENDITURES BY BUDGET ELEMENTS 2024-25

MAJOR BUDGET ELEMENTS - EXPENDITURES (\$13.1 million)



BUDGET RECAP - EXPENSE BY MAJOR CATEGORY 2024-25

MAJOR BUDGET CATEGORIES - EXPENDITURES (\$13.1 million)



RESOLUTION NO. 1959-24

**RESOLUTION OF THE BOARD OF DIRECTORS OF
YUIMA MUNICIPAL WATER DISTRICT
AWARDING AUDIT SERVICES FOR
FISCAL YEARS 2023/24, 2024/25 AND 2025/26**

(Nigro & Nigro)

WHEREAS, the District is required to have its books, reports, records and financial procedures audited annually, and

WHEREAS, the District requested proposals for audit services for the three fiscal years ending 2024, 2025, 2026, and received proposals from one CPA firm, and

WHEREAS, each proposal was evaluated by the General Manager covering the following areas; general, scope, qualifications, personnel and proposed rates, with evaluation ratings assigned to each category, and

WHEREAS, after receiving and reviewing information with regard to the experienced firms capable of providing audit services, the committee has determined the independent firm of Nigro & Nigro, PC is qualified and experienced to provide the audit services as set out in the scope of services.

NOW, THEREFORE, BE IT RESOLVED by the Board of Directors of Yuima Municipal Water District hereby awards the Audit Services under a contract for fiscal years ending 2024, 2025, 2026.

PASSED AND ADOPTED at a regular meeting of the Board of Directors of YUIMA MUNICIPAL WATER DISTRICT held this 3rd day of June, 2024 by the following roll-call vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

Roland Simpson, President

Attest:

Don Broomell, Secretary

**TECHNICAL PROPOSAL
FOR
PROFESSIONAL AUDITING SERVICES
Yuima Municipal Water District**

**For the Fiscal Years Ending
June 30, 2024-2026
(with option for two subsequent years)**



Respectfully Submitted on April 29, 2024 by:

Paul J. Kaymark, CPA
Nigro & Nigro, PC
pkaymark@nncpas.com
Federal Tax ID: 30-0636241
Nncpas.com

Murrieta Office: 25220 Hancock Ave. #400, Murrieta, CA 92562 • P: (951) 698-8783 • F: (951) 699-1064
Walnut Creek: 2121 N. California Blvd. #290, Walnut Creek, CA 94596 • P: (844) 557-3111 • F: (844) 557-3444

Let's Work Together!



*By applying our financial expertise,
we partner with our clients to build
valuable relationships that inspire success.*

TABLE OF CONTENTS

Letter of Transmittal	1
License to Practice in California	3
Profile of the Firm	
Statement of Independence	3
Size of Our Firm	3
Size and Location of Offices	4
Range of Activities	4
Peer Review	5
Meet Your Audit Leadership Team	5
Resumés	6
Training & Resources	14
Similar Engagements with Other Water & Wastewater Districts	15
References	15
Scope of the Audit	16
Segmentation of Engagement	17
Proposed Schedule/Level of Staff & Number of Hours Assigned to Each Segment	17
Sample Size and the Extent to Which Statistical Sampling is to be Used	17
Type and Extent of Analytical Procedures to be Used	17
Approach to be Taken to Gain & Document an Understanding of Internal Control Structure	18
Approach to be Taken in Determining Laws & Regulations That Will be Subject to Audit Test Work	18
Approach to be Taken in Drawing Audit Samples	18
Use of Technology/Remote Proficiency	18
Proposing Firm Warranties	18
Additional Documents	
Proposer's Responder Forms	
Peer Review Letter	
Certificate of Insurance	



April 29, 2024

Ms. Amy Reeh, General Manager
Yuima Municipal Water District
PO Box 177
Pauma Valley, CA 92061-0177

Dear Ms. Reeh:

Thank you for the opportunity to submit this proposal to provide audit services for the Yuima Municipal Water District (District). Our understanding of the work to be done is: the annual audit of the District's financial statements and (ACFR) for the fiscal years ending June 30, 2024-2026, with an option to extend for two additional years. Based on our history with other water and wastewater districts, we believe our firm would be a great fit, and we would develop a great working relationship. Our staff works hard to help ensure our audits are completed with the highest level of service and meet all deadlines.

Currently, our current State Water Project clients are as follows:

Palmdale Water District, Littlerock Creek Irrigation District and San Geronio Pass Water Agency

Although many people think that all water and wastewater agencies function in the same manner, we know that's not the case. The audit leadership team we've assigned to your District, including myself, will take the time to learn the intricacies of your organization. We find that by delving deep into our client's structure and operations we are able to make recommendations that are not only useful, but also practical to implement.

At Nigro & Nigro, PC, our greatest strengths correspond to your most critical needs; we possess the full spectrum of resources needed to most effectively help the District's management team and Board members meet their goals – all at a very competitive rate. We believe we are your best choice.

- **Credibility, Reputation, and Resources of a Large Firm** without sacrificing the small-firm touch. Our CPAs and consultants can help you analyze and address financial, operational, and regulatory issues so you can focus attention on serving your citizens. We were originally formed in 1999, and now perform annual audits for approximately 100+ public agencies annually.
- **State-Wide Reach with Local Presence.** At Nigro & Nigro, we have the benefit of having the resources of a state-wide firm while serving you from our Murrieta (Headquarters) office. We also have an office in Walnut Creek for additional resources.
- **Efficiency.** Our use of portal software allows you to upload audit documentation at any time, which will minimize disruption to your staff and enable timely completion of all deliverables.

- **An Efficient and Effective Work Plan.** We currently serve over 100+ governmental entities statewide, which enables our staff to understand the scope of the audit. We also understand the District's complexities, not just from a compliance standpoint but also from an operational point of view. We have developed an effective work plan that takes into consideration your needs for high quality audit services, as well as timely deliverables. As a result of our efficient work plan, we commit to meeting your deadlines to complete our auditing services within the time-period you have specified.
- **Thought Leadership.** Members of our firm have been actively involved as presenters in numerous industry conferences and programs, including the GFOA, CSDA, and CSMFO. We have incorporated our experience with these committees into our audit framework.
- **Engagement Team.** We know that quality people drive quality results, which is why our commitment to you starts with the engagement team members who are selected based on their experience, focus on serving local government agencies, and who are the best fit for you. Each of the District's engagement team members have completed and exceeded the mandatory requirement for continuing professional education hours as requested in the RFP. Paul Kaymark, Partner, will be the main contact for the District regarding this project.
- **A Focus on Providing Consistent, Dependable Service to Government Entities.** Nigro & Nigro is organized by industry, affording our clients with industry-specific expertise supplemented by valuable local service and insight. Therefore, the District will enjoy the service of members of our Governmental Audit Services Team who have experience with similar governmental entities and understand the issues and environment critical to you. You will not have to train our auditors.

You may have many options in selecting a professional audit firm. By choosing Nigro & Nigro, you will gain value-added accounting and operational insights. We are the right fit for the District, as we have the expertise and depth of resources within our firm to offer you exceptional service while maintaining a sincere and honest relationship. We understand the work, we are committed to meeting your deadlines, and we would like the opportunity to continue to be your auditors. We also commit to meeting or exceeding your expectations.

Thank you once again for the opportunity to present our qualifications. If you have any questions about our offerings, please do not hesitate to contact me.

Sincerely,



Paul J. Kaymark, CPA
Audit Services Partner



LICENSE TO PRACTICE IN CALIFORNIA

The Firm and its entire CPA staff hold licenses to practice in the State of California. The Firm's CPA's are all members in good standing with the California Society of CPA's and the AICPA. We will assign a California licensed CPA as the auditor in charge of the audit.

PROFILE OF THE FIRM

Statement of Independence

Our standards require that we be without bias with respect to your operations. The Firm is independent of all entities listed in the RFP, as defined by auditing standards generally accepted in the United States of America and the U.S. General Accounting Office's "Governmental Auditing Standards". In addition, the Firm shall give the District written notice of any relevant professional relationships entered into during the period of this agreement.

Experience

Nigro & Nigro team members are highly trained in governmental accounting and auditing, which sets us apart as being able to add value beyond the basic attest engagement. We are comfortable working with clients of various sizes. Within the past five years, we have worked with numerous governmental clients with revenues ranging from \$200,000 to over \$300 million.

Prior to any audit engagement, our engagement team leader will meet with the Board, Audit Committee and Management to gain a full understanding of the philosophy, objectives and policies for operating the organization, as well as to discuss significant business, regulatory and accounting matters that will affect the audit. At the conclusion of the audit, we will communicate the results of the audit with the Board, Audit Committee and Management.

Areas of specialization include:

- Audit and Review Services
- Government Auditing Standards & Single Audits
- Annual Report of Financial Transactions
- Agreed Upon Procedures Engagements
- Annual Comprehensive Financial Report (ACFR) development

PROFILE OF THE FIRM (CONTINUED)

Size of Our Firm

Firm-wide, we have the following staffing for our governmental audit services:

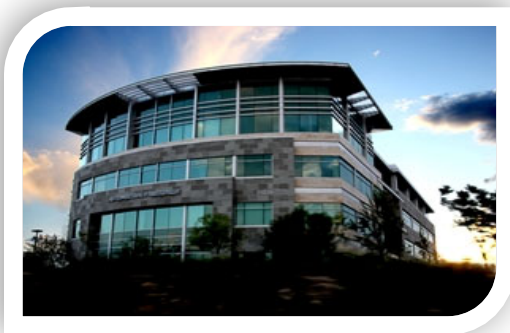
Position	Number of Employees	Number of Licensed CPA's
Partner*	7	7
Senior Manager	1	1
Manager	3	3
Supervisor	1	-
Senior	8	-
Associates	13	-
Support Staff	3	-
Total	36	11

**Although the term "partner" is used throughout this proposal to avoid confusion, the firm is organized as a Professional Corporation, and the firm's owners are "shareholders."*

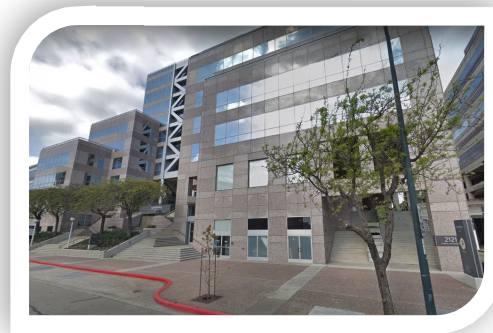
Size and Location of Offices

The firm was originally established in 1999. In 2013, we opened our second office in Northern California in order to better serve our growing client base of agencies in the San Francisco Bay Area. The Firm now has five partners and a professional staff of 18 accountants and expects to add more in the coming years as we continue to grow. We are a full service firm, providing audit and review, tax, consulting, and accounting services to local government, non-profit organizations, charter schools, commercial businesses and homeowners' associations. The office serves clients of all sizes and industries, however, we focus on government agencies, just like yours.

We are prepared to do what it takes to provide the extra level of service required to maintain a long-term business relationship.



MURRIETA OFFICE



WALNUT CREEK OFFICE

Range of Activities Performed

- Consulting and other services for numerous other agencies and not-for-profits
- Tax services for individuals, corporations, and non-profit organizations

PROFILE OF THE FIRM (CONTINUED)

Peer Review

Our firm's most recently issued peer review report can be found under the "Additional Documents" section of the proposal. A firm can receive a "Fail", "Pass with Deficiencies", or a "Pass" rating. The firm's most recent peer review report rating was a Pass. This rating indicates that the firm's system of quality control has been suitably designed and complied with to provide the audit organization with reasonable assurance of performing and reporting in conformity with professional standards and applicable legal and regulatory requirements in all material respects. As required by our membership in the Government Audit Quality Center (GAQC), the peer review included a selection of a sample of governmental audit engagements.

Meet Your Audit Leadership Team

Listed on the following pages are the resumes of the management team that will be assigned to your audit. As mentioned previously, our staff members have considerable governmental audit experience. This gives us a pool to draw on in addition to the group listed.

Name	Role	Years of Experience in Audits
Paul J. Kaymark, CPA	Lead Partner	30
Peter Glenn, CPA	Review Partner	17
Jared Solmons, CPA	Audit Senior Manager	6
Stacy Macias, CPA	Audit Manager – Federal Compliance	6
Anabel Cruz, CPA	Audit Manager	5
Tyler Cook	Audit Supervisor	2
Angelina Paunkov	Audit Senior	1

Paul J. Kaymark, CPA

Lead Audit Partner

Paul joined the firm in 2019 and has more than 30 years of public accounting and auditing governmental entities experience. Paul is our choice for new governmental audit clients, having extensive experience in the areas of governmental entities. His main responsibilities include assistance in the preliminary planning of audit work, review of assistants' work, and performing audit procedures in more complex audit areas.

Audit Services:

Mr. Kaymark has been working on audit engagements of governmental agencies, not-for-profit organizations, as well as for-profit corporations and companies. His previous experience includes audit and consulting work for large and small businesses with a focus on client service. Paul strives to build strong relationships with his clients by assisting them with any emerging issues and being available as a resource.

Consulting Services:

Mr. Kaymark has experience in a variety of governmental issues, garnered from his auditing experience over the years. He regularly consults with clients in areas of:

Special District Accounting:

- Internal controls
- Financial reporting
- Annual report of financial transactions

Financial Reporting:

- Year-end closing procedures
- Cash flows
- Budget development and projections
- Multi-Year projections
- Pension and OPEB accounting

Some Agencies Served:

- Metropolitan Water District of So Cal
- Palmdale Water District
- Oxnard Harbor District
- Western Municipal Water District
- El Toro Water District
- East Orange County Water District
- Trabuco Canyon Water District



California Special Districts Association
Districts Stronger Together

CSDA Workshop Speaker



Education:

Bachelor of Science, Business Administration, Accountancy
California State University, Long Beach
1994

Licenses and Certifications:

- Certified Public Accountant, California
- GFOA Certificate for Excellence in Financial Reporting - Reviewer

Professional Affiliations:

- Government Finance Officers Association (GFOA)
- California Society of Municipal Finance Officers (CSMFO)
- California Special District Association (CSDA)

Continuing Education:

Various municipal accounting courses offered by the AICPA, CalCPA Education Foundation including:

- Governmental and Nonprofit Annual Update
- GASB Basic Financial Statements for State and Local Governments
- Single Audits: Uniform Grant Guidance (formerly OMB Circular A-133)
- Financial Accounting Standards Board Annual Updates



Water and Wastewater Clients Audited and/or Consulted With Over My Career

Water and Wastewater

Metropolitan Water District of Southern California
Los Angeles County Sanitation District
Long Beach Water Department
Glendale Water and Power
Colton Public Utilities
Baldy Mesa Water District
Bear Valley Community Services District
Beaumont-Cherry Valley Water District
Big Bear City Community Services District
Cabazon Water District
California Domestic Water Company
Casitas Municipal Water District
Castaic Lake Water Agency
Chino Basin Water Conservation District
Chino Basin Watermaster
Coachella Valley Water District
Diablo Water District
East Orange County Water District
El Toro Water District
Farm Mutual Water Company
Golden Hills Community Services District
Goleta Water District
Hi-Desert Water District
Inverness Public Utilities District
Irvine Ranch Water District
Joshua Basin Water District
Jurupa Community Services District
Leucadia Wastewater District
Mesa Consolidated Water District
Mojave Water Agency
Monte Vista Water District
Montecito Water District
North Coast County Water District
North Marin Water District
Novato Sanitary District
Palmdale Water District

Water and Wastewater, continued

Phelan Pinon Hills Community Services District
Pomona Valley Protective Agency
Purissima Hills Water District
Rincon del Diablo Water District
Rosamond Community Services District
Rossmoor Los Alamitos Area Sewer District
Sacramento Suburban Water District
San Bernardino Valley Water Conservation District
San Gabriel Valley Municipal Water District
San Lorenzo Valley Water District
Santa Ana Watershed Project Authority
Santa Margarita Water District
Saticoy Sanitary District
Solano County Water Agency
Soquel Creek Water District
Stallion Springs Community Services District
Summerland Sanitary District
Trabuco Canyon Water District
Tres Pinos Water District
Triunfo Sanitation District
Twentynine Palms Water District
Vallecitos Water District
Valley County Water District
Ventura Regional Sanitation District
Victor Valley Water District
Victor Valley Wastewater Reclamation Authority
Victorville Water District
Water Facilities Authority - Joint Power Agency
Water Replenishment District
West County Agency
West County Wastewater District
West Valley Water District
Westborough Water District
Western Municipal Water District
Western Riverside County Regional Wastewater
Yorba Linda Water District

Peter Glenn, CPA

Review Partner

Peter joined the firm in 2011 after nearly three years of previous public accounting and auditing experience. Peter will work under the general direction of the partner. Peter is our choice for new governmental audit clients, having successfully worked on each of the Firm's clients since beginning with the Firm. His main responsibilities include assistance in the preliminary planning of audit work, review of assistants' work, and performing audit procedures in more complex audit areas.

Audit Services:

Peter Glenn began his auditing career with Nigro & Nigro in 2011, participating in audits of special districts, LEAs, other governmental audits, and agreed-upon procedure engagements. Prior to joining the firm, he worked for three years at another public accounting firm, developing his auditing skills. He has previously been the in-charge accountant for some of the firm's largest clients.

Consulting Services:

Mr. Glenn has experience in a variety of governmental accounting issues, derived from his auditing experience at the firm. He regularly consults with clients in areas of:

Special District Accounting:

- Internal controls
- Financial reporting & GASB 34
- Annual report of financial transactions

Financial Reporting:

- Uniform Guidance
- Performance Audits
- Year-end closing procedures
- Cash flows
- Budget development and projections
- Multi-Year projections

Other Agencies Served:

- Calleguas Municipal Water District
- Costa Mesa Sanitary District
- East Orange County Water District
- Hi-Desert Water District
- Oxnard Harbor District
- Montecito Water District
- North Coast County Water District
- Palmdale Water District
- San Geronio Pass Water Agency



Education:

Bachelor of Science, Business Administration, Accounting
California State University,
San Marcos, 2008, Magna Cum Laude

Licenses and Certifications:

- Certified Public Accountant, California

Continuing Education:

- CASBO Annual Conference
- SSC Finance & Management Conferences
- Government Accounting & Auditing Conference
- In-house training for audit staff (presenter)



Jared Solmosen, CPA

Audit Senior Manager

After completing his degree, Jared went to work for a midsize construction company where he worked as an estimator and project manager before transitioning into more of an accounting and finance role. It was working in this role that led him to the decision to pursue the goal of becoming a Certified Public Accountant. He continues to hone his skills and expand his knowledge as he branches out into different areas of accounting services and working with various governmental agencies and not-for-profit organizations. Jared will work with the audit partner and oversee staff as they work together through different audit areas.

Audit Services:

Jared began his career with Nigro & Nigro in 2019 focusing on special districts and not-for-profit organizations. He has a customer-oriented approach to auditing, striving to build strong relationships by working with clients to help them navigate the ever-changing world of accounting rules and standards.

Consulting Services:

Jared has experience with a variety of governmental and not-for-profit accounting issues, as well as other tax and audit concerns, derived from his audit and consulting experience at the firm.

Special District Accounting:

- Internal control policies, procedures, and best practices
- Year-end closing procedures
- Capital asset and depreciation schedule

Financial Reporting:

- Federal and state compliance
- Single audits
- Revenue and expense tracking by program/grant
- Statement of functional expense
- Compiling financial statements
- Disclosure requirements
- GASB 68 Pensions
- GASB 75 OPEB
- GASB 87 Leases
- GASB 96 SBIA's

Other Agencies Served:

- Calleguas Municipal Water District
- Costa Mesa Sanitary District
- East Orange County Water District
- Hi-Desert Water District
- Oxnard Harbor District
- Montecito Water District
- North Coast County Water District
- Palmdale Water District
- San Geronio Pass Water Agency



Education:

Bachelor of Science, Business Administration, Finance
California State University,
San Marcos, 2013

Licenses and Certifications:

- Certified Public Accountant, California

Continuing Education:

- Government Accounting & Auditing Conference
- Not-For-Profit Organizations Conference
- In-house training for audit staff
- Spidell Tax Seminar
- Western CPE Tax update webinars
- In-house training for audit staff (presenter)

Additional Areas:

- Tax preparation
- QuickBooks knowledge

Stacy Macias, CPA

Audit Manager – Federal Compliance

Stacy joined the firm in 2018 as a staff accountant after completing her degree at California State University, Chico and has worked her way up to Audit Manager. Stacy continues to expand her knowledge as she branches out into different areas of accounting services and working with varying governmental and not-for profit clients. Stacy will work under the general direction of the audit partner and oversee staff as they work together through different audit areas.

Audit Services:

Stacy began her auditing career on audit engagements of governmental agencies, and non-for-profit organizations. Stacy enjoys auditing governmental agencies and non-for-profit due to their varying structures and sizes. Stacy truly values customer service and building client relationships. Her friendly demeanor makes clients comfortable in reaching out to her during the audit process or throughout the year.

Consulting Services:

Stacy has experience in a variety of governmental and not-for-profit accounting, tax, and audit concerns, derived from her audit and consulting experience with those industries.

Financial Reporting:

- Year-end closing procedures
- Internal control policies and procedures and best practices
- Compiling Financial Statements
- Revenue and Expense tracking by program/grant
- Statement of Functional Expenses
- Capital assets and depreciation schedules
- Disclosure requirements
- Federal and State compliance
- GASB 68 Pensions
- GASB 75 OPEB
- GASB 87 Leases
- GASB 96 SBIA's

Additional Areas:

- Tax preparation
- QuickBooks knowledge

Other Agencies Served:

- Calleguas Municipal Water District
- Costa Mesa Sanitary District
- East Orange County Water District
- Hi-Desert Water District
- Oxnard Harbor District
- Montecito Water District
- North Coast County Water District
- Palmdale Water District
- San Geronio Pass Water Agency



Education:

Bachelor of Science, Business Administration, Accounting
California State University,
Chico, 2018

Licenses and Certifications:

- Certified Public Accountant, California

Continuing Education:

- Government Accounting & Auditing Conference
- Not-For-Profit Organizations Conference
- In-house training for audit staff
- Spidell Tax Seminar
- Western CPE Tax update webinars
- In-house training for audit staff (presenter)

Anabel Cruz, CPA

Audit Manager

Anabel began her career in public accounting in 2019 with Nigro & Nigro, PC. Previous to joining the firm, she worked as an Accountant at private sector companies. Her audit experience includes audits of governmental and not-for-profit organizations, Anabel values building quality relationships with clients while providing timely and reliable services. Anabel will work under the general direction of the audit partner and oversee staff as they work together through different audit areas.

Audit Services:

Anabel enjoys auditing governmental agencies and non-for-profits due to their varying structures and sizes.

Consulting Services:

Anabel has experience in a variety of governmental and not-for-profit accounting and audit concerns, derived from her audit and consulting experience with those industries.

Financial Reporting:

- Year-end closing procedures
- Agreed upon procedures
- Internal control policies and procedures and best practices
- Capital assets and depreciation schedules
- GASB 68 Pensions
- GASB 75 OPEB
- GASB 87 Leases
- GASB 96 SBIA's

Other Agencies Served:

- Calleguas Municipal Water District
- Costa Mesa Sanitary District
- East Orange County Water District
- Hi-Desert Water District
- Oxnard Harbor District
- Montecito Water District
- North Coast County Water District
- Palmdale Water District
- San Geronio Pass Water Agency



Education:

Bachelor of Science, Finance and Accountancy
California State University, Northridge,
2014

Licenses and Certifications:

- Certified Public Accountant, California

Continuing Education:

- Government Accounting & Auditing Conference
- Not-For-Profit Organizations Conference
- In-house training for audit staff
- Spidell Tax Seminar
- Western CPE Tax update webinars
- In-house training for audit staff (presenter)

Tyler Cook

Audit Supervisor

Tyler began his career in public accounting in 2022 with Nigro & Nigro, PC. Tyler's audit experience includes audits of governmental and not-for-profit organizations such as cemeteries, resource conservation districts, water districts, fire protection districts and community service districts. Tyler values building quality relationships with clients while providing timely and reliable services. Tyler is working under the general direction of the Audit Manager.

Audit Services:

Tyler enjoys auditing governmental agencies and non-for-profits due to their varying structures and sizes.

Consulting Services:

Tyler has experience in a variety of governmental and not-for-profit accounting and audit concerns, derived from his audit and consulting experience with those industries.

Financial Reporting:

- Year-end closing procedures
- Agreed upon procedures
- Internal control policies and procedures and best practices
- Capital assets and depreciation schedules
- GASB 68 Pensions
- GASB 75 OPEB
- GASB 87 Leases
- GASB 96 SBIA's

Other Agencies Served:

- Calleguas Municipal Water District
- Costa Mesa Sanitary District
- East Orange County Water District
- Hi-Desert Water District
- Oxnard Harbor District
- Montecito Water District
- North Coast County Water District
- Palmdale Water District
- San Geronio Pass Water Agency



Education:

Bachelor of Science, Accountancy
BYU Hawaii – 2022
Master's in Accountancy
San Diego State University – 2023

Licenses and Certifications:

- CPA License Candidate

Continuing Education:

- Government Accounting & Auditing Conference
- Not-For-Profit Organizations Conference
- In-house training for audit staff

Angelina Paunkov

Audit Senior

Angelina began her career in public accounting in 2023 with Nigro & Nigro, PC. Angelina's audit experience includes audits of governmental and not-for-profit organizations such as cemeteries, resource conservation districts, water districts, fire protection districts and community service districts. Angelina values building quality relationships with clients while providing timely and reliable services. Angelina is working under the general direction of the Audit Supervisor.

Audit Services:

Angelina enjoys auditing governmental agencies and non-for-profits due to their varying structures and sizes.

Consulting Services:

Angelina has experience in a variety of governmental and not-for-profit accounting and audit concerns, derived from her audit and consulting experience with those industries.

Financial Reporting:

- Year-end closing procedures
- Agreed upon procedures
- Internal control policies and procedures and best practices
- Capital assets and depreciation schedules
- GASB 68 Pensions
- GASB 75 OPEB
- GASB 87 Leases
- GASB 96 SBIA's

Other Agencies Served:

- Calleguas Municipal Water District
- Costa Mesa Sanitary District
- East Orange County Water District
- Hi-Desert Water District
- Oxnard Harbor District
- Montecito Water District
- North Coast County Water District
- Palmdale Water District
- San Geronio Pass Water Agency



Education:

Bachelor of Science, Accountancy
California State University, San Marcos,
2023

Licenses and Certifications:

- Certified Public Accountant, California

Continuing Education:

- Government Accounting & Auditing Conference
- Not-For-Profit Organizations Conference
- In-house training for audit staff

PROFILE OF THE FIRM (CONTINUED)


Training & Resources

The Firm is committed to a continuing professional education program, which emphasizes the areas of expertise of each member of our professional staff. The Firm is required to comply with the *Government Auditing Standards* for each professional practicing in the area of governmental accounting and auditing. We are committed to follow those standards, which result in quality audit services, including continuing education for all staff of 60-80 hours each year, specifically in school districts and governmental auditing. As required by *Government Auditing Standards*, all governmental audit staff receives the required continuing education in the area of governmental auditing and accounting. These policies are monitored internally, reviewed annually and certified periodically by independent peer review.

Library facilities are maintained which include current professional literature and specific information for the industries that we serve. The Firm library is also reviewed as part of the external quality review program. The Firm has in-house training programs specific to our school district clients. We also perform auditing and accounting updates for our clients that are organized by our staff. These practices ensure the quality of our staff over the term of the engagement.

Our staff participates in activities relating to government accounting and reporting issues through our membership and involvement with the following organizations:

- a. American Institute of CPA's Governmental Audit Quality Center
- b. California Society of CPAs
- c. Government Finance Officers Association (GFOA)
- d. California Special Districts Association (CSDA)
- e. Government Accounting Standards Board (GASB)
- f. Association of Certified Fraud Examiners (ACFE)



We recognize that our most important product is prompt and effective service.

Through our participation in these organizations and continuing education provided by them, the Firm continues to stay abreast of all current governmental accounting and reporting issues. Some of the professional education our audit team members have either presented at or attended in the last two years include:

- SSC Annual Finance and Management Conference
- SSC Governor's Budget Workshop
- CSDA Annual Conference
- CSMFO Conference
- GFOA Annual Conference
- Various other governmental workshops

We recognize that our most important product is prompt and effective service. We believe the District should work with its CPA firm throughout the entire year. We are available at any time throughout the year to provide any assistance you may need.

PROFILE OF THE FIRM (CONTINUED)

Similar Engagements with Other Water and Wastewater Districts

We currently conduct over 100+ government audits each year and have well rounded experience with local governmental agencies. We are excited for the opportunity to devote our attention to you and your specific needs. Below is a partial list of some similar governmental clients we are currently auditing.

Please contact our clients for a Reference of our services!

Let's start with our State Water Contractor clients:

Palmdale Water District - Dennis Hoffmeyer, CFO (661) 456-1021

Littlerock Creek Irrigation District - Gina Burroughs, OM (661) 944-2015

San Gorgonio Pass Water Agency - Thomas Todd, CFO (951) 845-2577

Here is a Local Client to the District's Location:

Grossmont Healthcare District - Tom Scaglione, CFO, (619) 825-5034

ACFR Preparation Clients:

Costa Mesa Sanitary District - Kaitlin Tran, FM (949) 645-8400

Hi-Desert Water District - Tanya Gruwell, CFO (760) 228-6271

Las Gallinas Valley Sanitary District - Dale McDonald, ASM (415) 526-1519

Scotts Valley Water District - Nicolas Kuns, FM (831) 600-1904

Trabuco Canyon Water District - Michael Perea, AGM (949) 858-0277

Other Water District Clients:

Calleguas Municipal Water District - Dan Smith, MAS - (805) 579-7132

Montecito Water District - Olivia Rojas, BM (805) 969-2271

Rowland Water District - Myra Malner, DF (562) 697-1726

*** Please check the websites of these above noted clients to review the Financials prepared by our Firm.**

SCOPE OF THE AUDIT

We will audit the basic financial statements of the District for the fiscal year ended June 30, 2023-2025 in accordance with the following standards:

- Auditing Standards Generally Accepted in the United States of America
- *Government Auditing Standards*, issued by the Comptroller General of the United States
- Minimum Audit Requirements and Reporting Guidelines for Special Districts

Our audit will be for the purpose of expressing an opinion on the basic financial statements, and will include such auditing procedures as considered necessary to accomplish this purpose. We will also provide an "in-relation-to" opinion on any other supplemental information and statistical schedules. We anticipate issuing the following reports:

- Independent Auditors' Report on the basic financial statements.
- Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*.

In addition, we will provide the District with a management letter that will give written appraisals of its accounting and related systems. This letter will identify any control deficiencies, significant control deficiencies or material weaknesses that are identified during the audit. We will work with management before audit fieldwork and during the course of the audit to assess internal controls and review mitigating controls in place in an effort to reduce the control deficiencies, significant control deficiencies and material weaknesses that need to be reported to management in writing, assuming there are mitigating controls in place. The letter will also offer recommendations for the elimination of weaknesses that we identify, and we will suggest any methods we discover to help improve efficiency and effectiveness.

We will schedule an appearance with the Board and the Audit Committee that allows an opportunity for us to present the audit and management letter. This is an excellent time for the District to resolve any questions it has regarding our audit or management letter. As mentioned earlier, the value in hiring our Firm comes from not only the audit, but from our experience and the education, we can provide. We hope that as questions or concerns arise throughout the year, the District staff will contact us and draw on our knowledge and experience.

Non-significant deficiencies discovered during the audit process shall be reported in a separate letter to management, the Board and the Audit Committee, which shall be referred to in the report(s) on internal controls. This separate letter also informs the Board and the Audit Committee of the following:

- 1) The auditor's responsibility under auditing standards generally accepted in the United States of America.
- 2) Significant accounting policies.
- 3) Management judgments and accounting estimates.
- 4) Significant audit adjustments.
- 5) Other information in documents containing audited financial statements.
- 6) Disagreements with management.
- 7) Management consultation with other accountants.
- 8) Major issues discussed with management prior to retention.
- 9) Difficulties encountered in performing the audit.

All working papers and reports will be retained at the Firm's expense for a minimum of seven (7) years, unless the Firm is notified in writing by the District of the need to extend the retention period.

SCOPE OF THE AUDIT(CONTINUED)

Segmentation of Engagement

STEP 1: Planning

Our goal in preliminary fieldwork is to gain a thorough understanding of your internal controls, processes and procedures. Our goal is to accomplish as much interim fieldwork as possible so that our stay during final fieldwork is kept to a minimum. Our preliminary work focuses on planning and internal control documentation.

STEP 2: Interim Field Work

Internal Control Documentation

Our internal control documentation usually occurs during interim fieldwork. Our documentation process will be as follows:

- 1) Gather or update documentation for significant processes defined in our preliminary fieldwork.
- 2) Perform a "walk-through" of these significant processes.
- 3) Ask "what can go wrong" questions.
- 4) Identify controls in place. This will include both preventative and detective controls.
- 5) Evaluate the design of internal controls.
- 6) Decide whether to test and rely on controls.
- 7) Summarize preliminary fieldwork and submit management letter of all areas of concern.

STEP 3: Final Fieldwork

We assess risks, design procedures and obtain evidence to support financial statement amounts and disclosures during final fieldwork. Our Firm utilizes a methodology designed specifically for special districts. Our process emphasizes continuous communication with our staff.

Assess Risks and Design Procedures

As outlined in the risk based statements of audit standards (SAS 104 to 111), our Firm uses a risk-based approach to the audit. Our procedures to assess risks and design procedures are as follows:

- 1) Assess risk of material misstatement from errors or fraud based on internal controls combined with inherent risk of significant accounts.
- 2) Design procedures to test controls if considered necessary.
- 3) Design procedures to test details of account balances and classes of transactions based on risk.

Interim and Year End Testing

- 1) Perform tests of controls if considered necessary.
- 2) Perform tests of details of account balances and classes of transactions.
- 3) Evaluate quality and sufficiency of audit evidence.
- 4) Evaluate misstatements.

STEP 4: Audit Completion

Preparation of Audit Report and Management Letter

After reviewing the financial statements, notes and required supplementary schedules, we will agree the data to our working papers and provide a thorough review of all information by using written Firm standards and checklists. We will also review and incorporate any statistical data. This will verify appropriate presentation and disclosure. We will also at this time prepare our management letter that identifies financial trends and recommendations for improvement, reports required communications to the governing board, and discusses change in the environment in which the District operates.

SCOPE OF THE AUDIT (CONTINUED)

Proposed Schedule/Level of Staff & Number of Hours Assigned to Each Segment

We will provide a detailed audit plan and prepare a list of schedules upon proposal acceptance. The following table summarizes our proposed segmentation of the engagement by date, segment, and level of staff as we have estimated based on the RFP timeline:

Date/Segment	Total Hours			Total
	Partner/Manager	Supervisor	Staff/Admin	
April				
Preliminary planning and fieldwork	8	8	10	26
May/July				
Interim fieldwork	12	12	26	50
Oct/Nov				
Final fieldwork, report preparation, review, finalization, and presentation	24	16	34	74
Total hours	44	36	70	150
	44	36	70	
	8	8	10	26
Preliminary planning and fieldwork	12	12	26	50
Control	12	8	34	54
Substantive	12	8	0	20
Reporting	44	36	70	150

Sample Size and the Extent to Which Statistical Sampling is to be Used

We perform sampling techniques and determine sample size after assessing the risk associated with specific transaction classes. No single “cookie-cutter” approach will be followed in regards to sampling techniques, but the District can be assured that an appropriate sampling methodology will be utilized. We use the following methods of sampling during our audits: statistical, haphazard, and judgmental. For statistical sampling we use guidance provided by the AICPA and by federal guidelines in accordance with industry standards, which typically recommends sample sizes between 40 to 60 items.

Type and Extent of Analytical Procedures to be Used

We will perform analytical procedures throughout the course of our audit. Professional standards require that analytical procedures be performed in the planning and wrap-up stages of the audit. Analytical review will be used during our expenditure, revenue, budget information as well as many other areas.

These procedures typically entail a review of interim reports, budgets, and comparisons to prior year data. We also use financial statement amounts to calculate certain ratios to determine whether any unusual or unexpected relationships exist in the financial data.

These procedures are then followed by inquiry of key District personnel to corroborate the auditors' expectations based on the data.

SPECIFIC AUDIT APPROACH (CONTINUED)

Approach to be Taken to Gain and Document an Understanding of Internal Control Structure(s)

Our audit approach will entail interviews with key personnel in the District involved in the design and implementation of internal controls. In conjunction with the interviews, we will perform tests and observations of how well the controls function. Key areas of internal control generally include: cash receiving, accounts payable/purchasing, payroll/personnel, technology, facilities, and maintenance and operations.

Approach to be Taken in Determining Laws and Regulations That Will be Subject to Audit Test Work

We are required to obtain an understanding of the possible financial statement effect of laws and regulations that have a direct and material effect on the determination of financial statement amounts. The determination of laws and regulations is addressed in the planning stage through reading available grant documentation, inquiry of the client, a preliminary review of finance system accounts and search of the Board minutes. We also have working knowledge of the types of laws and regulations under which California special districts operate. We also obtain further information about federal laws and regulations through the Catalog of Federal Domestic Assistance (CFDA) and the Uniform Guidance.

Approach to be Taken in Drawing Audit Samples

Since each program or grant agreement is different, we use many different approaches to sampling in our tests of compliance. The size of the sample considers many factors; size and risk of the program, program maturity, complexity, level of oversight and prior audit findings. AICPA Guidelines generally recommend sample sizes of 25, 40, or 60 items when the population is greater than 250. Ultimately, our professional judgment determines that a representative number of transactions have been selected. You can be confident in our judgment because our peer reviews and an outside review by the U.S. Department of Education have all accepted our audit sampling techniques and procedures.

Use of Technology/Remote Proficiency

In order to facilitate the exchange of data between us and our clients in a secured manner throughout the course of the audit, we employ the use of an online secured portal. Our clients have appreciated this unique and forward-thinking platform which helps minimize duplicate requests and unnecessary email and phone exchanges to request and receive audit documentation. The software is very user-friendly and easy to understand. This also allows us to perform much of the audit remotely without being onsite to reduce our carbon footprint.

Proposing Firm Warranties

1. The firm is willing and able to obtain an Errors and Omissions Insurance Policy providing a prudent amount of coverage for the willful or negligent acts or omissions of any officers, employees, or agents thereof.
2. The firm will not delegate or subcontract its responsibilities under an agreement without the express prior written permission of the District.
3. All information provided by the firm in connection with this proposal is true and correct.
4. The firm will acknowledge and agree with all terms and conditions stated in this Request for Proposal.



Paul J. Kaymark, CPA
Audit Services Partner

**COST PROPOSAL
FOR
PROFESSIONAL AUDITING SERVICES
Yuima Municipal Water District**

**For the Fiscal Years Ending
June 30, 2024-2026
(with option for two subsequent years)**



Respectfully Submitted on April 29, 2024 by:

Paul J. Kaymark, CPA

Nigro & Nigro, PC

pkaymark@nncpas.com

Federal Tax ID: 30-0636241

Nncpas.com

Murrieta Office: 25220 Hancock Ave. #400, Murrieta, CA 92562 • P: (951) 698-8783 • F: (951) 699-1064
Walnut Creek: 2121 N. California Blvd. #290, Walnut Creek, CA 94596 • P: (844) 557-3111 • F: (844) 557-3444

COST PROPOSAL

Proposed Pricing Per Professional Staff Member

Professional	Hours	Rates		Total	
		Standard	Quoted		
Partner	16.00	\$ 200.00	\$ 175.00	\$ 2,800.00	
Managers	28.00	175.00	150.00	4,200.00	
Seniors	36.00	150.00	125.00	4,500.00	
Staff Members	70.00	125.00	100.00	7,000.00	
Admin	-	100.00	75.00	-	
Subtotal	150.00			18,500.00	
Out-of-Pocket - Included in Rates				-	
Total Max				\$ 18,500.00	

Fiscal Year	FY 2024	FY 2025	FY 2026	Total
District Financials	\$ 18,000	\$ 18,000	\$ 18,000	\$ 54,000
State Controller's Report	500	500	500	1,500
Total	\$ 18,500	\$ 18,500	\$ 18,500	\$ 55,500

Same Price for FY 2027 to FY 2028

Single-Audit of Federal Funding \$5,000

ADDITIONAL INFORMATION

Testimonial

"Few people have the opportunity to work with someone who was a coach and a mentor-but I did when I worked with Paul. I had the pleasure working directly under Paul's supervision and I was particularly impressed by his ability to handle even the toughest clients - and effortlessly. That skill often takes years to develop, but it seemed to come perfectly natural to him. Paul was one of those rare partners who also naturally serve as an inspiring mentor for the whole staff and I was grateful to learn a lot from him."

*Deana Miller
Accounting Manager
PolyCera, Inc.*

Fraud Hotline



Throughout the audit process, we will make available our fraud hotline reporting service at no additional charge over the period of the contract to ensure the District has an effective anti-fraud program.




ADDITIONAL DOCUMENTS

Yuima Municipal Water District
Request for Proposal
Page Seven

The proposing firm warrants the following:

1. The firm is willing and able to obtain an Errors and Omissions Insurance Policy providing a prudent amount of coverage for the willful or negligent acts or omissions of any officers, employees, or agents thereof
2. The firm will not delegate or subcontract its responsibilities under an agreement without the express prior written permission of the District
3. All information provided by the firm in connection with this proposal is true and correct
4. The firm will acknowledge and agree with all terms and conditions stated in this request for proposal.



Signature/Proposing Firm

April 29, 2024

Date



Report on the Firm's System of Quality Control

To Nigro & Nigro, PC
and the Peer Review Committee of the California Society of CPAs

We have reviewed the system of quality control for the accounting and auditing practice of Nigro & Nigro, PC (the firm) in effect for the year ended August 31, 2020. Our peer review was conducted in accordance with the Standards for Performing and Reporting on Peer Reviews established by the Peer Review Board of the American Institute of Certified Public Accountants (Standards).

A summary of the nature, objectives, scope, limitations of, and the procedures performed in a System Review as described in the Standards may be found at www.aicpa.org/prsummary. The summary also includes an explanation of how engagements identified as not performed or reported in conformity with applicable professional standards, if any, are evaluated by a peer reviewer to determine a peer review rating.

Firm's Responsibility

The firm is responsible for designing a system of quality control and complying with it to provide the firm with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The firm is also responsible for evaluating actions to promptly remediate engagements deemed as not performed or reported in conformity with professional standards, when appropriate, and for remediating weaknesses in its system of quality control, if any.

Peer Reviewer's Responsibility

Our responsibility is to express an opinion on the design of the system of quality control and the firm's compliance therewith based on our review.

Required Selections and Considerations

Engagements selected for review included engagements performed under *Government Auditing Standards*, including compliance audits under the Single Audit Act.

As a part of our peer review, we considered reviews by regulatory entities as communicated by the firm, if applicable, in determining the nature and extent of our procedures.

Opinion

In our opinion, the system of quality control for the accounting and auditing practice of Nigro & Nigro, PC in effect for the year ended August 31, 2020, has been suitably designed and complied with to provide the firm with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Firms can receive a rating of *pass*, *pass with deficiency (ies)*, or *fail*. Nigro & Nigro, PC has received a peer review rating of *pass*.

June 11, 2021



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

8/1/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER RANCHO CAL INSURANCE SERVICES 29930 Hunter Rd Ste 106 Murrieta, CA 92563	CONTACT NAME: James Mitchell PHONE (A/C, No, Ext): (951)260-0190 E-MAIL ADDRESS: jim@ranchoins.com	FAX (A/C, No): (951)260-0189
	INSURER(S) AFFORDING COVERAGE	
INSURED Nigro & Nigro, PC PO Box 1247 Murrieta, CA 92564	INSURER A: Ohio Security Insurance Company	NAIC # 24082
	INSURER B: Amarian Fire and Casualty Company	24066
	INSURER C: Sequoia Insurance Company	22985
	INSURER D: Swiss Re Corporate Solutions	29874
	INSURER E:	
	INSURER F:	

COVERAGES**CERTIFICATE NUMBER:****REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:	X	X	BZS64971750	8/15/2023	8/15/2024	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 500,000 MED EXP (Any one person) \$ 15,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000
A	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY	X	X	BAS64971750	8/15/2023	8/15/2024	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
B	<input checked="" type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> EXCESS LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> CLAIMS-MADE DED RETENTION \$			ESA64971750	8/15/2023	8/15/2024	EACH OCCURRENCE \$ 3,000,000 AGGREGATE \$ 3,000,000
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A	QWC1302193	8/15/2023	8/15/2024	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
D	Cyber Insurance			C-4MQ8-065674-CYBER-2023	8/24/2023	8/24/2024	\$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER**CANCELLATION**

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

© 1988-2015 ACORD CORPORATION. All rights reserved.



June 3, 2024

Board of Directors and Ms. Amy Reeh, General Manager
Yuima Municipal Water District
PO Box 177
Pauma Valley, CA 92061

We are pleased to confirm our understanding of the services we are to provide Yuima Municipal Water District (District) as of and for the year ended June 30, 2024.

Audit Scope and Objectives

We will audit the business-type activities and each major fund of the District, as of June 30, 2024 and for the year then ended and the related notes, which collectively comprise the District's basic financial statements as listed in the table of contents of the financial statements.

The objectives of our audit are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with auditing standards generally accepted in the United States of America (GAAS) and, if applicable, in accordance with *Government Auditing Standards*, and/or any state or regulatory audit requirements will always detect a material misstatement when it exists.

Misstatements, including omissions, can arise from fraud or error and are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

Accounting principles generally accepted in the United States of America, (U.S. GAAP,) as promulgated by the Governmental Accounting Standards Board (GASB) require that certain required supplementary information (RSI) such as management's discussion and analysis be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the GASB, who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context.

As part of our engagement, we will apply certain limited procedures to the required supplementary information (RSI) in accordance with auditing standards generally accepted in the United States of America, (U.S. GAAS). These limited procedures will consist primarily of inquiries of management regarding their methods of measurement and presentation, and comparing the information for consistency with management's responses to our inquiries. We will not express an opinion or provide any form of assurance on the RSI. The following RSI is required by U.S. GAAP. This RSI will be subjected to certain limited procedures but will not be audited:

1. Management's Discussion and Analysis
2. Schedule of Proportionate Share of the Net Pension Liability
3. Schedule of Pension Contributions
4. Schedule of Changes in the Net OPEB Liability and Related Ratios
5. Schedule of OPEB Contributions

The following other information accompanying the financial statements will not be subjected to the auditing procedures applied in our audit of the financial statements, and our auditor's report will not provide an opinion or any assurance on that other information.

1. Introductory Section
2. Statistical Section

We will also provide a report (that does not include an opinion) on internal control related to the financial statements and compliance with the provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the financial statements as required by *Government Auditing Standards*. The report on internal control and on compliance and other matters will include a paragraph that states (1) that the purpose of the report is solely to describe the scope of testing of internal control and compliance, and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control on compliance, and (2) that the report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the entity's internal control and compliance. The paragraph will also state that the report is not suitable for any other purpose. If during our audit we become aware that the District is subject to an audit requirement that is not encompassed in the terms of this engagement, we will communicate to management and those charged with governance that an audit in accordance with U.S. generally accepted auditing standards and the standards for financial audits contained in *Government Auditing Standards* may not satisfy the relevant legal, regulatory, or contractual requirements.

Auditor Responsibilities

We will conduct our audit in accordance with GAAS and in accordance with *Government Auditing Standards*. As part of an audit in accordance with GAAS and in accordance with *Government Auditing Standards*, we exercise professional judgment and maintain professional skepticism throughout the audit. We also:

1. Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
2. Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the District's internal control. However, we will communicate to you in writing concerning any significant deficiencies or material weaknesses in internal control relevant to the audit of the financial statements that we have identified during the audit.
3. Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.
4. Conclude, based on the audit evidence obtained, whether there are conditions or events, considered in the aggregate, that raise substantial doubt about the District's ability to continue as a going concern for a reasonable period of time.

Because of the inherent limitations of an audit, together with the inherent limitations of internal control, an unavoidable risk that some material misstatements may not be detected exists, even though the audit is properly planned and performed in accordance with GAAS and in accordance with *Government Auditing Standards*.

Our responsibility as auditors is limited to the period covered by our audit and does not extend to any other periods.

Compliance with Laws and Regulations

As previously discussed, as part of obtaining reasonable assurance about whether the basic financial statements are free of material misstatement, we will perform tests of the District's compliance with the provisions of applicable laws, regulations, contracts, and agreements. However, the objective of our audit will not be to provide an opinion on overall compliance and we will not express such an opinion.

Management Responsibilities

Our audit will be conducted on the basis that management acknowledge and understand that they have responsibility:

- a) For the preparation and fair presentation of the basic financial statements in accordance with accounting principles generally accepted in the United States of America;
- b) For the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of basic financial statements that are free from material misstatement, whether due to error, fraudulent financial reporting, misappropriation of assets, or violations of laws, governmental regulations, grant agreements, or contractual agreements; and
- c) To provide us with:
 - i. Access to all information of which management is aware that is relevant to the preparation and fair presentation of the basic financial statements such as records, documentation, and other matters;
 - ii. Additional information that we may request from management for the purpose of the audit;
 - iii. Unrestricted access to persons within the District from whom we determine it necessary to obtain audit evidence.
 - iv. A written acknowledgement of all the documents that management expects to issue that will be included in the annual report and the planned timing and method of issuance of that annual report; and
 - v. A final version of the annual report (including all the documents that, together, comprise the annual report) in a timely manner prior to the date of the auditor's report.
- d) For including the auditor's report in any document containing basic financial statements that indicates that such basic financial statements have been audited by us;
- e) For identifying and ensuring that the District complies with the laws and regulations applicable to its activities;
- f) For adjusting the basic financial statements to correct material misstatements and confirming to us in the management representation letter that the effects of any uncorrected misstatements aggregated by us during the current engagement and pertaining to the current year period(s) under audit are immaterial, both individually and in the aggregate, to the basic financial statements as a whole; and
- g) For acceptance of nonattest services, including identifying the proper party to oversee nonattest work;
- h) For maintaining adequate records, selecting and applying accounting principles, and safeguarding assets;
- i) For informing us of any known or suspected fraud affecting the District involving management, employees with significant role in internal control and others where fraud could have a material effect on the financials; and
- j) For the accuracy and completeness of all information provided.

With regard to the supplementary information referred to above, you acknowledge and understand your responsibility:

- a) for the preparation of the supplementary information in accordance with the applicable criteria;
- b) to provide us with the appropriate written representations regarding supplementary information;
- c) to include our report on the supplementary information in any document that contains the supplementary information and that indicates that we have reported on such supplementary information; and
- d) to present the supplementary information with the audited basic financial statements, or if the supplementary information will not be presented with the audited basic financial statements, to make

the audited basic financial statements readily available to the intended users of the supplementary information no later than the date of issuance by you of the supplementary information and our report thereon.

As part of our audit process, we will request from management, written confirmation concerning representations made to us in connection with the audit.

Nonattest Services

With respect to any nonattest services we perform,

At the end of the year, we agree to perform the following:

- a) Propose adjusting or correcting journal entries detected during the audit, if applicable, to be reviewed and approved by the District's management.
- b) Word process the financial statements using information provided by management.

We will not assume management responsibilities on behalf of the District. However, we will provide advice and recommendations to assist management of the District in performing its responsibilities.

The District's management is responsible for:

- a) making all management decisions and performing all management functions;
- b) assigning a competent individual to oversee the services;
- c) evaluating the adequacy of the services performed;
- d) evaluating and accepting responsibility for the results of the services performed; and
- e) establishing and maintaining internal controls, including monitoring ongoing activities.

Our responsibilities and limitations of the nonattest services are as follows:

- a) We will perform the services in accordance with applicable professional standards
- b) The nonattest services are limited to the services previously outlined. Our firm, in its sole professional judgment, reserves the right to refuse to do any procedure or take any action that could be construed as making management decisions or assuming management responsibilities, including determining account coding and approving journal entries. Our firm will advise the District with regard to tax positions taken in the preparation of the tax return, but the District must make all decisions with regard to those matters.

Reporting

We will issue a written report upon completion of our audit of the District's basic financial statements. Our report will be addressed to the Board of Directors of the District. Circumstances may arise in which our report may differ from its expected form and content based on the results of our audit. Depending on the nature of these circumstances, it may be necessary for us to modify our opinions, add an emphasis-of-matter or other-matter paragraph(s) to our auditor's report, or if necessary, withdraw from the engagement. If our opinions on the basic financial statements are other than unmodified, we will discuss the reasons with you in advance. If, for any reason, we are unable to complete the audit or are unable to form or have not formed opinions, we may decline to express opinions or to issue a report as a result of this engagement.

In accordance with the requirements of Government Auditing Standards, we will also issue a written report describing the scope of our testing over internal control over financial reporting and over compliance with laws, regulations, and provisions of grants and contracts, including the results of that testing. However, providing an opinion on internal control and compliance will not be an objective of the audit and, therefore, no such opinion will be expressed.

Preparation of State Controller Report

Our Responsibilities

The objective of our engagement is to prepare the annual Financial Transactions Report (FTR) in accordance with the California State Controller's Office Instructions based on information provided by you. We will conduct our engagement in accordance with Statements on Standards for Accounting and Review Services (SSARs) promulgated by the Accounting and Review Services Committee of the AICPA and comply with the AICPA's Code of Professional Conduct, including the ethical principles of integrity, objectivity, professional competence, and due care.

We are not required to, and will not, verify the accuracy or completeness of the information you will provide to us for the engagement or otherwise gather evidence for the purpose of expressing an opinion or a conclusion. Accordingly, we will not express an opinion or a conclusion or provide any assurance on the FTR.

Our engagement cannot be relied upon to identify or disclose any FTR misstatements, including those caused by fraud or error, or to identify or disclose any wrongdoing within the District or noncompliance with laws and regulations.

Management Responsibilities

The engagement to be performed is conducted on the basis that management acknowledges and understands that our role is to prepare the FTR in accordance with the State Controller's Office Instructions. Management has the following overall responsibilities that are fundamental to our undertaking the engagement to prepare your FTR in accordance with SSARs:

- a) The selection of accounting principles generally accepted in the United States of America as the financial reporting framework to be applied in the preparation of the financial statements
- b) The design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error
- c) The prevention and detection of fraud
- d) To ensure that the District complies with the laws and regulations applicable to its activities
- e) The accuracy and completeness of the records, documents, explanations, and other information, including significant judgments, you provide to us for the engagement to prepare financial statements
- f) To provide us with:
 - i. Documentation, and other related information that is relevant to the preparation and presentation of the financial statements,
 - ii. Additional information that may be requested for the purpose of the preparation of the financial statements, and
 - iii. Unrestricted access to persons of whom we determine necessary to communicate.

As part of our engagement, we will issue a disclaimer that will state that the FTR were not subjected to an audit, review, or compilation engagement by us and, accordingly, we do not express an opinion, a conclusion, nor provide any assurance on them.

Engagement Fees

Our fixed fees for the services previously outlined will be as follows:

Financial Statements and Auditor Reports	\$18,000
Preparation of the State Controller's Report	500
Total	\$18,500

If significant changes occur in the District's audit requirements with the implementation of new Governmental Accounting Standards Board (GASB) Standards, Government Auditing Standards or the Audit and Accounting Guide for State and Local Governments issued by the AICPA for attest and/or nonattest services, this may render additional services needed which may increase the above noted fixed fee.

Our invoices for these fees will be rendered each month as work progresses and are payable on presentation. In accordance with our firm policies, work may be suspended if the District's account becomes 60 days or more overdue and may not be resumed until the District's account is paid in full. If we elect to terminate our services for nonpayment, our engagement will be deemed to have been completed upon written notification of termination, even if we have not completed our report. The District will be obligated to compensate us for all time expended and to reimburse us for all out-of-pocket costs through the date of termination. The above fee is based on anticipated cooperation from District personnel and the assumption that unexpected circumstances will not be encountered during the audit. If significant additional time is necessary, we will discuss it with management and arrive at a new fee estimate before we incur the additional costs.

Additionally, our fees are dependent on the availability, quality, and completeness of the District's records and, where applicable, upon the District's personnel providing the level of assistance identified in the "prepared by client" request list distributed at the end of our planning work (e.g., District employees preparing confirmations and schedules we request, locating documents selected by us for testing, etc.).

We will schedule the engagement based in part on deadlines, working conditions, and the availability of District key personnel. We will plan the engagement based on the assumption that District personnel will cooperate and provide assistance by performing tasks such as preparing requested schedules, retrieving supporting documents, and preparing confirmations. If, for whatever reason, District personnel are unavailable to provide the necessary assistance in a timely manner, it may substantially increase the work we have to do to complete the engagement within the established deadlines, resulting in an increase in fees over our original fee estimate.

If circumstances occur related to the condition of District records, the availability of sufficient, appropriate audit evidence, or the existence of a significant risk of material misstatement of the financial statements caused by error, fraudulent financial reporting, or misappropriation of assets, which in our professional judgment prevent us from completing the audit or forming an opinion on the financial statements, we retain the right to take any course of action permitted by professional standards, including declining to express an opinion or issue a report, or withdrawing from the engagement.

Should our assumptions with respect to these matters be incorrect, or should the condition of the records, degree of cooperation, or other matters beyond our reasonable control require additional commitments by us beyond those upon which our estimated fees are based, we may adjust our fees and planned completion dates. If significant additional time is necessary, we will discuss it with management and arrive at a new fee estimate as soon as reasonably practicable.

Other Engagement Matters

During the course of the engagement, we may communicate with you or your personnel via fax or e-mail, and you should be aware that communication in those mediums contains a risk of misdirected or intercepted communications.

Government Auditing Standards require that we document an assessment of the skills, knowledge, and experience of management, should we participate in any form of preparation of the basic financial statements and related schedules or disclosures as these actions are deemed a non-audit service.

Paul J Kaymark, CPA is the engagement partner responsible for supervising the engagement and signing the report.

During the course of the audit we may observe opportunities for economy in, or improved controls over, your operations. We will bring such matters to the attention of the appropriate level of management, either orally or in writing.

You agree to inform us of facts that may affect the basic financial statements of which you may become aware during the period from the date of the auditor's report to the date the financial statements are issued.

We agree to retain our audit documentation or work papers for a period of at least seven years from the date of our report.

The audit documentation for this engagement is the property of Nigro & Nigro, PC and constitutes confidential information. However, we may be requested to make certain audit documentation available to regulatory agencies pursuant to authority given to it by law or regulation, or to peer reviewers. If requested, access to such audit documentation will be provided under the supervision of Nigro & Nigro, PC's personnel. Furthermore, upon request, we may provide copies of selected audit documentation to regulatory agencies. The regulatory agencies may intend, or decide, to distribute the copies of information contained therein to others, including other governmental agencies. We will notify the District of any such request.

Conflict Resolution

Should any litigation or adverse action (such as audits by outside governmental agencies and/or threatened litigation, etc.), by third parties arise against the District or the board of directors subsequent to this engagement, which results in the subpoena of documents from Nigro & Nigro, PC and/or requires additional assistance from us to provide information, depositions or testimony, the District hereby agrees to compensate Nigro & Nigro, PC (at our standard hourly rates) for additional time charges and other costs (copies, travel, etc.), and to indemnify us for any attorney's fees to represent Nigro & Nigro, PC.

If any dispute arises among the parties hereto, the parties agree to first try in good faith to settle the dispute by mediation administered by the American Arbitration Association under its applicable rules for resolving professional accounting and related services disputes before resorting to litigation. The costs of any mediation proceeding shall be shared equally by all parties.

The District and Nigro & Nigro, PC both agree that any dispute over fees charged by the auditor to the District will be submitted for resolution by arbitration in accordance with the applicable rules for resolving professional accounting and related services disputes of the American Arbitration Association, except that under all circumstances the arbitrator must follow the laws of California. Such arbitration shall be binding and final. **IN AGREEING TO ARBITRATION, WE BOTH ACKNOWLEDGE THAT IN THE EVENT OF A DISPUTE OVER FEES CHARGED BY THE ACCOUNTANT, EACH OF US IS GIVING UP THE RIGHT TO HAVE THE DISPUTE DECIDED IN A COURT OF LAW BEFORE A JUDGE OR JURY AND INSTEAD WE ARE ACCEPTING THE USE OF ARBITRATION FOR RESOLUTION.** The prevailing party shall be entitled to an award of reasonable attorneys' fees and costs incurred in connection with the arbitration of the dispute in an amount to be determined by the arbitrator.

Conclusion

At the conclusion of our audit engagement, we will communicate to the Board of Directors the following significant findings from the audit:

- a) Our view about the qualitative aspects of the District's significant accounting practices;
- b) Significant difficulties, if any, encountered during the audit;
- c) Uncorrected misstatements, other than those we believe are trivial, if any;
- d) Disagreements with management, if any;
- e) Other findings or issues, if any, arising from the audit that are, in our professional judgment, significant and relevant to those charged with governance regarding their oversight of the financial reporting process;
- f) Material, corrected misstatements that were brought to the attention of management as a result of our audit procedures;
- g) Representations we requested from management;
- h) Management's consultations with other accountants, if any; and

- i) Significant issues, if any, arising from the audit that were discussed, or the subject of correspondence, with management.

Please sign and return the attached copy of this letter to indicate your acknowledgment of, and agreement with, the arrangements for our audit of the basic financial statements including our respective responsibilities.

Enclosed, as required by *Government Auditing Standards*, is a copy of the report on the most recent peer review of our firm.

We appreciate the opportunity to provide these services and believe this letter accurately summarizes the significant terms of our engagement.

Very truly yours,



Nigro & Nigro, PC

The services and arrangements described in this letter are in accordance with our understanding and are acceptable to us.

Management signature: _____

Title: _____

Date: _____

Governance signature: _____

Title: _____

Date: _____

RESOLUTION NO. 1960-24

**RESOLUTION OF THE BOARD OF DIRECTORS OF
YUIMA MUNICIPAL WATER DISTRICT
ADOPTING A CYBER SECURITY POLICY
AND RESCIND RESOLUTION NO. 1700-16**

WHEREAS, the Board of Directors of Yuima Municipal Water District recognizes that we live in a world that is more connected than ever before; and

WHEREAS, as a member of the Joint Powers Insurance Authority (JPIA), this District has Cyber Liability Coverage that will protect the District from a variety of exposures; and

WHEREAS, the Board of Directors wants to provide the tools and resources needed to protect the District to stay online, and increase the resiliency of the District in the event of a cyber incident; and,

WHEREAS, it is in the best interest of the District to define a Cyber Security Policy for the District and to establish the minimum requirements for the Policy.

NOW, THEREFORE, BE IT RESOLVED by the Board of Directors of Yuima Municipal Water District that the Cyber Security Policy, attached hereto, is hereby adopted and Resolution No. 1700-16 is hereby rescinded.

PASSED AND ADOPTED at a regular adjourned meeting of the Board of Directors of YUIMA MUNICIPAL WATER DISTRICT held this 3rd day of June, 2024 by the following roll-call vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

Roland Simpson, President

Attest:

Don Broomell, Secretary



Yuima Municipal Water District

Cybersecurity Policy

June 3, 2024

Introduction

Information Technology (IT) is an integral and critical component of Yuima Municipal Water District's, (YMWD) daily business. This policy seeks to ensure that YMWD's IT resources efficiently serve the primary business functions of YMWD, provide security for YMWD and its electronic data, and comply with federal and other regulations. IT resources include hardware (computers, servers, peripherals), software (licensed applications, operating systems), network equipment (routers, firewalls, wiring), and IT personnel. The integrity of all IT resources is extremely important to the successful operation of YMWD's business.

All computer equipment, peripherals, and software are the property of YMWD and are provided for business purposes. Proper use and control of computer resources is the responsibility of all employees. Intentional or reckless violation of established policies or improper use of YMWD computers will result in corrective action up to and including termination. Employees should also be aware that any work completed on YMWD computers is subject to monitoring and review, and they should not expect their communications to be private.

This Policy supersedes any previous IT policies of Yuima Municipal Water District. The following Policy Statement, Disciplinary Action, and Review paragraphs apply to all individual policies contained within this Cybersecurity Policy.

Policy Statement

It is the policy of Yuima Municipal Water District to use IT resources in a cost-effective manner that safeguards member data and promotes accuracy, safety, Information, and efficiency. The overriding goal of this policy is to comply with all federal and other regulations and to protect the integrity of the private and confidential customer and business data that resides within YMWD's technology infrastructure.

Disciplinary Action

Violation of any of these policies may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to loss of YMWD Information Systems access privileges and may be subject to civil and criminal prosecution.

Review and Acceptance

The General Manager shall review this comprehensive policy at least annually, making such revisions and amendments as deemed appropriate and indicating approval and the date thereof in the policy header.

All YMWD staff are responsible for review and acceptance of this policy annually. Appropriate communications by way of reminder will be sent along with instructions for acceptance.

Policy 1: Acceptable Use of Information Systems

Definitions

Information Systems: All electronic means used to create, store, access, transmit, and use data, information, or communications in the conduct of administrative, instructional, research, or service activities. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Authorized User: An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

Extranet: An intranet that is partially accessible to authorized persons outside of a company or organization.

Overview

Data, electronic file content, information systems, and computer systems at YMWD must be managed as valuable organization resources.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol (FTP) are the property of YMWD. These systems are to be used for business purposes in serving the interests of YMWD and of its customers during normal operations.

Effective security is a team effort involving the participation and support of every YMWD employee, volunteer, and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at YMWD. These rules are in place to protect the authorized user and YMWD. Inappropriate use exposes YMWD to risks including virus attacks, malware, and compromise of network systems and services.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct YMWD business or interacts with internal networks and business systems, whether owned or leased by YMWD, the employee, or a third party.

All employees, volunteer/directors, contractors, consultants, temporaries, and other workers at YMWD, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with YMWD policies and standards, local laws, and regulations.

Policy Detail

Ownership of Electronic Files

All electronic files created, sent, received, or stored on YMWD owned, leased, or administered equipment or otherwise under the custody and control of YMWD are the property of YMWD.

Privacy

Electronic files created, sent, received, or stored on YMWD owned, leased, or administered equipment, or otherwise under the custody and control of YMWD are not private and may be accessed by management at any time without knowledge of the user, sender, recipient, or owner. Electronic file content may also be accessed by appropriate personnel in accordance with directives from the General Manager.

General Use and Ownership

Access requests must be authorized by the General Manager for employees to gain access to computer systems.

Authorized users are accountable for all activity that takes place under their username.

Authorized users should be aware that the data and files they create on the district's systems, immediately become the property of YMWD. Because of the need to protect YMWD's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to YMWD.

For security and network maintenance purposes, authorized individuals of YMWD may monitor equipment, systems, and network traffic at any time.

YMWD reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

YMWD reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with this policy and the following policies:

- Policy 2: Account Management
- Policy 3: Anti-Virus
- Policy 4: YMWD Owned Mobile Device Acceptable Use and Security
- Policy 5: E-mail
- Policy 10: Internet
- Policy 13: Password
- Policy 20: Cloud Computing
- Policy 21: Wireless (Wi-Fi) Connectivity

System level and user level passwords must comply with the Password Policy. Authorized users must not share their YMWD login ID(s), account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authentication purposes. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Authorized users may access, use, or share YMWD proprietary information only to the

extent it is authorized and necessary to fulfill the users assigned job duties.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less.

All users must lockdown their PCs, laptops, and workstations by locking (control-alt-delete) when the host will be unattended for any amount of time.

Employees must log-off, or restart (but not shut down) their PC after their shift.

YMWD proprietary information stored on electronic and computing devices, whether owned or leased by YMWD, the employee, or a third party, remains the sole property of YMWD. All proprietary information must be protected through legal or technical means.

All users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of YMWD proprietary information to their immediate supervisor and/or the General Manager.

All users must report any weaknesses in YMWD computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the General Manager.

Users must not divulge dial-up or dial-back modem phone numbers to anyone without prior consent of the General Manager.

Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan Horse codes.

Unacceptable Use

Users must not intentionally access, create, store, or transmit material which YMWD may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee, volunteer/director, contractor, consultant, or temporary employee of YMWD authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing YMWD-owned resources.

System and Network Activities

The following activities are prohibited by users, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by YMWD.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which YMWD or the end user does not have an active license is prohibited. Users must report unlicensed copies of installed software to the General Manager.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a YMWD computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Attempting to access any data, electronic content, or programs contained on YMWD systems for which they do not have authorization, explicit consent, or implicit need for their job duties.
- Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of YMWD General Manager.
- Installing or using non-standard shareware or freeware software without YMWD approval.
- Installing, disconnecting, or moving any YMWD owned computer equipment and peripheral devices without prior consent of YMWD.
- Purchasing software or hardware, for YMWD use, without prior IT compatibility review.
- Purposely engaging in activity that may;
 - degrade the performance of information systems;
 - deprive an authorized YMWD user access to a YMWD resource;
 - obtain extra resources beyond those allocated; or
 - circumvent YMWD computer security measures.
- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, YMWD users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non-approved programs on YMWD information systems. The YMWD General Manager is the only person authorized to perform these actions.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Access to the Internet at home, from a YMWD-owned computer, must adhere to all the same policies that apply to use from within YMWD facilities. Authorized users must not allow family members or other non-authorized users to access YMWD computer systems.

YMWD information systems must not be used for personal benefit.

Incidental Use

As a convenience to the YMWD user community, incidental use of information systems is permitted. The following restrictions apply:

- Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate supervisors are responsible for supervising their employees regarding excessive use.
- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to YMWD approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to YMWD without prior approval of management.
- 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, YMWD.
- Storage of personal email messages, voice messages, files, and documents within YMWD's information systems must be nominal.
- All messages, files, and documents — including personal messages, files, and documents — located on YMWD information systems are owned by YMWD, may be subject to public records requests, and may be accessed in accordance with this policy.

Review and Acceptance

All YMWD staff are responsible for review and acceptance of *Policy 1: Acceptable Use of Information Systems* upon starting work at YMWD (see below). New employee onboarding and training shall include this *Policy 1* at a minimum, and in addition to all other applicable training and orientation material, and instructions for acceptance shall be provided at that time. Signed acceptance will be received and retained by YMWD Management.

Receipt of Acceptable Use of Information Systems

I have received a copy of the Yuima Municipal Water District Acceptable Use of Information Systems Policy and have completed the Computer Security Awareness program course. I understand the information in the Acceptable Use of Information Systems policy is a summary only, and it is my responsibility to review and become familiar with all of the material contained in the Comprehensive IT Policy.

I further understand the content of the Cybersecurity Policy supersedes all policies previously issued. I also understand that YMWD may supersede, change, eliminate, or add to any policies or practices described in the Cybersecurity Policy.

My signature below indicates that I have received my personal copy of the Acceptable Use of Information Systems Policy and it will be my responsibility to review the Cybersecurity Policies as they are updated.

User Signature: _____

User Name (printed): _____

Date: _____

Policy 2: Account Management

Definitions

Account: Any combination of a User ID (sometime referred to as a username) and a password that grants an authorized user access to a computer, an application, the network, or any other information or technology resource.

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system.

System Administrator: The person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

Overview

Computer accounts are the means used to grant access to YMWD's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for YMWD usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of this policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at YMWD.

Audience

This policy applies to the employees, Directors, volunteers, contractors, consultants, temporaries, and other workers at YMWD, including all personnel affiliated with third parties with authorized access to any YMWD information system.

Policy Detail

Accounts

- All accounts created must have an associated written request and signed management approval that is appropriate for the YMWD system or service.
- All accounts must be uniquely identifiable using the assigned username.
- Shared accounts on YMWD information systems are not permitted.
- Removal of an employee's access while on a leave of absence as deemed necessary.
- All default passwords for accounts must be constructed in accordance with the YMWD Password Policy.
- All accounts must have a password expiration that complies with the YMWD Password Policy.
- Concurrent connections may be limited for technical or security reasons.
- All accounts must be disabled immediately upon employee's termination.

Account Management

The following items apply to System Administrators or other designated staff:

- Information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account. Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorize, perform, review, and audit a single transaction.
- All information system accounts will be actively managed. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
- Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leave of absence.
- All account modifications must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
- Information system accounts are to be reviewed monthly to identify inactive accounts. If an employee or third-party account is found to be inactive for 30 days, the owners (of the account) and their manager will be notified of pending disablement. If the account continues to remain inactive for 15 days, it will be manually disabled.
- A list of accounts, for the systems they administer, must be provided when requested by authorized YMWD management.
- An independent audit review may be performed to ensure the accounts are properly managed.

Policy 3: Anti-Virus

Definitions

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

Trojan Horse: Destructive programs, usually viruses or worms, which are hidden in an attractive or innocent looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or removable media, often from another unknowing victim, or may be urged to download a file from a web site or download site.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need

not attach to particular files or sectors at all.

Spyware: Programs that install and gather information from a computer without permission and reports the information to the creator of the software or to one or more third parties.

Malware: Short for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, worm, or a Trojan horse.

Adware: Programs that are downloaded and installed without user's consent or bound with other software to conduct commercial advertisement propaganda through pop-ups or other ways, which often lead to system slowness or exception after installing.

Keyloggers: A computer program that captures the keystrokes of a computer user and stores them. Modern keyloggers can store additional information, such as images of the user's screen. Most malicious keyloggers send this data to a third party remotely (such as via email).

Ransomware: A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files, unless a ransom is paid.

Server: A computer program that provides services to other computer programs in the same or other computers. A computer running a server program is frequently referred to as a server, although it may also be running other client (and server) programs.

Security Incident: In information operations, a security incident is an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent.

E-mail: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.

Overview

Malware threats must be managed to minimize the amount of downtime realized by YMWD's systems and prevent risk to critical systems and member data. This policy is established to:

- Create prudent and acceptable practices regarding anti-virus management
- Define key terms regarding malware and anti-virus protection
- Educate individuals, who utilize YMWD system resources, on the responsibilities associated with anti-virus protection

Note: The terms virus and malware, as well as anti-virus and anti-malware, may be used interchangeably.

Purpose

This policy was established to help prevent infection of YMWD computers, networks,

and technology systems from malware and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

Audience

This policy applies to all computers connecting to the YMWD network for communications, file sharing, etc. This includes, but is not limited to, desktop computers, laptop computers, servers, and any PC based equipment connecting to the YMWD network.

Policy Detail

All computer devices connected to the YMWD network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.

The virus protection software must not be disabled or bypassed without YMWD approval.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Each file server attached to the YMWD network, must utilize YMWD approved virus protection software and setup to detect and clean viruses that may infect YMWD resources.

Each e-mail gateway must utilize YMWD approved e-mail virus protection software.

All files on computer devices will be scanned periodically for malware.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Service Desk.

If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the YMWD network until the infection has been removed.

Users should:

- Avoid viruses by NEVER opening any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately then remove them from the Trash or Recycle Bin.
- Delete spam, chain, or other junk mail without opening or forwarding the item.
- Never download files from unknown or suspicious sources.
- Always scan removable media from an unknown or non-YMWD source (such as a CD or USB from a vendor) for viruses before using it.
- Back up critical data on a regular basis and store the data in a safe place. Critical

YMWD data can be saved to network drives and are backed up on a periodic basis.

Because new viruses are discovered every day, users should periodically check the Anti-Virus Policy for updates. The General Manager should be contacted for updated recommendations.

Policy 4: YMWD Owned Mobile Device Acceptable Use and Security

Definitions

Clear text: Unencrypted data

Full disk encryption: Technique that encrypts an entire hard drive, including operating system and data.

Key: Phrase used to encrypt or decrypt data

Overview

Acceptable use of YMWD owned mobile devices must be managed to ensure that employees, Board of Directors, and related constituents who use mobile devices to access YMWD's resources for business do so in a safe and secure manner.

This policy is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

Purpose

This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of YMWD's direct control. This mobile device policy applies to, but is not limited to, any mobile device issued by YMWD that contains stored data owned by YMWD and all devices and accompanying media that fit the following device classifications:

- Laptops, Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any YMWD owned mobile device capable of storing corporate data and connecting to an unmanaged network

This policy addresses a range of threats to, or related to, the use of YMWD data:

Threat	Description
Loss	Devices used to transfer, or transport work files could be lost or stolen
Theft	Sensitive corporate data is deliberately stolen and sold by an employee
Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, Trojans, Worms, Spyware and other threats could be introduced via a mobile device

Compliance	Loss or theft of financial and/or personal and confidential data could expose YMWD to the risk of non-compliance with various identity theft and privacy laws
------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of YMWD. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the YMWD network.

Audience

This policy applies to all YMWD employees, including full and part-time staff, and the Board of Directors who utilize company-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust YMWD has built with its members, suppliers, and other constituents. Consequently, employment at YMWD does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Policy Detail

This policy applies to any corporate owned hardware and related software that could be used to access corporate resources.

The overriding goal of this policy is to protect the integrity of the private and confidential business data that resides within YMWD’s technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to YMWD’s public image. Therefore, all users employing a YMWD owned mobile device, connected to an unmanaged network outside of YMWD’s direct control, to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

Affected Technology

Connectivity of all mobile devices will be centrally managed by YMWD’s General Manager and will utilize authentication and strong encryption measures. To protect YMWD’s infrastructure, failure to adhere to these security protocols will result in immediate suspension of all network access privileges.

Responsibilities

It is the responsibility of any employee or Board Member of YMWD, who uses a YMWD owned mobile device to access corporate resources, to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any YMWD owned mobile device that is used to conduct YMWD business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user’s account. Based on this, the following rules must be observed:

- **Access control**

YMWD reserves the right to refuse, by physical and non-physical means, the ability

to connect mobile devices to YMWD and YMWD-connected infrastructure. YMWD will engage in such action if it feels such equipment is being used in such a way that puts YMWD's systems, data, users, and members at risk.

End users who wish to connect such devices to non-corporate network infrastructure to gain access to YMWD data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by YMWD. YMWD data is not to be accessed on any hardware that fails to meet YMWD's established enterprise security standards.

All mobile devices attempting to connect to the YMWD network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by YMWD's General Manager. Devices that are not corporate issued are not in compliance with YMWD's security policies and will not be allowed to connect except by provision of the Personal Device Acceptable Use and Security Policy. YMWD owned laptop computers may only access the corporate network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) or Internet Protocol Security (IPSec) VPN connection. The SSL or IPSec VPN portal Web address will be provided to users as required. Smart mobile devices such as Smartphones, PDAs, and UMPCs will access the YMWD network and data using Mobile VPN software installed on the device by YMWD.

- **Security**

Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices containing stored data owned by YMWD must use an approved method of encryption to protect data. Laptops must employ full drive encryption with an approved software encryption package. No YMWD data may exist on a laptop in clear text. All mobile devices must be protected by a strong password. Refer to the YMWD password policy for additional information. Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.

All keys used for encryption and decryption must meet complexity requirements described in YMWD's Password Policy.

All users of corporate owned mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain YMWD data. Users with devices that are not issued by YMWD must adhere to the Personal Device Acceptable Use and Security Policy.

To ensure the security of YMWD equipment, mobile devices will be transported and stored as specified in the "Mobile Device Transport and Storage" procedure.

Passwords and confidential data should not be stored on unapproved or unauthorized non-YMWD devices.

Any company owned mobile device that is being used to store YMWD data must adhere to the authentication requirements of YMWD. In addition, all hardware security configurations must be pre-approved by YMWD before any enterprise

data-carrying device can be connected to it.

YMWD will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and addressed accordingly.

Employees, Board of Directors, and temporary staff will contact YMWD's

General Manager to permanently erase company specific data from such devices once their use is no longer required.

In the event of a lost or stolen mobile device, it is incumbent on the user to report this to the General Manager immediately. If the device is recovered, it can be submitted to the General Manager for re-provisioning.

YMWD maintains the process for patching computing equipment and devices. A device's firmware/operating system must be up to date in order to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of YMWD.

YMWD maintains the process for security audits on mobile devices. Since handheld devices are not completely under the control of YMWD, a periodic audit will be performed to ensure the devices are not a potential threat to YMWD.

- **Organizational Protocol**

YMWD will establish audit trails, and these will be accessed, published, and used without notice. The resulting reports may be used for investigation of possible breaches and/or misuse. To identify unusual usage patterns or other suspicious activity, the end user agrees to and accepts that his or her access and/or connection to YMWD's networks may be monitored to record dates, times, duration of access, etc. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains YMWD's highest priority.

The end user agrees to immediately report to YMWD's General Manager, any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of YMWD resources, databases, networks, etc.

- **Network Traffic Rules and Restrictions**

Intra-network traffic is subject to distinct operating rules and restrictions. Through the use of firewall technology, outside parties are directed only to approved, internal resources. An example of this is web page services that allow certain types of traffic from the Internet (web page browsing) but have other types of traffic blocked (i.e. administrative tasks). This strategy dramatically reduces the risk of any party gaining unauthorized access to a protected server.

The internal network is also protected from virus attacks through the use of network-level anti-virus software that is updated automatically on a regular basis. These regular updates are loaded automatically to each PC, as they are available. This provides the most up to date virus protection and security available. E-mail is also scanned prior to delivery, reducing the potential of a virus entering the network in this manner.

- **Physical Site Security**

IT equipment is protected by locked access doors allowing only authorized personnel into the Department. Sensitive data, hardware, and software Access is further limited to a small number of authorized personnel. It is YMWD's practice to change administrative passwords and immediately remove card access privileges after any change in staff.

In addition to on-site storage of data, YMWD stores overnight backups of critical systems data and replicated Storage Area Network (SAN) storage to a secure, off-site location. This ensures that data is available in the event of a disaster or other critical situation.

- **Staff Training and Review**

Staff receives training and reviews all procedures at least annually or as major system additions or changes are implemented.

- **User Password Maintenance**

YMWD's policy prohibits users from sharing or disclosing their passwords, is intended to prohibit unauthorized access to systems and data. After receiving a change in status staff immediately removes user access codes from appropriate systems.

- **Expert Assistance**

New threats to security, safety, and accuracy appear daily and system vendors publish updates and patches regularly to eliminate the threat. To assist in the ongoing maintenance of key components of system security, YMWD may engage a third party to provide audit oversight.

- **Communications Network**

YMWD employs the use of several types of data communication lines including dial-up phone lines, direct point-to-point circuits, and other private and public network connections. Data transmissions are secured, encrypted, and/or password protected, as needed.

Response Program

In the event YMWD suspects or detects unauthorized individuals have gained access to District information systems, YMWD will report such actions to appropriate regulatory and law enforcement agencies according to YMWD's information security response procedures.

Policy 5: E-Mail

Definitions

Anti-Spoofing: A technique for identifying and dropping units of data, called packets, that have a false source address.

Antivirus: Software used to prevent, detect, and remove malicious software.

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (e-mail): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email spoofing: The forgery of an email header so the message appears to have originated from someone other than the actual source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation to provide sensitive data or perform an action such as processing a wire transfer.

Inbound filters: A type of software-based traffic filter allowing only designated traffic to flow towards a network.

Quarantine: Suspicious email message may be identified by an antivirus filter and isolated from the normal mail inbox.

SPAM: Unsolicited e-mail, usually from Internet sources. It is often referred to as junk e-mail.

Overview

E-mail at YMWD must be managed as valuable and mission critical resources. Thus, this policy is established to:

- Create prudent and acceptable practices regarding the use of information resources
- Educate individuals who may use information resources with respect to their responsibilities associated with such use
- Establish a schedule for retaining and archiving e-mail

Purpose

The purpose of this policy is to establish rules for the use of YMWD email for sending, receiving, or storing of electronic mail.

Audience

This policy applies equally to all individuals granted access privileges to any YMWD information resource with the capacity to send, receive, or store electronic mail.

Legal

Individuals involved may be held liable for:

- Sending or forwarding e-mails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission
- Sending or forwarding copyrighted material without permission
- Knowingly sending or forwarding an attachment that contains a virus

Policy Detail

Company e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on YMWD's computer systems. YMWD can, but is not obliged to, monitor emails without prior notification. All e-mails, files, and documents – including personal e-mails, files, and documents – are owned by YMWD, may be subject to open records requests, and may be accessed in accordance with this policy.

Incoming email must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy. Introducing a virus or malicious code to YMWD systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, IT must be immediately notified.

Anti-spoofing practices have been initiated for detecting spoofed emails. Employees should be diligent in identifying a spoofed email. If email spoofing has occurred, the General Manager must be immediately notified.

Incoming emails are scanned for malicious file attachments. If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed from the email prior to delivery.

Email rejection is achieved through listing domains and IP addresses associated with malicious actors. Any incoming email originating from a known malicious actor will not be delivered.

Any email account misbehaving by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.

E-mail is to be used for business purposes and in a manner that is consistent with other forms of professional business communication. All outgoing attachments are automatically scanned for viruses and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm YMWD's reputation.

The following activities are prohibited by policy:

- Sending e-mail that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability.
- Using e-mail for conducting personal business.
- Using e-mail for the purpose of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.
- Sending e-mail using another person's e-mail account, except when authorized to send messages for another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- Forging or attempting to forge e-mail messages.
- Using unauthorized e-mail software.

- Knowingly disabling the automatic scanning of attachments on any YMWD personal computer.
- Knowingly circumventing e-mail security measures.
- Sending or forwarding joke e-mails, chain letters, or hoax letters.
- Sending unsolicited messages to large groups, except as required to conduct YMWD business.
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding email with computer viruses.
- Setting up or responding on behalf of YMWD without management approval.

All confidential or sensitive YMWD material transmitted via e-mail, outside YMWD's network, must be encrypted. Passwords to decrypt the data should not be sent via email.

E-mail is not secure. Users must not e-mail passwords, social security numbers, account numbers, pin numbers, dates of birth, mother's maiden name, etc. to parties outside the YMWD network without encrypting the data.

All user activity on YMWD information system assets is subject to logging and review. YMWD has software and systems in place to monitor email usage.

E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of YMWD, unless appropriately authorized (explicitly or implicitly) to do so.

Users must not send, forward, or receive confidential or sensitive YMWD information through non-YMWD email accounts. Examples of non-YMWD e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and e-mail provided by other Internet Service Providers (ISP).

Users with non-YMWD issued mobile devices must adhere to the Personal Device Acceptable Use and Security Policy for sending, forwarding, receiving, or storing confidential or sensitive YMWD information.

Incidental Use

Incidental personal use of sending e-mail is restricted to YMWD approved users; it does not extend to family members or other acquaintances.

Without prior management approval, incidental use must not result in direct costs to YMWD.

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 liability for or

embarrassment to YMWD.

Storage of personal files and documents within YMWD's IT systems should be nominal.

E-mail Retention

- Deleted and archived emails are subject to automatic purging.
- Appointments, Tasks, and Notes older than the retention period are subject to automatic purging.

Policy 6: Firewall

Definitions

Firewall: Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.

Firewall configuration: The system setting affecting the operation of a firewall appliance.

Firewall ruleset: A set of policy statements or instructions used by a firewall to filter network traffic.

Host firewall: A firewall application that addresses a separate and distinct host, such as a personal computer.

Internet Protocol (IP): Primary network protocol used on the Internet.

Network firewall: A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).

Network topology: The layout of connections (links, nodes, etc.) of a computer network.

Simple Mail Transfer Protocol (SMTP): An Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Virtual private network (VPN): A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with private, secure access to their organization's network.

Overview

YMWD operates network firewalls between the Internet and its private internal network to create a secure operating environment for YMWD's computer and network resources. A firewall is just one element of a layered approach to network security.

Purpose

This policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to YMWD's network and information systems.

The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks
- Block unwanted traffic as determined by the firewall ruleset
- Hide vulnerable internal systems from the Internet
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet
- Log traffic to and from the internal network
- Provide robust authentication
- Provide virtual private network (VPN) connectivity

Policy Detail

All network firewalls, installed and implemented, must conform to the current standards as determined by YMWD. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

The approach adopted to define firewall rulesets is that all services will be denied by the firewall unless expressly permitted in this policy.

- Outbound – allows all Internet traffic to authorized groups
- All traffic is authorized by Internet Protocol (IP) address and port

The firewalls will provide:

Packet filtering – selective passing or blocking of data packets as they pass through a network interface. The most often used criteria are source and destination address, source and destination port, and protocol.

Application proxy – every packet is stopped at the proxy firewall and examined and compared to the rules configured into the firewall.

Stateful Inspection – a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

The firewalls will protect against:

- IP spoofing attacks – the creation of IP packets with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
- Denial-of-Service (DoS) attacks - the goal is to flood the victim with overwhelming amounts of traffic and the attacker does not care about receiving responses to the attack packets.
- Any network information utility that would reveal information about the YMWD domain.

A change control process is required before any firewall rules are modified. All related Firewall documentation is to be retained for three (3) years.

All firewall implementations must adopt the position of “least privilege” and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow

permissible traffic.

Firewall rulesets and configurations require periodic review to ensure they afford the required levels of protection.

Firewall rulesets and configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained, to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.

Responsibilities

The General Manager is responsible for implementing and maintaining YMWD firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to a primary firewall administrator and designees as assigned. Password construction for the firewall will be consistent with the strong password creation practices outlined in the YMWD Password Policy.

The specific guidance and direction for information systems security is the responsibility of the General Manager. Accordingly, the General Manager will manage the configuration of the YMWD firewalls.

General Manager is responsible for:

- Retention of the firewall rules
- Patch Management
- Review the firewall logs for:
 - System errors
 - Blocked web sites
 - Attacks
- Sending alerts to the YMWD network administrators and YMWD Management in the event of attacks or system errors
- Backing up the firewalls

Policy 7: Hardware and Electronic Media Disposal

Definitions

Beyond reasonable repair: Refers to any and all equipment whose condition requires fixing or refurbishing that is likely to cost as much or more than total replacement.

Chain of Custody (CoC): Refers to the chronological documentation of the custody, transportation, or storage of evidence to show it has not been tampered with prior to destruction.

Disposition: Refers to the reselling, reassignment, recycling, donating, or disposal of IT equipment through responsible, ethical, and environmentally sound means.

Non-leased: Refers to any and all IT assets that are the sole property of YMWD, that is, equipment not rented, leased, or borrowed from a third-party supplier or partner company.

Obsolete: Refers to any and all equipment that no longer meets requisite functionality.

Surplus: Refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

Overview

Hardware and electronic media disposition is necessary at YMWD to ensure the proper disposition of all non-leased YMWD IT hardware and media capable of storing member information. Improper disposition can lead to disclosing information that would be potentially damaging.

Purpose

YMWD owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this policy. Where assets have not reached end of life, it is desirable to take advantage of residual value through reselling, auctioning, donating, or reassignment to a less critical function. This policy will establish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner. YMWD's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and YMWD's upgrade guidelines. All disposition procedures for retired IT assets must adhere to company approved methods.

Policy Detail

Disposition procedures for all IT assets and equipment will be centrally managed and coordinated by YMWD. YMWD is responsible for backing up data from IT assets slated for disposition (if applicable) and removing company tags and/or identifying labels. IT is responsible for selecting and approving external agents for hardware sanitization, reselling, recycling, or destruction of the equipment. IT is also responsible for the chain of custody in acquiring credible documentation from contracted third parties that verify adequate disposition and disposal that adhere to legal requirements and environmental regulations.

It is the responsibility of any employee of YMWD, with the appropriate authority, to ensure that IT assets are disposed of according to the methods in the Hardware and Electronic Media Disposal Procedure. It is imperative that all dispositions are done appropriately, responsibly, and according to IT lifecycle standards, as well as with YMWD's resource planning in mind.

Hardware asset types and electronic media that require secure disposal include, but are not limited to, the following:

- Computers (desktops and laptops)
- Printers
- Handheld devices
- Servers
- Networking devices (hubs, switches, bridges, and routers)
- Floppy disks
- Backup tapes
- CDs and DVDs
- Zip drives
- Hard drives
- Flash memory
- Other portable storage devices

Policy 8: Security Incident Management

Definitions

Security incident: Refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include, but are not limited to, unauthorized access, malicious code, network probes, and denial of service attacks.

Overview

Security Incident Management at YMWD is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify YMWD members of the breach.

Purpose

This policy defines the requirement for reporting and responding to incidents related to YMWD information systems and operations. Incident response provides YMWD with the capability to identify when a security incident occurs. If monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

This policy applies to all information systems and information system components of YMWD. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- Devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities.

In the event a breach of member's information occurs, YMWD is required to notify the government authority.

Policy Detail

Program Organization

- **Computer Emergency Response Plan**
YMWD management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service. For example, intranet or internet connectivity is interrupted or an isolated malware discovery.
- **Incident Response Plan Contents**
The YMWD incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:

- Specific incident response procedures
 - Business recovery and continuity procedures
 - Data backup processes
 - Analysis of legal requirements for reporting compromises
 - Identification and coverage for all critical system components
 - Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers
- **Incident Response and Recovery**

A security incident response capability will be developed and implemented for all information systems that house or access YMWD controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activity

To facilitate incident response operations, responsibility for incident handling operations will be assigned to an incident response team. If an incident occurs, the members of this team will be charged with executing the incident response plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations on an annual basis.

Incident response plans will be reviewed and, where applicable, revised on an annual basis. The reviews will be based upon the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.

- **Intrusion Response Procedures**

The General Manager must document and periodically revise the Incident Response Plan with intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.
- **Malicious Code Remediation**

Steps followed will vary based on scope and severity of a malicious code incident as determined by Information Security Management. They may include but are not limited to: malware removal with one or more tools, data quarantine, permanent data deletion, hard drive wiping, or hard drive/media destruction.
- **Data Breach Management**

YMWD management should prepare, test, and annually update the Incident Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.

- **Incident Response Plan Evolution**
The Incident Response Plan must be updated to reflect the lessons learned from actual incidents.
- The Incident Response Plan must be updated to reflect developments in the industry.
- Refer to the [Incident Response Plan](#) details.

Program Communication

- **Reporting to Third Parties**
Senior management, in conjunction with the Board of directors and the IT representative will determine if external disclosure is needed per this policy before reporting these violations.

If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.

- **Display of Incident Reporting Contact Information**
YMWD contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters, and the intranet.

Policy 9: Information Technology Purchasing

Overview

Information Technology purchasing at YMWD must be managed to ensure compatibility and to control costs of the technology and services requested.

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for the purchase of all IT hardware, software, computer-related components, and technical services purchased with YMWD funds.

Purchases of technology and technical services for YMWD must be approved and coordinated by the General Manager.

Scope

The scope of this policy includes, but is not limited to, the following YMWD technology resources:

- Desktops, laptops, smartphones/PDAs, cell phones, tablets, servers, and other equipment
- Software running on the devices mentioned above
- Peripheral equipment, such as printers and scanners
- Cables or connectivity-related devices
- Audio-visual equipment, such as projectors and cameras

This policy extends to technical services, such as off-site disaster recovery solutions and

Internet Service Providers (ISPs), as well as professional services, such as consultants and legal professionals hired through the YMWD. These include, but are not limited to, the following:

- Professionals or firms contracted for application development and maintenance
- Web services provided by a third party
- Consulting professionals
- Recruiting services
- Training services
- Disaster recovery services
- Hosted telephone services
- Telephone network services
- Data network services

Policy Detail

All hardware, software, or components purchased with YMWD funds are the property of YMWD. This also includes all items purchased using a personal credit card, for which the employee is later reimbursed.

All purchase requests for hardware, software, computer-related components, internet services, or third-party electronic services must be submitted to the General Manager for final purchase approval and ensures that they meet or exceed security requirements.

Policy 10: Internet

Definitions

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

Intranet: A private network for communications and sharing of information that, like the Internet, is based on Transmission Control Protocol/Internet Protocol (TCP/IP), but is accessible only to authorized employees within an organization. An organization's intranet is usually protected from external access by a firewall.

User: An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

World Wide Web (www): A system of Internet hosts that supports documents formatted in Hypertext Markup Language (HTML) that contains links to other documents (hyperlinks) and to audio, video, and graphic images. Individuals can access the Web with special applications called browsers, such as Microsoft Internet Explorer.

Overview

Internet access and usage at YMWD must be managed as valuable and mission critical resources. This policy is established to:

- Create prudent and acceptable practices regarding the use of the Internet.
- Educate individuals who may use information resources with respect to their responsibilities associated with such use.

Purpose

The purpose of this policy is to establish the rules for the use of YMWD Internet for access to the Internet or the Intranet.

Audience

This policy applies equally to all individuals granted access privileges to any YMWD information system or resource with the capacity to access the Internet, the Intranet, or both.

Policy Detail

Accessing the Internet

Users are provided access to the Internet to assist them in the performance of their jobs. At any time, at the request of management, Internet access may be revoked. IT may restrict access to certain Internet sites that reduce network performance or are known or found to be compromised with and by malware. YMWD will use internet filters to block high-risk content and deny access to any unwanted material or malware in support of the Acceptable Use Policy.

All software used to access the Internet must be part of the YMWD standard software suite or approved by IT. Such software must incorporate all vendor provided security patches.

Users accessing the Internet through a computer connected to YMWD's network must do so through an approved Internet firewall or other security device. All software used to access the Internet shall be configured to use a proxy or other means of managing or controlling. Bypassing YMWD's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using YMWD Internet access for: unauthorized access to local and remote computer systems, software piracy, illegal activities, the transmission of threatening, obscene, or harassing materials, or personal solicitations.

Expectation of privacy

Users should have no expectation of privacy in anything they create, store, send, or receive using YMWD's Internet access.

Users expressly waive any right of privacy in anything they create, store, send, or receive using YMWD's Internet access.

File downloads and virus protection

Users are prohibited from downloading and installing software on their PC without proper authorization from IT. Technical controls may be utilized to limit the download and installation of software.

Downloaded software may be used only in ways that conform to its license and copyrights.

All files, downloaded from the Internet, must be scanned for viruses using YMWD approved virus detection software. If a user suspects a file may be infected, he/she must notify IT immediately.

Users are prohibited from using the Internet to deliberately propagate any virus, worm,

Trojan Horse, trap-door, or other malicious program.

Monitoring of computer and Internet usage

All user activity on YMWD IT assets is subject to logging and review. YMWD has the right to monitor and log all aspects of its systems including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

Frivolous use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

Personal use, beyond incidental use of the Internet, may be done only on break room PCs and only in compliance with this policy.

Content

YMWD utilizes software that makes it possible to identify and block access to Internet sites containing sexually explicit material or other material deemed inappropriate in the workplace. The display, storing, archiving, or editing of such content on any YMWD PC is prohibited.

Users are prohibited from attempting to access or accessing inappropriate sites from any YMWD PC. If a user accidentally connects to a site containing such material, the user must disconnect at once and report the incident immediately to IT.

YMWD Departments may not host their own websites or contract for the hosting of websites by a vendor without the permission of IT.

Content on all YMWD hosted web sites must comply with the YMWD Acceptable Use of Information Systems and Privacy Policies. No internal data will be made available to hosted Internet websites without approval of IT.

Incidental use

Incidental personal use of Internet access is restricted to YMWD approved Users; it does not extend to family members or other acquaintances.

Incidental use must not result in direct costs to YMWD.

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 liability for, or embarrassment to, YMWD.

Storage of personal files and documents within YMWD's IT should be nominal.

All files and documents, including personal files and documents, are owned by YMWD, may be subject to open records requests, and may be accessed in accordance with this policy.

Policy 11: Log Management

Definitions

End points: Any user device connected to a network. End points can include personal computers, personal digital assistants, scanners, etc.

Flow: The traffic that corresponds to a logical connection between two processes in the network.

IP: Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet.

Packet: The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

Overview

Most components of the IT infrastructure at YMWD are capable of producing logs chronicling their activity over time. These logs often contain very detailed information about the activities of applications and the layers of software and hardware that support those applications.

Logging from critical systems, applications, and services can provide key information and potential indicators of compromise and is critical to have for forensics analysis.

Purpose

Log management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance. -YMWD will perform a periodic risk assessment to determine what information may be captured from the following:

- Access – who is using services
- Change Monitoring – how and when services were modified
- Malfunction – when services fail
- Resource Utilization – how much capacity is used by services
- Security Events – what activity occurred during an incident, and when
- User Activity – what people are doing with services

Policy Detail

Log generation

Depending on the volume of activity and the amount of information in each log entry, logs have the potential of being very large. Information in logs often cannot be controlled by application, system, or network administrators, so while the listed items are highly desirable, they should not be viewed as absolute requirements.

Application logs

Application logs identify what transactions have been performed, at what time, and

for whom. Those logs may also describe the hardware and operating system resources that were used to execute that transaction.

System logs

System logs for operating systems and services, such as web, database, authentication, print, etc., provide detailed information about their activity and are an integral part of system administration. When related to application logs, they provide an additional layer of detail that is not observable from the application itself. Service logs can also aid in intrusion analysis, when an intrusion bypasses the application itself.

Change management logs, that document changes in the IT or business environment, provide context for the automatically generated logs.

Other sources, such as physical access or surveillance logs, can provide context when investigating security incidents.

Client workstations also generate system logs that are of interest, particularly for local authentication, malware detection, and host-based firewalls.

Network logs

Network devices, such as firewalls, intrusion detection/prevention systems, routers, and switches are generally capable of logging information. These logs have value of their own to network administrators, but they also may be used to enhance the information in application and other logs.

Many components of the IT infrastructure, such as routers and network-based firewalls, generate logs. All of the logs have potential value and should be maintained. These logs typically describe flows of information through the network, but not the individual packets contained in that flow.

Other components for the network infrastructure, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers, provide valuable information about network configuration elements, such as IP addresses, that change over time.

Time synchronization

One of the important functions of a log management infrastructure is to relate records from various sources by time. Therefore, it is important that all components of the IT infrastructure have synchronized clocks. YMWD uses Network Time Protocol (NTP) for time synchronization.

Use of log information

Logs often contain information that, if misused, could represent an invasion of the privacy of members of YMWD. While it is necessary for YMWD to perform regular collection and monitoring of these logs, this activity should be done in the least invasive manner.

Baseline behavior

It is essential that a baseline of activity, within the IT infrastructure, be established and tracked as it changes over time. Understanding baseline behavior allows for the detection of anomalous behavior, which could indicate a security incident or a change in normal usage patterns. Procedures will be in place to ensure that this information

is reviewed on a regular and timely basis.

Investigation

When an incident occurs, various ad hoc questions will need to be answered. These incidents may be security related, or they may be due to a malfunction, a change in the IT infrastructure, or a change in usage patterns. Whatever the cause of the incident, it will be necessary to retrieve and report log records.

Thresholds shall be established that dictate what level of staff or management response is required for any given log entry or group of entries and detailed in a procedure.

Log record life-cycle management

When logs document or contain valuable information related to activities of YMWD's information resources or the people who manage those resources, they are YMWD Administrative Records, subject to the requirements of YMWD to ensure that they are appropriately managed and preserved and can be retrieved as needed.

Retention

To facilitate investigations, as well as to protect privacy, the retention of log records should be well defined to provide an appropriate balance among the following:

- Confidentiality of specific individuals' activities
- The need to support investigations
- The cost of retaining the records

Care should be taken not to retain log records that are not needed. The cost of long-term retention can be significant and could expose YMWD to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.

Log management infrastructure

A log management infrastructure will be established to provide common management of log records. To facilitate the creation of log management infrastructures, system-wide groups will be established to address the following issues:

- Technology solutions that can be used to build log management infrastructures
- Typical retention periods for common examples of logged information

Incident response plan

Incident response is defined as an organized approach to addressing and managing the aftermath of a security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

As required in the Incident Response Plan, YMWD will assemble a team to handle any incidents that occur. Necessary actions to prepare YMWD and the Incident Response Team will be conducted prior to an incident as required in the Incident Response Plan.

Below is a summary of the steps YMWD management, would take:

- The General Manager will immediately investigate the intrusion to:
 - Prevent any further intrusion to the system

- Determine the extent of the intrusion and any damage caused
 - Take any steps possible to prevent any future such intrusions
 - Determine the best action to restore all data and access functionality
- The General Manager shall notify the Board of Directors.
 - The General Manager will follow escalation processes and notification procedures as outlined in the Incident Response Plan. Examples include, but are not limited to, notifications to staff, regulatory agencies, law enforcement agencies, FBI, or the public.
 - If applicable, notices will be sent to affected customers members in compliance with the requirements of California State Civil Codes.

Training

YMWD recognizes that adequate training is of primary importance in preventing IT security breaches, virus outbreaks, and other related problems. YMWD will conduct regular IT training through methods such as staff meetings and computer-based tutorial programs. In addition, employees will be trained to recognize, respond to, and where appropriate, report any unauthorized or fraudulent attempts to obtain member information.

Refer to CSATE program for training.

All new employees will receive IT Security Training, as part of their orientation training, emphasizing security and IT responsibility. The General Manager, or designee, is responsible for training new employees on Information Security.

Testing

YMWD will require periodic tests of the key controls, systems, and procedures of the information security program.

Policy 12: Network Security and VPN Acceptable Use

Definitions

Virtual Private Network (VPN): A private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Some VPNs allow employees to securely access a corporate intranet while located outside the office.

User Authentication: A method by which the user of a system can be verified as a legitimate user independent of the computer or operating system being used.

Multi-Factor Authentication: A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories:

- Knowledge (something they know)
- Possession (something they have)
- Inherence (something they are)

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Examples include:

- Being logged into the corporate network via a local Ethernet connection, and dialing into AOL or another Internet Service Provider (ISP)
- Being on a YMWD provided remote access home network, and connecting to another network, such as a spouse's remote access
- Configuring an Integrated Services Digital Network (ISDN) router to dial into YMWD and an ISP, depending on packet destination

DSL: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

ISDN: There are two flavors of ISDN: BRI and PRI. BRI is used for home/office/remote access. BRI has two "Bearer" channels at 64kb (aggregate 128kb) and 1 D channel for signaling information.

Remote Access: Any access to YMWD's corporate network through a non-YMWD controlled network, device, or medium.

Split-tunneling: Simultaneous direct access to a non-YMWD network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into YMWD's corporate network via a Virtual Private network (VPN) tunnel. VPN is a method for accessing a remote network via "tunneling: through the Internet.

IPSec Concentrator: A device in which VPN connections are terminated.

Cable Modem: Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.

Overview

This policy is to protect YMWD's electronic information from being inadvertently compromised by authorized personnel connecting to the YMWD network locally and remotely via VPN.

Purpose

The purpose of this policy is to define standards for connecting to YMWD's network from any host. These standards are designed to minimize the potential exposure to YMWD from damages, which may result from unauthorized use of YMWD resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical YMWD internal systems, etc.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, SSH, and cable modems, etc.

Audience

This policy applies to all YMWD employees, volunteers/directors, contractors, vendors, and agents with a computer or workstation used to connect to the YMWD network. This

policy applies to remote access connections used to do work on behalf of YMWD, including reading or sending email and viewing intranet resources.

Network Security

Users are permitted to use only those network addresses assigned to them by YMWD.

All remote access to YMWD will be through a secure VPN connection on a YMWD owned device that has up-to-date anti-virus software.

Remote users may connect to YMWD Information Systems using only protocols approved by YMWD.

Users inside the YMWD firewall may not be connected to the YMWD network at the same time a remote connection is used to an external network.

Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point to the YMWD network without YMWD approval.

Users must not install network hardware or software that provides network services without YMWD approval.

Non-YMWD computer systems that require network connectivity must be approved by YMWD.

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, YMWD users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the YMWD network infrastructure.

Users are not permitted to alter network hardware in any way.

Remote Access

It is the responsibility of YMWD employees, volunteers/directors, contractors, vendors, and agents, with remote access privileges to YMWD's corporate network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to YMWD.

General access to the Internet, through the YMWD network is permitted for employees who have flat-rate services and only for business purposes. YMWD employees are responsible to ensure that they:

- Do not violate any YMWD policies
- Do not perform illegal activities
- Do not use the access for outside business interests

YMWD employees bear responsibility for the consequences should access be misused.

Employees are responsible for reviewing the following topics (listed elsewhere in this policy) for details of protecting information when accessing the corporate network via remote access methods and acceptable use of YMWD's network:

- Virtual Private Network (VPN)
- Wireless Communications

Dial-in modem usage is not a supported or acceptable means of connecting to the YMWD network.

Requirements

Secure remote access must be strictly controlled.

YMWD employees, volunteers/directors, and contractors should never provide their login or email password to anyone, including family members.

YMWD employees, volunteers/directors, and contractors with remote access privileges:

- Must ensure that their computer, which is remotely connected to YMWD's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Must not use non-YMWD email accounts (i.e. Hotmail, Yahoo, AOL), or other external resources to conduct YMWD business, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home user's equipment for split-tunneling or dual homing is not permitted at any time.

For remote access to YMWD hardware, all hardware configurations must be approved by YMWD.

All hosts that are connected to YMWD internal networks, via remote access technologies, must use up-to-date, anti-virus software applicable to that device or platform.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the YMWD production network must obtain prior approval from YMWD.

Virtual Private Network (VPN)

The purpose of this section is to provide guidelines for Remote Access IPsec or L2TP Virtual Private Network (VPN) connections to the YMWD corporate network. This applies to implementations of VPN that are directed through an IPsec Concentrator.

This applies to all YMWD employees, volunteers/directors, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPN's to access the YMWD network.

Approved YMWD employees, volunteers/directors, and authorized third parties (customers, vendors, etc.) may utilize the benefit of a VPN on a YMWD device, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying associated fees. Further details may be found in the Remote Access section.

The following guidelines will also apply:

- It is the responsibility of employees or volunteer/directors, with VPN privileges, to ensure that unauthorized users are not allowed access to YMWD internal

networks.

- VPN use is controlled using a multi-factor authentication paradigm.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.
- VPN gateways will be set up and managed by YMWD.
- All computers connected to YMWD internal networks via VPN or any other technology must use up-to-date, anti-virus software applicable to that device or platform.
- VPN users will be automatically disconnected from YMWD's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- Only YMWD approved VPN clients may be used.
- By using VPN technology, users must understand that their machines are an extension of YMWD's network and as such are subject to the same rules and regulations, as well as monitoring for compliance with this policy.

VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a YMWD approved VPN configured to drop all unauthenticated and unencrypted traffic and will be provisioned with split-tunneling disabled.

VPN Approval, Acceptable Use Review and Acceptance

Approval from the General Manager is required for a user's VPN access account creation.

Wireless Communications

Access to YMWD networks is permitted on wireless systems that have been granted an exclusive waiver by the General Manager for connectivity to YMWD's networks.

This section covers any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to YMWD's networks do not fall under the review of this policy.

Register Access Points and Cards

All wireless Access Points/Base Stations connected to the corporate network must be registered and approved by YMWD. If they are installed in corporate PCs, all wireless Network Interface Cards (i.e. PC cards) used in corporate laptop or desktop computers must be registered with YMWD.

Approved Technology

All wireless LAN access must use YMWD approved vendor products and security configurations.

Setting the Service Set Identifier (SSID)

The SSID shall be configured so that it does not contain any identifying information about

the organization, such as the company name, division title, employee name, or product identifier.

Policy 13: Password

Definitions

Application Administration Account: Any account that is for the administration of an application (i.e. SQL database administrator, etc.).

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant or deny access to private or shared data.

Strong Password: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about the password owner such as a birth date, social security number, and so on.

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of YMWD's entire corporate network. As such, all YMWD employees or volunteers/directors (including contractors and vendors with access to YMWD systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Audience

This policy applies to all personnel or volunteers/directors who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any YMWD facility, has access to the YMWD network, or stores any non-public YMWD information.

Policy Detail IR

User Network Passwords

Passwords for YMWD network access must be implemented according to the following guidelines:

- Recommend Password changes on a regular basis, every 90 days.
- Passwords should not be dictionary words or acronyms
- Passwords must adhere to a minimum length of 8 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits
- Passwords must not be easily tied back to the account owner such as: username, social security number, nickname, relative's names, birth date, etc.

System-Level Passwords

All system-level passwords must adhere to the following guidelines:

- Passwords must be changed at least every 6 months
- All administrator accounts must have 12 character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the Password Policy for the sake of ease of use

Password Protection

- The same password **must not** be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential YMWD information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, “my family name”).
- YMWD passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
 - Take control of the passwords and protect them
 - Report the discovery to the General Manager
- Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of YMWD. For an exception to be approved, there must be a procedure to change the passwords.
- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.

Policy 14: Patch Management

Overview

Patch Management at YMWD is required to mitigate risk to the confidential data and the integrity of YMWD's systems. Patch management is an effective tool used to protect against vulnerabilities, a process that must be done routinely, and should be as all-encompassing as possible to be most effective. YMWD must prioritize its assets and protect the most critical ones first; however, it is important to ensure patching takes place on all machines.

Purpose

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing YMWD at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.

Given the number of computer workstations and servers that comprise the YMWD network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches when they are made available. Effective security is a team effort involving the participation and support of every YMWD employee and the Board of Directors.

This policy is to assist in providing direction, establishing goals, enforcing governance, and to outline compliance.

Audience

This policy applies to all employees, contractors, consultants, temporaries, and the Board of Directors at YMWD. This policy applies to all equipment that is owned or leased by YMWD, such as, all electronic devices, servers, application software, computers, peripherals, routers, and switches.

Adherence to this policy is mandatory.

Policy Detail

Many computer operating systems, such as Microsoft Windows, Linux, and others, include software application programs which may contain security flaws.

Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the YMWD network, and all computers connected to it. Almost all operating systems and many software applications have periodic security patches, released by the vendor, that need to be applied. Patches, which are security related or critical in nature, should be installed as soon as possible.

- In the event that a critical or security related patch cannot be centrally deployed by IT, it must be installed in a timely manner using the best resources available.
- Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a violation of policy.

Responsibility

The General Manager is responsible for providing a secure network environment for YMWD. It is YMWD's policy to ensure all computer devices (including servers, desktops, printers, etc.) connected to YMWD's network, have the most recent operating system, security, and application patches installed.

Every user, both individually and within the organization, is responsible for ensuring prudent and responsible use of computing and network resources.

The General Manager is responsible for ensuring all known and reasonable defenses are in place to reduce network vulnerabilities, while keeping the network operating.

The General Manager and designees are responsible for monitoring security mailing lists, reviewing vendor notifications and Web sites, and researching specific public Web sites for the release of new patches. Monitoring will include, but not be limited to:

- Scheduled third party scanning of YMWD's network to identify known vulnerabilities
- Identifying and communicating identified vulnerabilities and/or security breaches to YMWD's General Manager
- Monitoring Computer Emergency Readiness Team (CERT), notifications, and Web sites of all vendors that have hardware or software operating on YMWD's network

The General Manager's designee is responsible for maintaining accuracy of patching procedures which detail the what, where, when, and how to eliminate confusion, establish routine, provide guidance, and enable practices to be auditable.

Documenting the implementation details provides the specifics of the patching process, which includes specific systems or groups of systems and the timeframes associated with patching.

Once alerted to a new patch, YMWD will download and review the new patch. The patch will be categorized by criticality to assess the impact and determine the installation schedule.

Policy 15: Physical Access Control

Definitions

Information systems: Is any combination of information technology and individuals' activities using that technology, to support operations management.

Display mechanisms: A monitor on which to view output from an information system.

Overview

Physical access controls define who is allowed physical access to YMWD facilities that house information systems, to the information systems within those facilities, and/or the display mechanisms associated with those information systems. Without physical access controls, the potential exists that information systems could be illegitimately physically

accessed and the security of the information they house could be compromised.

Purpose

This policy applies to all facilities of YMWD, within which information systems or information system components are housed. Specifically, it includes:

- Data centers or other facilities for which the primary purpose is the housing of IT infrastructure
- Data rooms or other facilities, within shared purpose facilities, for which one of the primary purposes is the housing of IT infrastructure
- Switch and wiring closets or other facilities, for which the primary purpose is not the housing of IT infrastructure

Policy Detail

Access to facilities, information systems, and information system display mechanisms will be limited to authorized personnel only.

Access to facilities will be controlled at defined access points of locked doors. Before physical access to facilities, information systems, or information system display mechanisms is allowed, authorized personnel are required to authenticate themselves at these access points. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility, without prior authorization, and all deliveries and removals will be logged.

A list of authorized personnel will be established and maintained so that newly authorized personnel are immediately appended to the list and those personnel who have lost authorization are immediately removed from the list. This list shall be reviewed and, where necessary, updated on at least an annual basis.

If visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified, and must have their authorization verified before physical access is granted. Once access has been granted, visitors must be escorted, and their activities monitored at all times.

Policy 16: Server Security

Definitions

File Transfer Protocol (FTP): *Is a standard Internet protocol for transmitting files between computers on the Internet.*

Overview

The servers at YMWD provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for YMWD. These hardware devices are vulnerable to attacks from outside sources which require due diligence to secure the hardware against such attacks.

Purpose

The purpose of this policy is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on YMWD's internal network(s) or related technology resources via any means. This can include, but is not limited to, the following:

- Internet servers (FTP servers, Web servers, Mail servers, Proxy servers, etc.)
- Application servers
- Database servers
- File servers
- Print servers
- Third-party appliances that manage network resources

This policy also covers any server device outsourced, co-located, or hosted at external/third-party service providers, if that equipment resides in the YMWD.org domain or appears to be owned by YMWD.

The overriding goal of this policy is to reduce operating risk. Adherence to the YMWD Server Security Policy will:

- Eliminate configuration errors and reduce server outages
- Reduce undocumented server configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect YMWD data, networks, and databases from unauthorized use and/or malicious attack

Therefore, all server equipment that is owned and/or operated by YMWD must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all YMWD company-owned, company operated, or company controlled server equipment. Addition of new servers, within YMWD facilities, will be managed at the sole discretion of IT. Non-sanctioned server installations, or use of unauthorized equipment that manage networked resources on YMWD property, is strictly forbidden.

Policy Detail

Responsibilities

YMWD's IT has the overall responsibility for the confidentiality, integrity, and availability of YMWD data.

Other IT staff members, under the direction of the Director of IT, are responsible for following the procedures and policies within IT.

Supported Technology

All servers will be centrally managed by YMWD and will utilize approved server configuration standards. Approved server configuration standards will be established and maintained by YMWD.

The following outlines YMWD's minimum system requirements for server equipment supporting YMWD's systems.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the General Manager.
- Access to services must be logged or protected through appropriate access

control methods.

- Security patches must be installed on the system as soon as possible through YMWD's configuration management processes.
- Trust relationships allow users and computers to be authenticated (to have their identity verified) by an authentication authority. Trust relationships should be evaluated for their inherent security risk before implementation.
- Authorized users must always use the standard security principle of "Least Required Access" to perform a function.
- System administration and other privileged access must be performed through a secure connection. Root is a user account that has administrative privileges which allows access to any file or folder on the system. Do not use the root account when a non-privileged account will do.
- All YMWD servers are to be in access-controlled environments.
- All employees are specifically prohibited from operating servers in environments with uncontrolled access (i.e. offices).

This policy is complementary to any previously implemented policies dealing specifically with security and network access to YMWD's network.

It is the responsibility of any employee of YMWD who is installing or operating server equipment to protect YMWD's technology based resources (such as YMWD data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to YMWD's public image.

Procedures will be followed to ensure resources are protected.

Policy 17: Systems Monitoring and Auditing

Overview

Systems monitoring and auditing, at YMWD, must be performed to determine when a failure of the information system security, or a breach of the information systems itself, has occurred, and the details of that breach or failure.

Purpose

System monitoring and auditing is used to determine if inappropriate actions have occurred within an information system. System monitoring is used to look for these actions in real time while system auditing looks for them after the fact.

This policy applies to all information systems and information system components of YMWD. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities
- Devices that provide centralized storage capabilities
- Desktops, laptops, and other devices that provide distributed computing capabilities
- Routers, switches, and other devices that provide network capabilities

- Firewall, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities

Policy Details

Information systems will be configured to record login/logout and all administrator activities into a log file. Additionally, information systems will be configured to notify administrative personnel if inappropriate, unusual, and/or suspicious activity is noted. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to the General Manager.

Information systems are to be provided with sufficient primary (on-line) storage to retain 30 days' worth of log data and sufficient secondary (off-line) storage to retain one year's worth of data. If primary storage capacity is exceeded, the information system will be configured to overwrite the oldest logs. In the event of other logging system failures, the information system will be configured to notify an administrator.

System logs shall be manually reviewed weekly. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel.

System logs are considered confidential information. As such, all access to system logs and other system audit information requires prior authorization and strict authentication. Further, access to logs or other system audit information will be captured in the logs.

Policy 18: Vulnerability Assessment

Overview

Vulnerability assessments, at YMWD, are necessary to manage the increasing number of threats, risks, and responsibilities. Vulnerabilities are not only internal and external, but there are also additional responsibilities and costs associated with ensuring compliance with laws and rules, while retaining business continuity and safety of YMWD and member data.

Purpose

The purpose of this policy is to establish standards for periodic vulnerability assessments. This policy reflects YMWD's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels.

This policy covers all computer and communication devices owned or operated by YMWD. This policy also covers any computer and communications device that is present on YMWD premises, but which may not be owned or operated by YMWD. Denial of Service testing or activities will not be performed.

Policy Detail

The operating system or environment for all information system resources must undergo a regular vulnerability assessment. This standard will empower YMWD to perform periodic security risk assessments for determining the area of vulnerabilities and to initiate appropriate remediation. All employees are expected to cooperate fully with any risk assessment.

Vulnerabilities to the operating system or environment for information system resources

must be identified and corrected to minimize the risks associated with them.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources
- Investigate possible security incidents and to ensure conformance to YMWD's security policies
- Monitor user or system activity where appropriate

To ensure these vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo an authenticated vulnerability assessment.

The frequency of these vulnerability assessments will be dependent on the operating system or environment, the information system resource classification, and the data classification of the data associated with the information system resource.

Retesting will be performed to ensure the vulnerabilities have been corrected. An authenticated scan will be performed by either a Third-Party vendor or using an in-house product.

All data collected and/or used as part of the Vulnerability Assessment Process and related procedures will be formally documented and securely maintained.

Policy 19: Workstation Configuration Security

Definitions

Domain: In computing and telecommunication in general, a domain is a sphere of knowledge identified by a name. Typically, the knowledge is a collection of facts about some program entities or a number of network points or addresses.

Overview

The workstations at YMWD provide a wide variety of services to process sensitive information for YMWD. These hardware devices are vulnerable to attacks from outside sources which require due diligence by YMWD to secure the hardware against such attacks.

Purpose

The purpose of this policy is to enhance security and quality operating status for workstations utilized at YMWD. Workstation users are expected to maintain these guidelines and to work collaboratively with YMWD resources to maintain the guidelines that have been deployed.

The overriding goal of this policy is to reduce operating risk. Adherence to the YMWD Workstation Configuration Security Policy will:

- Eliminate configuration errors and reduce workstation outages
- Reduce undocumented workstation configuration changes that tend to open up security vulnerabilities

- Facilitate compliance and demonstrate that the controls are working
- Protect YMWD data, networks, and databases from unauthorized use and/or malicious attack

Therefore, all new workstation equipment that is owned and/or operated by YMWD must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all YMWD company-owned, company operated, or company controlled workstation equipment. Addition of new workstations, within YMWD facilities, will be managed at the sole discretion of IT. Non-sanctioned workstation installations, or use of unauthorized equipment that manage networked resources on YMWD property, is strictly forbidden.

Responsibilities

YMWD's General Manager has the overall responsibility for the confidentiality, integrity, and availability of YMWD data.

Other designees, under the direction of the General Manager, are responsible for following the procedures and policies.

Supported Technology

All workstations will be centrally managed by YMWD and will utilize approved workstation configuration standards, which will be established and maintained by YMWD.

The following outlines YMWD's minimum system requirements for workstation equipment.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the General Manager.
- All patch management to workstations will be monitored through reporting with effective remediation procedures. YMWD has deployed a patch management process; reference the Patch Management Policy.
- All workstations joined to the YMWD domain will automatically receive a policy update configuring the workstation to obtain future updates from our desktop management system.
- All systems within YMWD are required to utilize anti-virus, malware, and data leakage protection. YMWD will obtain alerts of infected workstations and perform certain remediation tasks.
- All workstations will utilize the YMWD domain so that all general policies, controls, and monitoring features are enabled for each workstation. No system should be managed manually but should be managed through some central tool or model in order to efficiently manage and maintain system security policies and controls.

- Third-party applications, including browsers, shall be updated and maintained in accordance with the YMWD patch management program.
- Any critical security updates for all applications and operating systems need to be reviewed and appropriate actions taken by the Yuima to guarantee the security of the workstations in accordance with the YMWD patch management program.
- By default, all workstations joined to the YMWD domain will obtain local security settings through policies.

This policy is complementary to any previously implemented policies dealing specifically with security and network access to YMWD's network.

It is the responsibility of each employee of YMWD to protect YMWD's technology based resources from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to YMWD's public image. Procedures will be followed to ensure resources are protected.

Policy 20: Server Virtualization

Definitions

Virtualization: The creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device, or network resources.

Overview

This policy encompasses all new and existing workloads.

Purpose

The purpose of this policy is to establish server virtualization requirements that define the acquisition, use, and management of server virtualization technologies. This policy provides controls that ensure that Enterprise issues are considered, along with business objectives, when making server virtualization related decisions.

Platform Architecture policies, standards, and guidelines will be used to acquire, design, implement, and manage all server virtualization technologies.

Policy Detail

YMWD's General Manager has the overall responsibility for ensuring that policies are followed in order to establish contracts and the confidentiality, integrity, and availability of YMWD data.

YMWD's legacy IT practice was to dedicate one physical server to a single workload. The result of this practice was excessive server underutilization, an ever-expanding data center footprint, and excessive data center power consumption.

Server virtualization software allows the consolidation of new and existing workloads onto high capacity x86 servers. Consolidating workloads onto high capacity x86 servers allows YMWD to reduce the x86 server inventory, which in turn decreases the data center footprint and data center power consumption.

YMWD will migrate all new and existing workloads from physical servers to virtual machines. Hardware will be retired at such time as planned by the General Manager or required by incompatibility with Operating Systems (OS) and/or workload specific software updates.

Server Virtualization Requirements:

- Support industry-wide open-standards
- Embedded security technology, such as, Trusted Platform Module (TPM) or other technologies
- Single centralized management console
- Support industry standard management tools
- Support industry standard backup and recovery tools
- Interoperate with other platform technologies
- Support industry standard x86 hardware
- Support industry standard storage
- Support unmodified guest operating systems
- Functionality to support virtual server management network isolation
- Migrate running guests without interruption
- Add disks to a running guest
- Automatically detect a hardware failure and restart guests on another physical server
- Functionality to configure role based access for the administrative console
- Support Lightweight Directory Access Protocol (LDAP) for authentication and authorization for administrative console
- Encrypt all intra host and administrative console traffic
- Integrated graphical Central Processing Unit (CPU), memory, disk, and network performance monitoring, alerting, and historical reporting for hosts and guests
- Other industry standard or best in class features as required

Policy 21: Wireless (Wi-Fi) Connectivity

Definitions

Wireless Access Point (AP): A device that allows wireless devices to connect to a wired network using Wi-Fi or related standards.

Keylogger: The action of recording or logging the keystrokes on a keyboard.

Wi-Fi: A term for certain types of wireless local area networks (WLAN) that use specifications in the 802.11 family.

Wireless: A term used to describe telecommunications in which electromagnetic waves, rather than some form of wire, carry the signal over all or part of the communication path.

Purpose

The purpose of this policy is to secure and protect the information assets owned by YMWD and to establish awareness and safe practices for connecting to free and unsecured Wi-Fi, and that which may be provided by YMWD. YMWD provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. YMWD grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

Policy Detail

YMWD Wi-Fi Network

The YMWD Wi-Fi network is provided on a best-effort basis, primarily as a convenience to employees and others who may receive permission to access it. For employee business use, it is designed to be a supplement to, and not a substitute for, the production wired local area network. For non-employees, it is also provided as a convenience, primarily as a way for members to access YMWD online products and services. Staff may easily demonstrate YMWD online products and services to members or prospects. Wi-Fi access points, located at the Court Street facilities and in most branch offices, allow for compatible wireless device connectivity.

Microwaves, cordless telephones, neighboring APs, and other Radio Frequency (RF) devices that operate on the same frequencies as Wi-Fi are known sources of Wi-Fi signal interference. Wi-Fi bandwidth is shared by everyone connected to a given Wi-Fi access point (AP). As the number of Wi-Fi connections increase, the bandwidth available to each connection decreases and performance deteriorates. Therefore, the number and placement of APs in a given building is a considered design decision. Due to many variables out of direct YMWD control, availability, bandwidth, and access is not guaranteed.

The YMWD Wi-Fi network and connection to the Internet shall be:

- Secured with a passphrase and encryption, in accordance with current industry practice
 - Passphrases will be of appropriate complexity and changed at appropriate intervals, balancing security practice with the intended convenient business use of the Wi-Fi
- Physically or logically separate from the YMWD production wired local area network (LAN) and its resources
- Provided as a convenience for the use of YMWD employees, their vendors while visiting YMWD, the members of YMWD, and other visitors with YMWD's express permission via provision of an appropriate passphrase
- Optionally provided to members and qualifying visitors, by YMWD staff, with the provision of an appropriate passphrase and may be accessed only with the agreement to acceptable use policy statements provided online or in a written or verbal format

- Accessed by employees only in accordance with the Acceptable Use policy and its cross-referenced policies seen in Policy 1 in this document
- Used for access to the YMWD production LAN only for business use and with the approved use of a YMWD issued virtual private network (VPN) connection

YMWD's Wi-Fi service may be changed, the passphrase re-issued or rescinded, the network made unavailable, or otherwise removed without notice for the security or sustainability of YMWD business

Public Wi-Fi Usage

When using Wi-Fi on a mobile device in a public establishment, there are precautions that should be followed.

Do:

- As with any Internet-connected device, defend your laptop, tablet, phone, etc. against Internet threats. Make sure your computer or device has the latest antivirus software, turn on the firewall, never perform a download on a public Internet connection, and use strong passwords.
- Look around before selecting a place to sit, consider a seat with your back to a wall and position your device so that someone nearby cannot easily see the screen.
- Assume all Wi-Fi links are suspicious, so choose a connection carefully. A rogue wireless link may have been set up by a hacker. Actively choose the one that is known to be the network you expect and have reason to trust.
- Try to confirm that a given Wi-Fi link is legitimate. Check the security level of the network by choosing the most secure connection, even if you have to pay for access. A password-protected connection (one that is unique for your use) is better than one with a widely shared passphrase and infinitely better than one without a passphrase.
- Consider that one of two similar-appearing SSIDs or connection names may be rogue and could have been set up by a hacker. Inquire of the manager of the establishment for information about their official Wi-Fi access point.
- Avoid free Wi-Fi with no encryption. Even if your website or other activity is using https (with a lock symbol in your browser) or other secure protocols, you are at much greater risk of snooping, eavesdropping, and hacking when on an open Wi-Fi connection (such as at Starbuck's, McDonald's, some hotels, etc.).
- Seek out Wi-Fi connections that use current industry accepted encryption methods and that generally will require the obtaining of a passphrase from the establishment.
- Consider using your cell phone data plan for sensitive activities rather than untrusted Wi-Fi, or your own mobile hotspot if you have one or have been provided with one.
- If you must use an open Wi-Fi, do not engage in high-risk transactions or highly-confidential communication without first connecting to a virtual private network (VPN).
- If sensitive information absolutely must be entered while using a public network, limit your activity and make sure that, at a minimum, your web browser connection is encrypted with the locked padlock icon visible in the corner of the browser window, and make sure the web address begins with https://. If possible, save your financial transactions for when you are on a trusted and secured connection, at home, for instance. Passwords, credit card numbers, online banking logins, and

other financial information is less secure on a public network.

- Avoid visiting sites that can make it easier or more tempting for hackers to steal your data (for example, banking, social media, and any site where your credit card information is stored).
- If you need to connect to the YMWD network and are authorized to do so, choose a trusted and encrypted Wi-Fi AP or use your personal hotspot. In every case, you must use your YMWD-provided VPN at all times. The VPN tunnel encrypts your information and communications and besides, hackers are much less likely to be able to penetrate this tunnel and will prefer to seek less secure targets.
- In general, turn off your wireless network on your computer, tablet, or phone when you are not using it to prevent automatic connection to open and possibly dangerous APs. Set your device to not connect automatically to public or unknown and untrusted networks.

Finally,

Do Not:

- Leave your device unattended, not even for a moment. Your device may be subject to loss or theft, and even if it is still where you left it, a thief could have installed a keylogger to capture your keystrokes or other malware to monitor or intercept the device or connection.
- Email or originate other messages of a confidential nature or conduct banking or other sensitive activities, and definitely not when connected to an open, unencrypted Wi-Fi.
- Allow automatic connection to or connection to first Wi-Fi AP your device finds, as it may be a rogue AP set up by a thief. Rather, choose the one that is known to be the network you expect and have reason to trust.

RESOLUTION NO. 1960-24

**RESOLUTION OF THE BOARD OF DIRECTORS OF
YUIMA MUNICIPAL WATER DISTRICT
ADOPTING A WORKPLACE VIOLENCE PREVENTION PROGRAM**

WHEREAS, Senate Bill 553 was signed into law on September 20, 2023 and becomes effective July 1, 2024; and

WHEREAS, the District is required to adhere to the requirements and establish a Workplace Violence and Prevention Policy by July 1, 2024; and

WHEREAS, the Board of Directors wants to provide the tools and resources needed to protect the Staff and Customers of the District; and,

WHEREAS, it is in the best interest of the District to define a Workplace Violence and Prevention Program for the District and to establish the minimum requirements for the Program.

NOW, THEREFORE, BE IT RESOLVED by the Board of Directors of Yuima Municipal Water District that the Workplace Violence and Prevention Program, attached hereto, is hereby adopted.

PASSED AND ADOPTED at a regular adjourned meeting of the Board of Directors of YUIMA MUNICIPAL WATER DISTRICT held this 3rd day of June, 2024 by the following roll-call vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

Roland Simpson, President

Attest:

Don Broomell, Secretary

YUIMA MUNICIPAL WATER DISTRICT



Workplace Violence Prevention Plan

Yuima Municipal Water District's (YMWD) Workplace Violence Prevention Plan (WVPP) addresses the hazards known to be associated with the four types of workplace violence as defined by Labor Code (LC) section 6401.9.

Date of Last Review: June 3, 2024

Date of Last Revision(s): Initial Plan

DEFINITIONS

Emergency - Unanticipated circumstances that can be life threatening or pose a risk of significant injuries to employees or other persons.

Engineering controls - An aspect of the built space or a device that removes a hazard from the workplace or creates a barrier between the employee and the hazard.

Log - The violent incident log required by LC section 6401.9.

Plan - The workplace violence prevention plan required by LC section 6401.9.

Serious injury or illness - Any injury or illness occurring in a place of employment or in connection with any employment that requires inpatient hospitalization for other than medical observation or diagnostic testing, or in which an employee suffers an amputation, the loss of an eye, or any serious degree of permanent disfigurement, but does not include any injury or illness or death caused by an accident on a public street or highway, unless the accident occurred in a construction zone.

Threat of violence - Any verbal or written statement, including, but not limited to, texts, electronic messages, social media messages, or other online posts, or any behavioral or physical conduct, that conveys an intent, or that is reasonably perceived to convey an intent, to cause physical harm or to place someone in fear of physical harm, and that serves no legitimate purpose.

Workplace violence - Any act of violence or threat of violence that occurs in a place of employment.

Workplace violence includes, but is not limited to, the following:

- The threat or use of physical force against an employee that results in, or has a high likelihood of resulting in, injury, psychological trauma, or stress, regardless of whether the employee sustains an injury.

- An incident involving a threat or use of a firearm or other dangerous weapon, including the use of common objects as weapons, regardless of whether the employee sustains an injury.
- The four workplace violence types:

Type 1 violence - Workplace violence committed by a person who has no legitimate business at the worksite and includes violent acts by anyone who enters the workplace or approaches employees with the intent to commit a crime.

Type 2 violence - Workplace violence directed at employees by customers, clients, patients, students, inmates, or visitors.

Type 3 violence - Workplace violence against an employee by a present or former employee, supervisor, or manager.

Type 4 violence - Workplace violence committed in the workplace by a person who does not work there but has or is known to have had a personal relationship with an employee.

Workplace violence does not include lawful acts of self-defense or defense of others.

Work practice controls - Procedures and rules which are used to effectively reduce workplace violence hazards.

RESPONSIBILITY

The WVPP administrator, Amy Reeh, General Manager of YMWD, has the authority and responsibility for implementing the provisions of this plan for and approving any changes.

The General Manager, Operations Manager, and Finance and Administrative Services Manager are responsible for:

- Supporting, implementing, and maintaining the WVPP
- Answering employee questions regarding the WVPP
- Employee involvement and training; organizing safety meetings, updating training materials and handling reports of workplace violence.
- Emergency procedures and hazard identification; conducting safety inspections, coordinating emergency response procedures, and communicating with employees about the plan.

EMPLOYEE ACTIVE INVOLVEMENT

Employees are expected to participate in the identification, evaluation, and determination of correct measures, in order to prevent workplace violence.

All employees are encouraged to report incidents of threats or acts of physical violence.

All employees (including Managers) are responsible for:

- Their own behavior by interacting responsibly with fellow employees, supervisors, customers, and vendors
- Being familiar with YMWD policy regarding workplace violence
- Promptly reporting actual and/or potential acts of violence to appropriate authorities

- Cooperating fully in investigations/assessments of allegations of workplace violence
- Informing appropriate personnel about restraining or protective court orders related to domestic situations so that assistance can be offered at the workplace

Managers and Supervisors are responsible for:

- Informing employees of YMWD's workplace violence policy and program
- Taking all reported incidents of workplace violence seriously
- Investigating all acts of violence, threat, and similar disruptive behavior in a timely fashion and taking the necessary actions
- Providing feedback to employees regarding the outcome of their reports regarding violent or potentially violent incidents
- Requesting, where appropriate, assistance from functional area experts
- Being cognizant of situations that have the potential to produce violent behavior and promptly addressing them with all concerned parties
- Encouraging employees who show signs of stress or evidence of possible domestic violence to seek assistance
- Assuring, where needed, that employees have the time and opportunity to attend training (i.e. conflict resolution, stress management, etc.)
- Providing help to defuse violent situations
- Act as liaison with local authorities and law enforcement agencies
- Advise employees, if they inquire, of the procedures for reporting violent behavior
- Management will work with and allow employees and authorized employee representatives to participate in:
 - Identifying, evaluating, and determining corrective measures to prevent workplace violence: All employees are responsible for reporting hazards and injury or illness incidents including those related to workplace violence. Hazards and incidents must be immediately reported to the General Manager or the employee's immediate supervisor.
 - Designing and implementing training: Employees are encouraged to participate in designing and implementing training programs, and their suggestions are incorporated into the training materials.
 - Reporting and investigating workplace violence incidents.
- Management will ensure that all workplace violence policies and procedures within this written plan are clearly communicated and understood by all employees. Managers and supervisors will enforce the rules fairly and uniformly.
- All employees will follow all workplace violence prevention plan directives, policies, and

procedures, and assist in maintaining a safe work environment.

- The plan shall be in effect at all times and in all work areas and be specific to the hazards and corrective measures for each work area and operation.

EMPLOYEE COMPLIANCE

Our system to ensure that employees comply with the rules and work practices that are designed to make the workplace more secure, and do not engage in threats or physical actions which create a security hazard for others in the workplace, include at a minimum:

- Training employees, supervisors, and managers in the provisions of YMWD's Workplace Violence Prevention Plan (WVPP)
- Effective procedures to ensure that supervisory and nonsupervisory employees comply with the WVPP.
- Provide retraining to employees whose safety performance is deficient with the WVPP.
- Recognizing employees who demonstrate safe work practices that promote the WVPP in the workplace by rewarding employees through the Employee Recognition Program.
- Discipline employees for failure to comply with the WVPP via YMWD's "Discipline and Involuntary Terminations" section of the Employee Handbook.
- Employees will not be threatened with adverse action or retaliated against in any way if they refuse to report to or leave a workplace because they have a reasonable belief that the workplace is unsafe.
- Employees will not be prevented from accessing their mobile devices to seek emergency assistance or communicate with a person to verify their safety.

COMMUNICATION WITH EMPLOYEES

We recognize that open, two-way communication between management and staff about workplace violence issues is essential to a safe and productive workplace. The following communication system is designed to facilitate a continuous flow of workplace violence prevention information between management and staff in a form that is readily understandable by all employees, and consists of one or more of the following:

- New employee orientation includes workplace violence prevention policies and procedures.
- Review of our WVPP.
- Regularly scheduled meetings that address security issues and potential workplace violence hazards.
- Effective communication between employees and supervisors about workplace violence prevention and violence concerns including translation where appropriate.
- Posted or distributed workplace violence prevention information.
- Employees can anonymously report a violent incident, threat, or other violence concerns.
- Updates on the status of investigations and corrective actions are provided to employees through email and/or meetings. These updates could include information about the progress of investigations, the results of investigations, and any corrective actions taken.

WORKPLACE VIOLENCE INCIDENT REPORTING PROCEDURE

YMWD will implement the following effective procedures to ensure that:

- All threats or acts of workplace violence are reported to an employee's supervisor or manager, who will inform the WVPP administrator. Or employees may report incidents directly to the WVPP administrator, Amy Reeh, General Manager.
- Employees may report incidents verbally in person, by telephone via voice or text message, or by email.

A strict non-retaliation policy is in place, and any instances of retaliation will be dealt with swiftly and decisively up to and including disciplinary procedures or termination.

EMERGENCY RESPONSE PROCEDURES

YMWD has in place the following specific measures to handle actual or potential workplace violence emergencies:

- Effective means to alert employees of the presence, location, and nature of workplace violence emergencies by the following telephone, text, or in person.
- YMWD has evacuation or sheltering plans detailed in our Emergency Response Plan.
- How to obtain help from staff, security personnel, or law enforcement. This information is included in our Emergency Response Plan. If there is immediate danger, call for emergency assistance by dialing 911, and then notify the General Manager or other Manager if the General Manager is not available.

WORKPLACE VIOLENCE HAZARD IDENTIFICATION AND EVALUATION

The following policies and procedures are established and required to be conducted by YMWD to ensure that workplace violence hazards are identified and evaluated:

- Inspections shall be conducted when the plan is first established, after each workplace violence incident, and whenever the employer is made aware of a new or previously unrecognized hazard.

Periodic Inspections

Periodic inspections of workplace violence hazards will identify unsafe conditions and work practices. This may require assessment for more than one type of workplace violence. Periodic Inspections shall be conducted as needed.

Inspections for Type I (Violence by Strangers) workplace security hazards include assessing:

- The exterior and interior of the workplace for its attractiveness to robbers.
- The need for security surveillance measures, such as mirrors and cameras.
- Adequate lighting outside of and within facilities.
- Signage notifying the public that limited cash is kept on the premises and that cameras are recording all activities.
- Procedures for worker response during a robbery or other criminal act, including our policy prohibiting workers, who are not security guards, from confronting violent persons or persons committing a criminal act.
- Procedures for reporting suspicious persons or activities.

- Effective location and functioning of emergency buttons and alarms.
- Posting of emergency telephone numbers for law enforcement, fire, and medical services.
- Whether workers have access to a telephone with an outside line.
- The amount of cash on hand and use of time access safes for large bills.
- Whether workers have effective escape routes from the workplace.
- Whether doors to offices and rooms can be locked.
- Whether workers have a designated safe area where they can go to in an emergency.

Inspections for Type II (Violence by Customers/Clients) workplace security hazards include assessing:

- Access to, and freedom of movement within the workplace.
- Adequacy of workplace security systems, such as door locks, entry codes or badge readers, security windows, physical barriers, and restraint systems.
- Frequency and severity of threatening or hostile situations that may lead to violent acts by persons who are service recipients of our establishment.
- Workers' skill in safely handling threatening or hostile service recipients.
- Effectiveness of systems and procedures that warn others of a security danger or that summon assistance, e.g., alarms or panic buttons.
- The use of work practices such as the "buddy" system for specified emergency events.
- The availability of worker escape routes.

Inspections for Types III (Violence by Current or Past Coworkers) workplace security hazards include assessing:

- How well our establishment's anti-violence policy has been communicated to workers, supervisors, or managers.
- How well our establishment's management and workers communicate with each other.
- Our workers', supervisors', and managers' knowledge of the warning signs of potential workplace violence.
- Access to and freedom of movement within the workplace by non-workers, including recently discharged workers or persons with whom one of our workers is having a dispute.
- Frequency and severity of workers' reports of threats of physical or verbal abuse by managers, supervisors, or other workers.
- Any prior violent acts, threats of physical violence, verbal abuse, property damage or other signs of strain or pressure in the workplace.
- Worker disciplinary and discharge procedures.

Periodic inspections and reviews are performed according to the following schedule:

1. Prior to annual training
2. When we initially established our WVPP.
3. When new workplace security hazards are introduced into our workplace.
4. When new, previously unidentified workplace security hazards are recognized.
5. When workplace security incidents occur.
6. When we hire and/or reassign permanent or intermittent workers to processes, operations, or tasks for which a workplace security evaluation has not yet been conducted.
7. Whenever workplace security conditions warrant an inspection.

WORKPLACE VIOLENCE HAZARD CORRECTION

Hazards that pose a higher risk for violence in our workplace will be corrected in a timely manner, based on the severity of the hazards (with the higher risk situations having higher priority). Hazards will be corrected according to the following procedures:

1. When first observed or discovered.
2. If an imminent hazard exists that cannot be immediately abated without endangering

worker(s) and/or property, all exposed workers will be removed from the situation except those necessary to correct the existing condition. Workers necessary to correct the hazardous condition will be provided with the necessary protection.

3. All corrective actions taken and dates they are completed will be documented on the appropriate forms.

Workplace violence hazards will be evaluated and corrected in a timely manner. YMWD will implement the following effective procedures to correct workplace violence hazards that are identified:

- If an imminent workplace violence hazard exists that cannot be immediately abated without endangering employee(s) , all exposed employee(s) will be removed from the situation except those necessary to correct the existing condition. Employees needed to correct the hazardous condition will be provided with the necessary protection (i.e. PPE).
- All corrective actions taken will be documented and dated on the appropriate forms.
- Corrective measures for workplace violence hazards will be specific to a given work area.

Corrective measures for Type I (Violence by Strangers) workplace security hazards include the following:

- Improve lighting around and at the workplace.
- Provide emergency buttons to workers and install emergency alarms at the workplace.
- Establish a safe room with a lockable door.
- Utilize surveillance measures, such as cameras and mirrors, to provide information as to what is going on outside and inside the workplace and to dissuade criminal activity.
- Procedures for reporting suspicious persons, activities, and packages.
- Post emergency telephone numbers for law enforcement, fire, and medical services.
- Ensure workers have access to a telephone with an outside line.
- Post of signs notifying the public that limited cash is kept on the premises and that cameras are monitoring the facility.
- Limit the amount of cash on hand and use time access safes for large bills.
- Worker, supervisor, and management training on emergency action procedures.

Corrective measures for Type II (Violence by Customers/Clients) workplace security hazards include the following:

- Control access to the workplace and freedom of movement within it, that is consistent with business necessity.
- Ensure the adequacy of workplace security systems, such as door locks, security windows, physical barriers, and restraint systems.
- Provide worker training on recognizing and handling threatening or hostile situations that may lead to violent acts by persons who are service recipients of our establishment.
- Install effective systems to warn others of a security danger or to summon assistance, e.g., alarms or panic buttons.
- Provide procedures for a "buddy" system for specified emergency events.
- Ensure adequate worker escape routes.

Corrective measures for Types III (Violence by Current or Past Coworkers) workplace security hazards include the following:

- Effectively communicate our establishment's anti-violence policy to all workers, supervisors, or managers.
- Improve how well our establishment's management and workers communicate with each other.
- Increase awareness by workers, supervisors, and managers of the warning signs of potential workplace violence.
- Control, access to, and freedom of movement within, the workplace by non-workers, include

- recently discharged workers or persons with whom one of our workers is having a dispute.
- Provide counseling to workers, supervisors or managers who exhibit behavior that represents strain or pressure which may lead to physical or verbal abuse of co-workers.
- Ensure that all reports of violent acts, threats of physical violence, verbal abuse, property damage or other signs of strain or pressure in the workplace are handled effectively by management and that the person making the report is not subject to retaliation by the person making the threat.
- Ensure that worker disciplinary and discharge procedures address the potential for workplace violence.

PROCEDURES FOR POST INCIDENT RESPONSE AND INVESTIGATION

After a workplace incident, the WVPP administrator or their designee will implement the following post-incident procedures:

- Visit the scene of an incident as soon as safe and practicable.
- Interview involved parties, such as employees, witnesses, law enforcement, and/or security personnel.
- Review security footage of existing security cameras if applicable.
- Examine the workplace for security risk factors associated with the incident, including any previous reports of inappropriate behavior by the perpetrator.
- Determine the cause of the incident.
- Take corrective action to prevent similar incidents from occurring.
- Record the findings and ensure corrective actions are taken.
- Obtain any reports completed by law enforcement.
- The violent incident log will be used for every workplace violence incident and will include information, such as:
 - The date, time, and location of the incident.
 - The workplace violence type or types involved in the incident.
 - A detailed description of the incident.
 - A classification of who committed the violence, including whether the perpetrator was a client or customer, family or friend of a client or customer, stranger with criminal intent, coworker, supervisor or manager, partner or spouse, parent or relative, or another perpetrator.
 - A classification of circumstances at the time of the incident, including, but not limited to, whether the employee was completing usual job duties, working in poorly lit areas, rushed, working during a low staffing level, isolated or alone, unable to get help or assistance, working in a community setting, or working in an unfamiliar or new location.
 - A classification of where the incident occurred, such as in the workplace, parking lot or other area outside the workplace, or other area.

- The type of incident, including, but not limited to, whether it involved any of the following:
 - Physical attack without a weapon, including, but not limited to, biting, choking, grabbing, hair pulling, kicking, punching, slapping, pushing, pulling, scratching, or spitting.
 - Attack with a weapon or object, including, but not limited to, a firearm, knife, or other object.
 - Threat of physical force or threat of the use of a weapon or other object.
 - Sexual assault or threat, including, but not limited to, rape, attempted rape, physical display, or unwanted verbal or physical sexual contact.
 - Animal attack.
 - Other.
- Consequences of the incident, including, but not limited to:
 - Whether security or law enforcement was contacted and their response.
 - Actions taken to protect employees from a continuing threat or from any other hazards identified as a result of the incident.
 - Information about the person completing the log, including their name, job title, and the date completed.
- Reviewing all previous incidents.
- Determine if additional resources are needed, such as counseling services, time off work, and ensure they are provided to affected employees.

Ensure that no personal identifying information is recorded or documented on the incident log. This includes information which would reveal identification of any person involved in a violent incident, such as the person's name, address, electronic mail address, telephone number, social security number, or other information that, alone or in combination with other publicly available information, reveals the person's identity.

TRAINING AND INSTRUCTION

All employees, including managers and supervisors, will have training and instruction on general and job-specific workplace violence practices. These sessions could involve presentations, discussions, and practical exercises. Training and instruction will be provided as follows:

- When the WVPP is first established.
- Annually to ensure all employees understand and comply with the plan.
- Whenever a new or previously unrecognized workplace violence hazard has been identified and when changes are made to the plan. The additional training may be limited to addressing the new workplace violence hazard or changes to the plan.

YMWD will provide its employees with training and instruction on the definitions found on page 1 of this plan and the requirements listed below:

- The employer's WVPP, how to obtain a copy of the employer's plan at no cost, and how to participate in development and implementation of the employer's plan.
- How to report workplace violence incidents or concerns to the employer or law enforcement without fear of reprisal.
- Workplace violence hazards specific to the employees' jobs, the corrective measures YMWD has implemented, how to seek assistance to prevent or respond to violence, and strategies to avoid physical harm.
- The violent incident log and how to obtain copies of records pertaining to hazard identification, evaluation and correction, training records, and violent incident logs.
- Strategies to avoid/prevent workplace violence and physical harm, such as:
 - How to recognize workplace violence hazards including the risk factors associated with the four types of workplace violence.
 - Ways to defuse hostile or threatening situations.
- How to recognize alerts, alarms, or other warnings about emergency conditions and how to use identified escape routes or locations for sheltering.
- Employee routes of escape.
- Emergency medical care provided in the event of any violent act upon an employee.
- Post-event trauma counseling for employees desiring such assistance.

Note: *Employers must use training material appropriate in content and vocabulary to the educational level, literacy, and language of employees.*

EMPLOYEE ACCESS TO THE WRITTEN WVPP

YMWD ensures that the WVPP plan shall be in writing and shall be available and easily accessible to employees, authorized employee representatives, and representatives of Cal/OSHA at all times. This will be accomplished by making the plan available upon request.

RECORDKEEPING

YMWD will:

- Create and maintain records of workplace violence hazard identification, evaluation, and correction, for a minimum of five (5) years.
- Create and maintain training records for a minimum of one (1) year and include the following:
 - Training dates.
 - Contents or a summary of the training sessions.
 - Names and qualifications of persons conducting the training.
 - Names and job titles of all persons attending the training sessions.
- Maintain violent incident logs for minimum of five (5) years.

- Maintain records of workplace violence incident investigations for a minimum of five (5) years.
 - The records shall not contain medical information per subdivision (j) of section 56.05 of the Civil Code.
- All records of workplace violence hazard identification, evaluation, and correction; training, incident logs and workplace violence incident investigations required by LC section 6401.9(f), shall be made available to Cal/OSHA upon request for examination and copying.

EMPLOYEE ACCESS TO RECORDS

The following records shall be made available to employees and their representatives, upon request and without cost, for examination and copying within **15 calendar days of a request**:

- Records of workplace violence hazard identification, evaluation, and correction.
- Training records.
- Violent incident logs.

REVIEW AND REVISION OF THE WVPP

The YMWD WVPP will be reviewed for effectiveness:

- At least annually.
- When a deficiency is observed or becomes apparent.
- After a workplace violence incident.
- As needed.

Review and revision of the WVPP will include the procedures listed in the EMPLOYEE ACTIVE INVOLVEMENT section of this WVPP, as well as the following procedures to obtain the active involvement of employees and authorized employee representatives in reviewing the plan's effectiveness:

- Review of YMWD's WVPP should include, but is not limited to:
 - Review of incident investigations and the violent incident log.
 - Assessment of the effectiveness of security systems, including alarms, emergency response, and security personnel availability (if applicable).
- Review that violence risks are being properly identified, evaluated, and corrected. Any necessary revisions are made promptly and communicated to all employees. [These revisions could involve changes to procedures, updates to contact information, and additions to training materials.]

EMPLOYER REPORTING RESPONSIBILITIES

As required by California Code of Regulations (CCR), Title 8, Section 342(a). Reporting Work-Connected Fatalities and Serious Injuries, YMWD will immediately report to Cal/OSHA any serious injury or illness (as defined by CCR, Title 8, Section 330(h)), or death (including any due to Workplace Violence) of an employee occurring in a place of employment or in connection with any employment.

Amy Reeh, General Manager

Date

YUIMA MUNICIPAL WATER DISTRICT



Violent Incident Log

This report must be used for every workplace violence incident that occurs in our workplace. At a minimum, it will include the information required by LC section 6401.9(d).

The information that is recorded will be based on:

- Information provided by the employees who experienced the incident of violence.
- Witness statements.
- All other investigation findings.

All information that personally identifies the individual(s) involved will be omitted from this log, such as:
Names, Addresses – physical and electronic, Telephone numbers, Social security number

Date of Incident: _____

Time of Incident: _____

Location of Incident: _____

Workplace Violence Type: Check type according to definitions in plan.

- Type 1 – Stranger
- Type 2 – Customer or Vendor
- Type 3 – Current / Past Employee
- Type 4 – Personal Relationship

Check which of the following describes the type(s) of incident, and explain in detail:

- Physical attack without a weapon, including, but not limited to, biting, choking, grabbing, hair pulling, kicking, punching, slapping, pushing, pulling, scratching, or spitting.
- Attack with a weapon or object, including, but not limited to, a firearm, knife, or other object.
- Threat of physical force or threat of the use of a weapon or other object.
- Sexual assault or threat, including, but not limited to, rape, attempted rape, physical display, or unwanted verbal or physical sexual contact.
- Animal attack.
- Other _____

Provide a detailed description of the incident and any additional information on the violence incident type and what it included. Use a separate sheet of paper if necessary.

Workplace violence committed by: For confidentiality, only include the classification of who committed the violence, including whether the perpetrator was a client or customer, family or friend of a client or customer, stranger with criminal intent, coworker, supervisor or manager, partner or spouse, parent or relative, or other perpetrator.

Circumstances at the time of the incident: Detail what was happening at the time of the incident, including, but not limited to, whether the employee was completing usual job duties, working in poorly lit areas, rushed, working during a low staffing level, isolated or alone, unable to get help or assistance, working in a community setting, or working in an unfamiliar or new location.

Where the incident occurred: Where the incident occurred, such as in the workplace, parking lot or other area outside the workplace, or other area.

Consequences of the incident, including, but not limited to:

- Whether security or law enforcement was contacted and their response.
- Actions taken to protect employees from a continuing threat or from any other hazards identified as a result of the incident.

○ Were there any injuries? Yes or No. Please explain:

○ Were emergency medical responders other than law enforcement contacted, such as a Fire Department, Paramedics, On-site First-aid certified personnel? Yes or No. If yes, explain below:

Did the severity of the injuries require reporting to Cal/OSHA? If yes, document the date and time this was done, along with the name of the Cal/OSHA representative contacted.

This violent incident log was completed by:

Name: _____

Title: _____

Signature

Date

Senate Bill ([SB553](#)) was signed into law on September 20, 2023. The legislation addresses two primary areas, new workplace violence prevention requirements, effective **July 1, 2024**, and expanded temporary restraining orders, effective **January 1, 2025**.

This advisory focuses on the new workplace violence prevention requirements, which are required for most employers. The legislation places a strong emphasis on actively involving employees and employee representatives in the process. The primary components include:

- Conducting a hazard assessment to identify workplace violence exposures.
- Developing and implementing a written plan.
- Logging all workplace violent incidents.
- Conducting employee training.

Exemptions

The following employers, employees, and places of employment are exempt from these requirements:

- Those who are required to comply with [CCR 3342](#), Violence Prevention in Healthcare. This includes firefighters and other emergency responders when providing emergency medical services and medical transport.
- POST participating law enforcement agencies and the Department of Corrections.
- Employers with less than 10 employees and no public access.
- Employees teleworking from a location of the employee’s choice, which is not under the control of the employer.



Hazard Assessment

A hazard assessment must be conducted to identify and evaluate the workplace to help identify situations that may place employees at risk of workplace violence.

The SDRMA WPV Hazard Assessment & Correction form will assist the District with:

- Identifying risk factors that may increase the District’s vulnerability to workplace violence events.
- Identifying physical and process vulnerabilities.
- Developing a corrective action program.

Workplace Violence Prevention Plan

The written plan can be stand-alone or included in the District’s Injury & Illness Prevention Program. It must include the following elements:

- Person(s) responsible for implementing the program.
- Process for how employees and employee representatives will be involved.
- Methods to coordinate the program with other employers, where applicable.

WVPP Continued

- Procedures for accepting and responding to reports of workplace violence and prohibiting retaliation against the reporting employee.
- Plan compliance.
- Employee communication that includes how to report an incident without fear of reprisal, the investigation process, and how findings are shared.
- Response procedures to actual or potential workplace violence emergencies.
- Training requirements.
- Hazard assessment to identify and evaluate workplace violence hazards.
- Workplace violence hazard correction.
- Post incident response and investigation.
- Annual Plan effectiveness review.

Violent Incident Log

Every workplace violence incident must be recorded and include:

- Date, time, and location of the incident.
- The workplace violence type(s) and details, such as physical attack, threat, sexual assault, etc.
- Detailed description of the incident, without including any personal information from any person involved.
- Classification of who committed the violence, such as client, family, coworker, etc.
- Consequences of the incident including whether security or law enforcement was contacted, and actions taken to protect the employee.



The log must be reviewed at least annually and retained for five years.

Employee Training

Employees must receive initial training when the plan is first established and annually thereafter. Employees must have an opportunity for interactive questions and answers. The training must include:

- How to participate in the development and implementation of the plan and location of the written plan.
- Important definitions of workplace violence.
- How to report workplace violence incidents and concerns.
- Specific workplace violence hazards and corrective measures the employer has implemented.
- How to seek assistance to prevent or respond to violence.
- Strategies to avoid physical harm.
- Information about the Violent Incident Log.
- Additional training is required when a new or previously unrecognized workplace violence hazard has been identified and when changes are made to the program.
- Training records must be maintained for a minimum of one year as required by CCR3203, Injury & Illness Prevention Plan.

Resources

SDRMA [MemberPlus](#) – Risk Control Page WVP Resources:

- [Sample written plan](#)
- [Incident log](#)
- [Hazard Assessment form](#)

Cal/OSHA Resources:

- [WVP Employer Factsheet](#)
- [WVP Worker Factsheet](#)
- [All Cal/OSHA Publications](#)

INFORMATION / REPORTS



MONTHLY

REGULATORY ROUNDUP



MAY 2024

UPCOMING ACWA EVENTS

ACWA SPRING 2024 CONFERENCE

ACWA will host its 2024 Spring Conference and Exhibition in Sacramento, CA from May 7-9. ACWA Regulatory Committee Meetings will be held in person on Tuesday, May 7 (schedule below). Access to Tuesday’s committee meetings is complementary, but [registration](#) is required.

8:00 am – 9:15 am	Agriculture Committee
9:30 am – 10:45 am	Groundwater Committee
11:00 am – 12:15 pm	Water Management Committee
11:00 am – 12:15 pm	Energy Committee
1:45 pm – 3:00 pm	Water Quality Committee

POLICY UPDATES

FEDERAL

ACWA’s Federal Regulatory Issues chart is accessible [here](#).

WATER MANAGEMENT

Annual Water Supply and Demand Assessment

- On April 30, Department of Water Resources (DWR) held an informational meeting to discuss the next round of the [Annual Water Supply and Demand Assessment](#) (AWSDA). Urban water suppliers are required to submit an AWSDA to DWR through the [WUEdata Portal](#).
 - Deadline to submit AWSDA: July 1

Staff Contact

Chelsea Haines
chelseah@acwa.com

PRIORITY Bay-Delta Plan: Agreements to Support Healthy Rivers and Landscapes

- On March 29, the State Water Resources Control Board (State Water Board) posted additional documents (e.g., Flow Accounting Procedures, Non-flow Measure Accounting Protocols, Enforcement Agreements) received from the Agreements to Support Healthy Rivers and Landscapes (Agreements) parties on their [File Transfer Protocol](#) (FTP) site. To receive access to the FTP site, email SacDeltaComments@waterboards.ca.gov.

Staff Contact

Stephen Pang
stephenp@acwa.com



PRIORITY Bay-Delta Plan: Peer Review Package

- On March 29, the State Water Board also posted the [Peer Review Package](#) for the [Final Draft Scientific Basis Report Supplement in Support of Proposed Agreements for the Sacramento/Delta Update to the San Francisco Bay/Sacramento-San Joaquin Delta Water Quality Control Plan](#).

Staff Contact

Stephen Pang
stephenp@acwa.com






California Financing Coordinating Committee

- The California Financing Coordinating Committee is holding a [funding fair](#) to provide information on available grant, loan, and bond financing options for infrastructure projects from federal, state, and local agencies.
 - Funding Fair #1: May 23 from 9:00 am – 12:00 pm (virtual)
 - Funding Fair # 2: May 29 from 9:00 am to 12:00 pm (virtual)

Staff Contact

Chelsea Haines
chelseah@acwa.com

<p>California Nature Based Solutions</p> <ul style="list-style-type: none"> On April 22, the State unveiled 81 targets for nature-based solutions to use millions of acres to help absorb more carbon emissions. The targets call for actions by 2045 that are intended to reduce wildfire risk, boost healthy soils, store carbon, protect diversity, and conserve lands. California Natural Resources Agency (CNRA) will host a webinar on the targets. <ul style="list-style-type: none"> Webinar: May 2 from 12:00 – 1:00 pm 	<p>Staff Contact Chelsea Haines chelseah@acwa.com</p>
<p>California Water Plan: Resource Management Strategies</p> <ul style="list-style-type: none"> On May 1, DWR released a public review draft of its 11 Resource Management Strategies (RMS). Each RMS includes techniques, programs, or policies that can be used by local agencies and governments to meet their water-related management needs. <ul style="list-style-type: none"> Written comments due May 31 	<p>Staff Contact Stephen Pang stephenp@acwa.com</p>
<p>California Water Plan Update</p> <ul style="list-style-type: none"> On April 2, DWR released the final California Water Plan Update 2023 (Update 2023). Update 2023 is the State’s Strategic Plan for managing and developing water resources and focuses on addressing climate urgency, strengthening watershed resilience, and achieving equity in water management through recommendations that revolve around seven objectives. 	<p>Staff Contact Chelsea Haines chelseah@acwa.com</p>
<p>Dam Safety and Climate Resilience Local Assistance Program</p> <ul style="list-style-type: none"> On April 25, DWR announced the start of a second 15-day comment period for the updated Draft Dam Safety and Climate Resilience Local Assistance Program (DSCR) Guidelines and Proposal Solicitation Package. The DSCR provides State funding for repairs, rehabilitation, enhancements, and other dam safety projects at existing State jurisdictional dams and associated facilities that were in service prior to January 1, 2023. There is currently \$47.5 million available for this program. <ul style="list-style-type: none"> Written comments due May 10 	<p>Staff Contact Chelsea Haines chelseah@acwa.com</p>
<p>Delta Conveyance Project</p> <ul style="list-style-type: none"> On April 18, the State Water Board released a revised Notice of Petition Requesting Changes in Water Rights of DWR for the Delta Conveyance Project. The revised Notice extends the deadline to submit petition protests to the State Water Board, with a copy provided to DWR, from April 29 to May 13. <ul style="list-style-type: none"> Deadline to submit Petition Protest: May 13 	<p>Staff Contact Stephen Pang stephenp@acwa.com</p> 
<p>Drought Resilience Interagency and Partners Collaborative Report</p> <ul style="list-style-type: none"> On April 24, DWR published its inaugural Report on 2023 Activities for the Drought Resilience Interagency and Partners (DRIP) Collaborative. The report documents the DRIP Collaborative’s first year and highlights its focus on drought definition and narrative, drought-relevant data, and drought preparedness for domestic wells. For each area, the DRIP Collaborative identified challenges and proposed actions to address them. 	<p>Staff Contact Soren Nelson sorenn@acwa.com</p>
<p>Sacramento River Temperature Management Plan</p> <ul style="list-style-type: none"> On April 25, the State Water Board announced the availability of the Draft Sacramento River Temperature Management Plan (TMP) for 2024. The TMP describes how the U.S. Bureau of Reclamation plans to operate Shasta Reservoir for water temperatures on the Sacramento River. A final TMP is 	<p>Staff Contact Stephen Pang stephenp@acwa.com</p> 

<p>anticipated to be released on May 20. To receive access to the FTP site, email Bay-Delta@waterboards.ca.gov.</p>	
<p>Salton Sea Management Program</p> <ul style="list-style-type: none"> On March 26, the State Water Board issued a Notice of Annual Public Notice on the Statue of Phase 1 of the Salton Sea Management Program (SSMP). The State Water Board will receive an update on the SSMP from CNRA, in collaboration with DWR and the California Department of Fish and Wildlife. No action will be taken. <ul style="list-style-type: none"> Public Workshop: May 22 from 9:00 am – 7:00 pm 	<p>Staff Contact Chelsea Haines chelseah@acwa.com</p>
<p>Supply and Demand Assessment Program</p> <ul style="list-style-type: none"> On April 30, the State Water Board released a Notice of Public Meetings on Watershed Selection for the Division of Water Rights' Water Supply and Demand Assessment Program. At the meetings, State Water Board staff will solicit input on the selection of watersheds for new water supply and demand modeling efforts. <ul style="list-style-type: none"> Public Meeting #1: May 14 from 10:00 am - 12:00 pm in Eureka Public Meeting #2: May 21 from 1:00 - 3:00 pm in Salinas Public Meeting #3: June 3 from 1:00 - 3:00 pm (virtual) 	<p>Staff Contact Chelsea Haines chelseah@acwa.com</p>
<p>UPWARD Advisory Group</p> <ul style="list-style-type: none"> The State Water Board is convening the second UPWARD Advisory Group meeting to showcase granular aspects of the legacy data system (eWRIMS) and demonstrate ways the new CalWATRS system will provide new functionalities and improve data quality. <ul style="list-style-type: none"> Advisory Group meeting: May 1 from 1:00 – 3:00 pm 	<p>Staff Contact Chelsea Haines chelseah@acwa.com</p>
GROUNDWATER	
<p>Groundwater Sustainability Plan Determinations</p> <ul style="list-style-type: none"> On April 24, DWR announced the start of the public comment period for six revised groundwater sustainability plans (GSP) that were previously deemed incomplete. The GSPs are open to public comment for 60 days after their posted date. Information about how to comment on GSPs can be found in this fact sheet. 	<p>Staff Contact Soren Nelson sorenn@acwa.com</p>
<p>PRIORITY State Intervention: Tulare Lake Subbasin Probationary Designation</p> <ul style="list-style-type: none"> On April 16, the State Water Board adopted its Final Tulare Lake Subbasin Probationary Hearing Staff Report and designated the Tulare Lake Subbasin as probationary under the Sustainable Groundwater Management Act. The determination compels, among other things, the installation of well meters by groundwater users who extract more than 500 acre-feet per year by July 15, 2024. The State Water Board will next consider placing the Tule Subbasin in probation in September. 	<p>Staff Contact Soren Nelson sorenn@acwa.com</p> 
<p>State Intervention: Tule Subbasin Staff Report</p> <ul style="list-style-type: none"> On March 7, the State Water Board released a Notice of Opportunity to Provide Feedback, Public Staff Workshops, and Public Board Hearing for the Proposed Designation of Tule Subbasin as a Probationary Basin. The State Water Board will not decide on a probationary designation for Tule Subbasin prior to the Public Board Hearing, but it will accept input on the Tule Subbasin Probationary Hearing Draft Staff Report. 	<p>Staff Contact Soren Nelson sorenn@acwa.com</p>

- Written comments due May 7 at 12:00 pm
- Public Board Hearing: September 17 at 9:00 am

SAFE DRINKING WATER

SAFER Advisory Group

- On April 3, the State Water Board released a [Notice of Public Meeting](#) of the Safe and Affordable Funding for Equity and Resilience (SAFER) Advisory Group. The meeting will consider the 2024 Needs Assessment results, draft priorities for the Fund Expenditure Plan, SAFER program updates, SAFER Advisory Group announcements, and public comment.
 - Public Meeting: May 3 from 10:00 am – 3:00 pm

Staff Contact

Soren Nelson
sorenn@acwa.com



WATER QUALITY

2028 California Integrated Report for Clean Water Act

- On April 18, the State Water Board released a [Notice of Public Solicitation of Water Quality Data and Information for the 2028 California Integrated Report for Clean Water Act Sections 303\(d\) and 305\(b\)](#). Data and information submitted will be assembled, evaluated, and if appropriate, assessed to determine surface water quality conditions and to identify impaired waters. Minimum data elements and submission instructions can be found [here](#).
 - Deadline to submit data and information: October 23 by 12:00 pm

Staff Contact

Stephen Pang
stephenp@acwa.com

PRIORITY Hexavalent Chromium Maximum Contaminant Level

- On April 17, the State Water Board [adopted](#) the Hexavalent Chromium (Cr(VI)) Maximum Contaminant Level of 0.010 milligrams per liter (mg/L) (or 10 parts per billion). The Regulation, which applies to all water suppliers including small public water systems, must next be approved by the Office of Administrative Law. Once approved, it is expected that the Regulation will take effect by October.

Staff Contact

Nick Blair
nickb@acwa.com



Municipal Stormwater Cost Policy

- On April 2, the State Water Board released a [Notice of Opportunity for Public Comment and Public Board Hearing on a Revised Draft Water Quality Control Policy for Standardized Cost Reporting in Municipal Stormwater Permits](#). The [Draft Municipal Stormwater Cost Policy](#) (Draft Policy) proposed a statewide cost reporting framework for Phase I and traditional Phase II municipal separate storm sewer system permittees.
 - Release date of Revised Draft Policy and Staff Report: May 9
 - Public Hearing: June 4 at 9:00 am
 - Written comments due June 25 by 12:00 pm

Staff Contact

Stephen Pang
stephenp@acwa.com

ENERGY


2024 Integrated Energy Policy Report

- On April 17, the California Energy Commission (CEC) released a [Notice of Staff Workshop on Forms and Instructions to Collect Electricity Resource Plan Data from Load-Serving Entities](#) (LSEs). The CEC is directed by California Public Resources Code Section 25301 to regularly assess energy demand and supply to develop energy policies that conserve resources, protect the environment, ensure energy reliability, enhance the state’s economy, and protect public health and safety. Under the CEC’s regulations, LSEs are required to submit

Staff Contact

Nick Blair
nickb@acwa.com



<p>10-year demand forecasts and 10-year resource plans, which will be used to inform the 2024 IEPR Update.</p> <ul style="list-style-type: none"> ○ Staff Workshop: May 8 from 2:00 – 4:00 pm ○ Written comments due May 22 by 5:00 pm ○ Public workshops on specific topics: May 2024 – December 2024 	
<p>PRIORITY Advanced Clean Fleets</p> <ul style="list-style-type: none"> ● On April 23, the California Air Resources Board shared an informational post about the Advanced Clean Fleets (ACF) regulation. The post discusses the ACF calculator tool, which helps fleet owners project the number of zero-emission vehicles (ZEV) needed to comply with either the High Priority Fleets Model Year Schedule of the ZEV Milestones Option. The post also discusses Hybrid and Zero-Emission Truck and Bus Voucher Incentive Project (HVIP) incentive tools like the HVIP Vehicle Catalog and HVIP Purchaser Resources. 	<p>Staff Contact Nick Blair nickb@acwa.com</p> 
<p>California Clean Energy Planning Program</p> <ul style="list-style-type: none"> ● On April 23, the CEC held a pre-application workshop on the California Clean Energy Planning Program. \$500,000 is available to local government entities to develop land use planning documents that support or advance the development of clean energy. <ul style="list-style-type: none"> ○ Applications due June 3 by 11:59 pm 	<p>Staff Contact Nick Blair nickb@acwa.com</p>
<p>International Standard for Organization 15118</p> <ul style="list-style-type: none"> ● On April 17, the CEC released a Notice of International Standard for Organization (ISO) 15118 Implementation Updates Workshop. The purpose of the workshop is to support the electric vehicle charging industry’s continued implementation of interoperable charging communications and to provide an update on ISO 15118 developments. CEC staff will also summarize their February 2024 Updated Recommendation on ISO 15118 Ready Chargers. <ul style="list-style-type: none"> ○ Public Workshop: May 13 from 9:00 – 11:15 am ○ Written comments due May 31 by 5:00 pm 	<p>Staff Contact Nick Blair nickb@acwa.com</p>

ACWA COMMENT LETTERS

- [California Department of Fish and Wildlife Southern California Steelhead \(Oncorhynchus mykiss\) Status Review Submission to Commission](#), Fish and Game Commission, April 4, 2024

To receive a monthly email of the Regulatory Roundup, please contact [Sonja Eschenburg](#). The Regulatory Roundup is also available on ACWA's [website](#).



Indicates ACWA Working Group

Indicates ACWA Priority Issue



SUMMARY OF FORMAL BOARD OF DIRECTORS' MEETING APRIL 25, 2024

1. Adopt positions on various state bills:
 - The Board adopted a position of Support on S 2514, Colorado River Salinity Control Fix Act (Senator Bennet)
 - The Board adopted a position of Support on AB 2501 (Alvarez), relating to cutting the green tape.
 - The Board adopted a position of Support on AB 2610 (Garcia), relating to extended environmental coverage.

2. Design professional services contract with Hazen and Sawyer for design and engineering support services for the Moosa Canyon Pipeline Replacement project.

The Board awarded a design professional services contract, as attached, with such non-material modifications as approved by the General Manager or General Counsel, to Hazen and Sawyer for a not-to-exceed amount of \$5,644,936, to provide design and engineering support services for the Moosa Canyon Pipeline Replacement project, and authorized the General Manager, or designee, to execute the contract.

3. Monthly Treasurer's Report on Investments and Cash Flow.

The Board noted and filed the Treasurer's report.

4. Ordinance making amendments to Chapter 2.00.

The Board adopted Ordinance No. 2024-02, an ordinance of the Board of Directors of the San Diego County Water Authority making amendments to Chapter 2.00, Section 2.00.080(a) of the Administrative Code.

5. Designations for Emergency Assistance and Relief.

The Board adopted Resolution No. 2024-06, a Resolution of the Board of Directors of the San Diego County Water Authority to designate officers and employees authorized to execute certain disaster relief or emergency assistance documents.

6. Approval of Minutes.

The Board approved the minutes of the Formal Board of Directors' meeting of March 28, 2024.



SUMMARY OF FORMAL BOARD OF DIRECTORS' MEETING MAY 23, 2024

1. Monthly Treasurer's Report on Investments and Cash Flow.
The Board noted and filed the Treasurer's report.
2. Date change for September 2024 Board of Directors Regular Meeting.
The Board approved a date change for the Board of Directors September regular meeting from September 26, 2024, to September 19, 2024.
3. Finance Planning Work Group Recommendation for the Capital Improvement Program Appropriation for Fiscal Years 2024 and 2025.
The Board approved the FPWG recommendation to defer approximately \$13 million in infrastructure projects and to increase the Fiscal Years 2024 and 2025 CIP Board approved appropriation of \$183.9 million by \$7 million to support the critical bifurcation structures, to a new two-year appropriation of \$190.9 million.
4. Resolution setting a Public Hearing date and time for proposed Calendar Year 2025 Rates and Charges.
The Board adopted Resolution Number 2024-07 setting the time and place for a public hearing on June 27, 2024, at or after 9:00 a.m., or as soon thereafter as may practicably be heard, during the Administrative and Finance Committee meeting, to receive comments regarding the recommended rates and charges.
5. Liquidity Facility Supporting the Water Authority Tax-Exempt Commercial Paper Program.
The Board adopted Resolution 2024-08 authorizing the issuance and sale of short-term revenue certificates, approving Bank of America, N.A., as the liquidity provider for the Series 11 Commercial Paper Notes program and authorizing and approving certain actions in connection therewith.
6. Construction Contract with J.F. Shea Construction, Inc. for the Pipeline 5 Relining San Luis Rey Canyon Project.
The Board authorized the General Manager, or designee, to award a construction contract to J.F. Shea Construction, Inc. in the amount of \$47,913,795 for the Pipeline 5 Relining San Luis Rey Canyon Project.
7. Externally-funded Professional Services Contract with EcoTech Services, Inc., for the Large Landscape Direct Install Project within Disadvantaged Communities.
The Board awarded a professional services contract, with such non-material modifications as approved by the General Manager or General Counsel, with EcoTech Services, Inc., for a not-to-exceed amount of \$1.2 million, for the implementation and administration of the Large Landscape Direct Install Project through June 30, 2026, with the option to extend the contract term for up to one additional year, and authorized the General Manager, or designee, to execute the contract.



8. Adopt positions on various bills.
The Board adopted a position of Support on the federal “Drought Relief Obtained Using Government Help Today (DROUGHT)” Act, authored by Representative Scott Peters and Senator Padilla.
9. Adopt positions on various bills.
The Board adopted a position of Support on AB 1827 (Papan), relating to low water-use protection act – ensuring proportional water rates for all water users.
10. Approval of Minutes.
The Board approved the minutes of the Formal Board of Directors’ meeting of April 25, 2024.



Member Agency State Regulatory Monthly Update
Water Resources Department
April 2024

Making Conservation a California Way of Life Regulation (Elizabeth Lovsted)

In March, the State Water Resources Control Board (SWRCB) released a [revised draft regulation](#) for Making Conservation a California Way of Life. The revisions provide additional flexibility, a delayed compliance timeline, and alternative compliance pathways. The SWRCB held a public hearing to receive comments on the revised regulation on March 20, 2024. Staff from the Water Authority and the Association of California Water Agencies (ACWA) provided testimony at the hearing. The SWRCB intends to adopt the regulation this summer.

Per- and Polyfluoroalkyl Substances (PFAS) (Jesica Cleaver)

Drinking Water Regulation

On April 10, 2024, the United States Environmental Protection Agency (USEPA) announced the final [National Primary Drinking Water Regulation](#) for six PFAS. Five PFAS (PFOA, PFOS, PFHxS, PFNA, and HFPO-DA) have individual Maximum Contaminant Levels (MCLs). PFAS mixtures containing at least two or more of PFHxS, PFNA, HFPO-DA, and PFBS are regulated using a [Hazard Index](#) to account for the combined and co-occurring levels of these PFAS in drinking water.

Compound	Final MCL
PFOA	4 parts per trillion (ppt) (also expressed as ng/L)
PFOS	4 ppt
PFHxS	10 ppt
HFPO-DA (GenX Chemicals)	10 ppt
PFNA	10 ppt
Mixtures containing two or more of PFHxS, PFNA, HFPO-DA, and PFBS	1 (unitless) Hazard Index

The regulation requires:

- Public water systems (PWS) must complete initial monitoring by 2027, followed by ongoing compliance monitoring.
- PWS must provide the public with information on the levels of these PFAS in their drinking water beginning in 2027.
- Beginning in 2029, PWS that have PFAS in drinking water which violate one or more of these MCLs must take action to reduce levels of these PFAS in their drinking water and provide notification to the public of the violation.



Designation of PFOA and PFOS as Hazardous Substances

The USEPA has issued the [final rule](#) designating two types of PFAS (PFOA and PFOS) as hazardous substances under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA). CERCLA provides USEPA authority to clean up contaminated sites and imposes liability that includes a citizen-suit provision on parties responsible for the presence of hazardous substances at the sites. Consistent with CERCLA's objectives, the USEPA will focus on holding accountable parties that have played a significant role in the spread of PFAS into the environment, such as manufacturers of PFAS. The USEPA does not intend to pursue otherwise potentially responsible parties where equitable factors do not support seeking response actions or costs under CERCLA, including community water systems (CWS) and public owned treatment works (POTWs). Liability concerns remain, however, and there are efforts underway in the legislature to enact additional protections for CWS and POTWs.

2024 Interim Guidance on PFAS Removal and Destruction

The National Defense Authorization Act for Fiscal Year 2020 directed the USEPA to publish interim guidance on the destruction and disposal of PFAS and materials containing PFAS, and to update the guidance at least every three years. The USEPA has released an update to the 2020 interim guidance for public comment: the [2024 Interim Guidance on the Destruction and Disposal of PFAS Containing Materials](#). The guidance includes recommendations for the destruction and disposal of PFAS in drinking water and wastewater treatment residuals. The document also identifies key data gaps and uncertainties that must be resolved before the USEPA can issue more definitive recommendations about PFAS destruction and disposal technologies. The USEPA is accepting comments on the guidance document through **October 15, 2024**.

Public Health Goals for PFOA and PFOS in Drinking Water

On April 5, 2024, the California Office of Environmental Health Hazard Assessment (OEHHA) adopted [public health goals \(PHG\) for PFOA and PFOS](#) in drinking water. A PHG is the level of a drinking water contaminant at which adverse health effects are not expected to occur from a lifetime of exposure. The PHG of **0.007 parts per trillion (ppt) for PFOA** is based on kidney cancer in humans and the PHG of **1 ppt for PFOS** is based on liver and pancreatic tumors in laboratory animals. The SWRCB Division of Drinking Water (DDW) has identified the development of a drinking water standard for PFAS as a high priority. DDW will use the PHGs to develop drinking water standards for PFOS and PFOA that are as close to the PHG as possible but still technically and economically feasible for drinking water systems.

Adoption of Maximum Contaminant Levels for Hexavalent Chromium (Jessica Cleaver)

On April 17, 2024, the SWRCB adopted a [Maximum Contaminant Level \(MCL\) for Hexavalent Chromium](#) (Chromium-6). In 2014, the SWRCB adopted a MCL for Chromium-6 at 10 parts per billion (ppb) with a Detection Limit for Purposes of Reporting (DLR) of 1 ppb. However, that regulation was invalidated in 2017 by the Superior Court of Sacramento County because it found the state had not performed an adequate economic analysis. The new **MCL is also 10 ppb** with a lower **DLR of .1 ppb**. Once approved, the regulation is expected to become effective in October 2024. PWS with 10,000 or more connections will have two years to come into compliance with the new requirements, PWS with 1,000-9,999 connections will have three years, and PWS with less than 1,000 connections will be required to comply with the regulation within four years.

Proposed Recycled Water Permitting Fees (Mina Ziaei)

Last year, the California Legislature authorized a SWRCB and Regional Water Quality Control Board Budget Change Proposal to grant the Water Boards authority to assess fees for recycled water permitting. These fees would support additional staffing and other expenses to increase recycled water permitting in support of the Governor's Water Supply Strategy. On April 18, 2024, the SWRCB held a stakeholder meeting to discuss three potential fee structures: flat surcharge on all types of recycled water produced, surcharge by flow, or surcharge by type of



recycled water produced and flow. Comments on the proposed options can be sent to FeeBranch@waterboards.ca.gov through **May 2, 2024**. SWRCB staff will hold another stakeholder meeting **May 22, 2024**. The SWRCB tentatively plans to adopt the recycled water permit fee structure in September 2024.

2021 Lead and Copper Rule Revision (LCRR) Supporting Documents (Jessica Cleaver)

The USEPA has released several [supporting documents](#) to support water systems with the implementation of the [LCRR](#) including a frequently asked questions document for water systems, Tier 1 public notification template, and lead action level exceedance Tier 1 public notice factsheet. The LCRR became effective in December 2021, and compliance is required starting **October 16, 2024**, for the initial service line inventory, notification of service line material, Tier 1 public notification of a lead action level exceedance, and associated reporting requirements.

Advanced Clean Fleets (ACF) Regulation Amendments (Jessica Cleaver)

In March, California Air Resources Board (CARB) held a [workshop](#) to discuss potential amendments to the ACF regulation to implement the requirements of [Assembly Bill 1594 \(Garcia\)](#). CARB is seeking feedback from utilities on the amendments. In particular, CARB would like input on ideas for alternative end-of-life criteria for utility specialized vehicles for the Zero-Emission Vehicle (ZEV) Purchase & Daily Usage exemptions. The Association of California Water Agencies (ACWA) is advocating that the regulation should allow public water agencies to provide written justification for vehicles determined to be at the end-of-life, such as odometer reading, usage data (i.e. hours of stationary usage), vehicle reliability, availability and affordability of maintenance, etc. CARB is accepting informal comments on the amendments through **April 30, 2024**, at ZEVFleet@arb.ca.gov. CARB expects to finalize the amendments in late 2025.

Staff Contacts

Jessica Cleaver
JCleaver@sdcwa.org

Mina Ziaei
MZiaei@sdcwa.org

Elizabeth Lovsted
ELovsted@sdcwa.org



San Diego County Water Authority
And Its 24 Member Agencies

Adopted Bill Positions
4/25/24

OPPOSE	NOT FAVOR	SUPPORT/SPONSOR	FAVOR	WATCH/NEUTRAL	OPPOSE UNLESS AMENDED	SUPPORT IF AMENDED	PENDING
--------	-----------	-----------------	-------	---------------	-----------------------	--------------------	---------

STATE LEGISLATION

Measure	Author	Topic	Overview	Status	Position
AB 2257	Wilson	Relating to local government: property-related water and sewer fees and assessments: remedies.	This bill would prohibit, if a local agency complies with specified procedures, a person or entity from bringing a judicial action or proceeding alleging noncompliance with the constitutional provisions for any new, increased, or extended fee or assessment, as defined, unless that person or entity has timely submitted to the local agency a written objection to that fee or assessment that specifies the grounds for alleging noncompliance, as specified.	03/21/24-Amended and re-referred to committee on local government.	Support
AB 2409	Papan	Relating to Office of Planning and Research: permitting accountability transparency dashboard.	This bill would require the office, on or before January 1, 2026, to create and maintain, as specified, a permitting accountability transparency internet website (dashboard). The bill would require the dashboard to include a display for each permit to be issued by specified state agencies for all covered projects	04/16/24- Passed committee on A, P, and W; referred to committee on Appropriations.	Support
AB 2501	Alvarez	Water quality control plans: donations and grants.	This bill would authorize the state board, on behalf of itself or a regional board, to accept moneys from donations, grants, or contributions, or through contractual agreements, from public agencies, foundations, or other not-for-profit entities for the purpose of planning, permitting, or providing technical support for projects of public benefit, as defined, within the state board's or regional board's jurisdiction. The bill would require all funds received to be deposited, and separately accounted for, in the State Water Pollution Cleanup and Abatement Account, for expenditure in accordance with the terms of the donation, grant, contribution, or contractual agreement.	03/19/24- Passed committee on Environmental Safety and Toxic Materials; referred to committee on appropriations. Referred to suspense file (4/10).	Support
AB 2610	Garcia	Protected species: authorized take: System Conservation Implementation Agreement.	This bill would additionally authorize the department, if certain conditions are fulfilled, to authorize the take of species resulting from impacts attributable to implementation of any System Conservation Implementation Agreement between the United States Bureau of Reclamation and the Imperial Irrigation District to implement the Lower Colorado River Basin System Conservation and Efficiency Program, as provided, on the specified lands and bodies of water. This bill would declare that it is to take effect immediately as an urgency statute.	04/24/24-Passed appropriations committee.	Support
AB 2715	Boerner	Relating to Ralph M Brown Act: closed sessions.	This bill would additionally authorize a closed session to consider or evaluate matters related to cybersecurity, as specified, provided that any action taken on those matters is done in open session.	04/09/24-First hearing cancelled at request of the author.	Support

SB 1072	Padilla	Relating to local government: Proposition 218: remedies.	This bill would require, if a property-related fee or charge creates revenues in excess of the local government's reasonable cost of providing the specific benefit or specific government service, that the excess revenues be used only to reduce the subsequently adopted and following property-related fee or charge. The bill would declare that this provision is declaratory of existing law.	04/17/24-First hearing set for May 1 in committee on Local Government.	Support
SB 1147	Portantino	Relating to drinking water: bottled water: microplastics.	This bill would require, upon adoption by the State Water Resources Control Board of a primary drinking water standard for microplastics, any water-bottling plant that produces bottled water that is sold in this state to provide the State Department of Public Health's Food and Drug Branch an annual report on the levels of microplastics found in the source water used for bottling and in the final bottled water product that is offered for sale, as provided.	04/18/24-Passed committee on RLS; referred to Committee on Health	watch
SB 1218	Newman	Related to emergency water supplies.	This bill would declare that it is the established policy of the state to encourage and incentivize, but not mandate, the development of emergency water supplies, and to support their use during times of water shortage.	04/02/24-Hearing set for April 23 in Committee on N.R. & W.	Support
SB 1342	Atkins	California Environmental Quality Act: infrastructure projects: County of San Diego.	This bill would include the San Vicente Energy Storage Facility project proposed by the San Diego County Water Authority and a project for the repair, rehabilitation, or replacement of the South Bay Sewage Treatment Plant in the County of San Diego, operated by the International Boundary and Water Commission, as infrastructure projects, thereby providing the above-described streamlining benefits to those 2 projects. To the extent the bill would increase the duties of a lead agency regarding projects proposed by a third party, this bill would impose a state-mandated local program.	04/17/24-Passed committee and referred to committee on Appropriations.	Sponsor

FEDERAL LEGISLATION

S. 2514	Bennet	Colorado River Salinity Control Fix Act	This bill seeks to increase the federal cost-share for salinity control programs and research authorized in the Colorado River Basin Salinity Control Act of 1974.	07/26/23- Referred to the Committee on Agriculture, Nutrition, and Forestry.	Support
S. 3830	Padilla	Low-Income Household Water Assistance Program Establishment Act	This bill seeks to establish the Low-Income Household Water Assistance Program as a permanent program under the EPA's authority.	02/28/24- Referred to Committee on Health, Education, Labor, and Pensions.	Support

April 25, 2024

WHAT'S HOT REPORT

Government Relations Department
San Diego County Water Authority

Meggan Quarles
MQarles@SDCWA.org

Daniel Gaytan
DGaytan@SDCWA.org



**San Diego County
Water Authority**

What's Hot?

State Legislative Activity

The legislature and the Governor have approved early actions they hope will reduce the state shortfall by about \$17 billion. The package includes solutions that would enable final budget negotiations to focus on closing the shortfall while protecting core programs. Meanwhile, both chambers continue to work diligently in the policy committees to consider all outstanding legislation. Any bill with a fiscal impact must be considered and approved by their respective committee of jurisdiction by the April 26 deadline.

Federal Legislative Activity

Congress has fully shifted gears now to focusing on FY 2025. Just this week, House Appropriators released their guidance and deadlines for Community Project Funding and Programmatic/Language requests. As anticipated, a quick deadline was created meaning that entities seeking federal funding and member offices will have a matter of days to get their requests submitted and prioritized (more on this below). Furthermore, despite months of consideration, Speaker Johnson and the House of Representatives approved a significant foreign aid package which will appropriate \$95 billion to support Ukraine, Israel, and Taiwan. This bill was largely passed by Democrats with many Republicans voting against it. Speaker Johnson's support of the measure represents a dramatic evolution on the issue and a threat to his speakership. Many in his caucus see this as the third 'betrayal' to their values. We will see what consequences, if any, he will face for allowing this measure to move forward.



Speaker Johnson addressing reporters shortly after passage of the foreign aid package.

State Update

What's Happening Around Sacramento

State Water Board adopts Chrom 6 MCL

On Wednesday, April 17, 2024, the State Water Resources Control Board (State Water Board) voted to adopt the final maximum contaminant level (MCL) for hexavalent chromium (CrVI/ Chrom 6) of 10 micrograms per liter (parts per billion). The adoption also sets a detection limit for purposes of reporting at 0.1 ppb and prescribes a compliance plan for systems that exceed the MCL through regular monitoring.

Systems will have staggering compliance deadlines based on size. Water systems with more than 10,000 connections will have two years from the regulation's effective date to comply, water systems with more than 1,000 connections but fewer than 9,999 connections will have three years, and water systems with fewer than 1,000 connections will have four years. The next step is for State Water Board staff to submit the information to the California Department of Finance and then submit the final regulation to the Office of Administrative Law. The anticipated effective date is October 1, 2024.

Climate (Water) Bond

As previously discussed, legislators in the Assembly and Senate have introduced climate bonds which, as currently written, include billions of dollars in funding for water infrastructure projects. They are among the many large general obligation bonds currently being considered by the Legislature that are also seeking to fund school facilities and increased housing. The legislature and the Governor are cognizant that there will be limitations on how much bond funding they will be able to place on the November ballot. First and foremost, the state is currently facing a significant state budget deficit and is projected to do so in future years. This makes general obligation bonds both attractive and challenging since they avoid a significant hit to the General Fund in a budget year but result in significant ongoing expenses in future years. Second, the state must be cautious and ensure that it does not threaten its own creditworthiness by borrowing too much.

Finally, and perhaps most importantly, all general obligation bonds must be approved by voters. They may have their own limited appetite for the state taking on additional debt. For all of these reasons, Governor Newsom insisted that his mental health bond, Proposition 1, appear on the March Primary ballot by itself so that voters weren't tempted to choose one bond while rejecting another. Nevertheless, the Governor struggled to piece together the votes necessary to pass Proposition 1. While the race has been called and the bond has passed now, in the days

and weeks following the election the bond appeared in real jeopardy of failing. In order to qualify for the November ballot, per election guidelines, the legislature and the Governor must approve the climate bond measure by end of June.

Legislative Calendar

April 26: Last day for policy committees to hear and report to fiscal committees fiscal bills introduced in their house.

May 3: Last day for policy committees to hear and report to the Floor nonfiscal bills introduced in their house.

May 24: Last day for each house to pass bills introduced in that house.



Federal Update

What's Happening Around DC

WaterSMART Environmental Water Resources Projects

On April 18, the Bureau of Reclamation opened a grant opportunity for WaterSMART Environmental Water Resources Projects. This opportunity will close on June 18, 2024. The funding opportunity supports collaboratively developed projects that provide significant ecological benefits, including water conservation and efficiency projects, water management and infrastructure improvements, river and watershed restoration, and nature-based solutions implementation. Through WaterSMART, Reclamation leverages Federal and non-Federal funding to work cooperatively with States, Tribes, and local entities as they plan for and implement actions to increase water supply reliability through investments in existing infrastructure and attention to local water conflicts. I've linked to the grant NOFO [here](#).

EPA Action Designating PFAS as Hazardous Substances Under Superfund Program

On April 10, 2024, EPA announced the final National Primary Drinking Water Regulation (NPDWR) for six PFAS. To inform the final rule, EPA evaluated over 120,000 comments submitted by the public on the rule proposal, as well as considered input received during multiple consultations and stakeholder engagement activities held both prior to and following the proposed rule. EPA expects that over many years the final rule will prevent PFAS exposure in drinking water for approximately 100 million people, prevent thousands of deaths, and reduce tens of thousands of serious PFAS-attributable illnesses.

EPA is also making unprecedented funding available to help ensure that all people have clean and safe water. In addition to today's final rule, \$1 billion in newly available funding through the Bipartisan Infrastructure Law to help states and territories implement PFAS testing and treatment at public water systems and to help owners of private wells address PFAS contamination.

EPA finalized a National Primary Drinking Water Regulation (NPDWR) establishing legally enforceable levels, called Maximum Contaminant Levels (MCLs), for six PFAS in drinking water. PFOA, PFOS, PFHxS, PFNA, and HFPO-DA as contaminants with individual MCLs, and PFAS mixtures containing at least two or more of PFHxS, PFNA, HFPO-DA, and PFBS using a Hazard Index MCL to account for the combined and co-occurring levels of these PFAS in drinking water.

EPA also finalized health-based, non-enforceable Maximum Contaminant Level Goals (MCLGs) for these PFAS.

The final rule requires:

- Public water systems must monitor for these PFAS and have three years to complete initial monitoring (by 2027), followed by ongoing compliance monitoring. Water systems must also provide the public with information on the levels of these PFAS in their drinking water beginning in 2027.
- Public water systems have five years (by 2029) to implement solutions that reduce these PFAS if monitoring shows that drinking water levels exceed these MCLs.
- Beginning in five years (2029), public water systems that have PFAS in drinking water which violates one or more of these MCLs must take action to reduce levels of these PFAS in their drinking water and must provide notification to the public of the violation.

FY 2025 Appropriations- Community Project Funding (CPF) Request

On April 25, the House Appropriations Committee released guidance and a quick deadline with member offices for programmatic/language and Community Funding Projects. As expected, our delegation has established its deadlines for submitting funding requests only a few days out. Please see the table below and submit your appropriations request as soon as possible!

Office	CPF	Programmatic	Language	Deadline
Sen. Alex Padilla	Link	Link	Link	March 29
Sen. Laphonza Butler	n/a	Link	Link	March 27
Rep. Scott Peters	Link	Link	Link	March 27
Rep. Juan Vargas	n/a	Link	Link	n/a
Rep. Sara Jacobs	Link	Link	Link	April 29 (P&L)/ 30 (CPF)
Rep. Darrell Issa	Link	Link	Link	April 29
Rep. Mike Levin	Link	n/a	n/a	April 28

House Appropriations-Energy and Water Subcommittee Hearing

On April 10, the House Appropriations Committee – Energy and Water Subcommittee held a hearing entitled Member Day – Energy and Water Development, and Related Agencies. The purpose of the Member Day was to learn about water and energy priorities from non-Subcommittee Members of Congress from different areas and regions of the country. The witnesses included Congressman Jim Costa (D-CA), Congressman John Garamendi (D-CA), Congressman James C. Moylan (R-Guam), Congressman Kevin Mullin (D-CA), Congressman Greg Stanton (D-AZ), and Congressman Juan Ciscomani (R-AZ).

Rep. Stanton focused his opening remarks on the Colorado River basin, stressing the low water levels at Lake Powell and Lake Mead. He urged the Subcommittee to continue to direct

resources to the Bureau of Reclamation to meet its obligation under the drought contingency plan and critical conservation efforts.

Rep. Costa talked about the importance of the Water Operations Technical Support program (WOTS) and the Forecast-Informed Reservoir Operations program (FIRO). He stressed the need to better prepare the Army Corps and Bureau of Reclamation to utilize the latest weather and seasonal forecasting observations to better operate the water infrastructure in the West. He asked the Subcommittee to fund WOTS and FIRO and extend the programs beyond the Army Corps and to the Bureau of Reclamation. He also urged the Subcommittee to support the report language addressing the subsidence issues impacting the Friant-Kern, the Delta Mendota Canal, and the California Aqueduct Canal. He also asked the Subcommittee to support efforts and funding that support the San Joaquin River Restoration Program.

Rep. Ciscomani opened his remarks talking about the Colorado River and said Arizona “desperately needs the federal government support for its water conservation needs.” He pointed to the importance of the Operative Watershed Management Program (CWMP), and said the successful program needs more funding. He said while the program is authorized at about \$20 million annually, it has never received appropriations close to that level, and with the current water shortage in the West, “it’s high time that we invest in this program and other drought related programs before the situation becomes even worse.” He also urged the Subcommittee to put drought resiliency as a top priority as the Subcommittee works to put together its FY 2025 bill language.

Legislative Calendar

End of April: CPF requests are due.



May 23, 2024

WHAT'S HOT REPORT

Government Relations Department
San Diego County Water Authority

Meggan Quarles
MQuarles@SDCWA.org

Daniel Gaytan
DGaytan@SDCWA.org



**San Diego County
Water Authority**

What's Hot?

State Legislative Activity

Last week, about a third of the Legislature's 1,009 bills ended their journey to becoming a law in the Appropriations process. Many of these bills didn't have a chance given the state's current difficult fiscal outlook. Amid this, Governor Newsom released his revised budget proposal (more on this below) which ultimately seeks to cut about \$31 billion to close the remaining shortfall. The legislature and the Governor have until June 15 to negotiate and balance a state budget.

Federal Legislative Activity

In an unprecedented move, a majority of House Democrats and Republicans voted to save Speaker Johnson from the latest Motion to Vacate (MTV) that threatened his speakership. Democrats are thankful that Speaker Johnson put forth and ultimately helped pass a foreign aid package for our allies abroad. He did this despite vocal opposition from within his caucus and with a MTV already pending. With this MTV behind them, Congress was able to pass a bipartisan FAA Reauthorization bill while continuing to make progress on the Farm Bill, Foreign Intelligence Surveillance Act Reauthorization, Water Resources Development Act, and judicial nominations (in the Senate). This Thursday (5/23) the Senate also promised a vote on an already failed Border bill. With the election looming, it is questionable if Congress will be able to enact any major policy initiatives either before the election or in the lame duck period.



Governor Newsom presenting his revised budget proposal (May Revise).

State Update

What's Happening Around Sacramento

May Revise

Last week, Governor Newsom released his revised budget request. To balance the 2024-25 budget, Newsom has proposed dipping into reserves, canceling spending and cutting existing programs. For 2024-25 and 2025-26 combined, he's calling to cut \$19.1 billion in one-time spending plus \$13.7 billion in ongoing programs. Budget subcommittees in both the state Assembly and Senate have begun to hold hearings on Gov. Gavin Newsom's revised budget and given the massive deficit, will begin the difficult process to consider which departments or programs to cut or reduce.

In regard to water updates in the May revise, the governor is seeking the following:

- One-time reduction of \$500 million in water storage funds from Prop 1 in the 2025-2026 year.
- Governor Newsom made it clear the Delta Conveyance Project and fast-tracking Sites Reservoir are still top priorities, and the reduction in water storage funds will not immediately impact any projects in the pipeline.

The clock is ticking on the June 15 deadline for the Legislature and Governor to come up with a budget deal. Below is a high level overview of how the Governor would like to reduce the shortfall.

Governor's Budget 2024-25 Solutions

Category	Amount
Reserves	\$13.1 billion
Reductions	\$8.5 billion
Revenue/Borrowing	\$5.7 billion
Delays	\$5.1 billion
Fund Shifts	\$3.4 billion
Deferrals	\$2.1 billion
Total	\$37.9 billion

Climate (Water) Bond

Negotiations continue on the Climate Bond. Committees of jurisdictions in the Assembly and Senate are currently trying to find consensus around the size of the bond. There is talk that the proposed bond could be in the neighborhood of \$8 billion but nothing has yet been finalized. While time is running out to get a bond approved in time for a November ballot, legislators remain confident in their ability to achieve this deadline.

Something worth nothing, Governor Newsom made no mention of the Climate Bond during his May Revised budget and when pressed on this by reporters he reiterated his continued participation in negotiation on all three bond proposals (climate, housing, and schools). He also highlighted the preservation of most of the “climate commitment” and emphasized increased federal investments. It is unclear if the Governor’s commitment to a climate bond is fading.

Committee Actions

Three bills related to the Making Conservation a California Way of Life legislation and subsequent regulations were heard this week in the Senate Natural Resources and Water Committee. SB 1110 (Ashby) would have made changes to the current enforcement structure and SB 1330 (Archuleta) tried to address some of the LAO Report recommendations. However, the committee and chair felt like it was premature to move legislation addressing a pending regulation, so both bills were gutted — leaving only statutory changes to compliance dates. Senator Roger Niello, the author of a third bill on the topic (SB 1185), did not take the committee amendments and his bill was voted down.

Low Income Rate Assistance (LIRA) Proposal

The Community Water Center, Clean Water Action and Leadership Counsel for Justice and Accountability are seeking to establish a locally administered water low-income rate assistance program. The proposal seeks to authorize water districts to raise funds from ratepayers utilizing a voluntary opt out program in order to fund the program. CMUA has established a strike team to work on the language of the bill which is expected to be in print soon. We will provide more updates on this potential legislation as it continues to develop.

Legislative Calendar

May 24: Last day for each house to pass bills introduced in that house.

June 15: Budget bill must be passed by midnight

June 27: Last day for a legislative measure to qualify for November General Election ballot.



Federal Update

What's Happening Around DC

Farm Bill Negotiations

House Agriculture Committee Chair Glen Thompson fulfilled his promise to markup a new five-year farm bill by Memorial Day. Despite this, no final agreement is expected until after Election Day. You may remember that Congress enacted a one-year extension on the Farm Bill in November of 2023. That extension will end September 30, 2024.

The farm bill is an omnibus, multiyear law that governs an array of agricultural and food programs. It provides an opportunity for policymakers to address agricultural and food issues comprehensively and periodically. Nutritional programs (primarily the Supplemental Nutrition Assistance Program [SNAP]) are the largest components of the Farm Bill. Additionally, the Farm Bill addresses commodities, conservation, trade, government credits, rural development, research, forestry, energy, and crop insurance.

In an effort to mitigate drought in the west, Congress may evaluate how well Farm Bill conservation programs assist producers in achieving climate change-related goals. The current package authorizes the funding for voluntary conservation programs like the Conservation Reserve Program (CRP), the Environmental Quality Incentives Program (EQIP) and the Agricultural Conservation Easement Program (ACEP). The last Farm Bill modified the EQIP to allow the U.S. Department of Agriculture (USDA) to contract directly with irrigation districts and groundwater management districts to deliver water conservation practices, reducing the burden of enrolling for landowners. It is worth noting, however, that neither of these conservation programs are specific to climate change adaptation or mitigation, but they do have the flexibility to incorporate such measures in their structure.

The House and Senate Committees on Agriculture did release their respective farm bill summaries (Senate [Summary](#)/House [Summary](#)). Ahead of the markup, the Congressional Budget Office (CBO) provided a preliminary score for the bill and determined that Title I of the proposal could add between \$37 and \$39 billion to the deficit over the next decade. While Republicans are banking on significant savings from conservation programs, the CBO is less bullish on such savings.

Updated Cybersecurity Memorandum

The White House unveiled the [National Security Memorandum on Critical Infrastructure Security and Resilience](#), an update to an earlier memo. It establishes federal requirements and protocols for how the nation's critical infrastructure sectors manage cybersecurity. It is the latest federal action to address the vulnerabilities of U.S. critical infrastructure to cyber threats and attacks.

The memorandum's comprehensive protocols apply to the sixteen critical infrastructure sectors.

- The identified sectors include water and wastewater.
- The scope is a whole-of-government approach to establish minimum security standards, shared responsibility, and leverage expertise and technical innovation.
- The scope also addresses the growing interdependencies among sectors.

The memorandum outlines an extensive management structure to achieve its policy objective. The Department of Homeland Security (DHS) serves as the key coordinating entity with subgroups carrying out sector specific activities.

- The memo assigns a lead federal agency to each of the 16 sectors. The agency is charged with managing the day-to-day policy enforcement and management responsibilities.
- The U.S. Environmental Protection Agency (USEPA) is lead agency for water and wastewater infrastructure. The Department of Homeland Security is tasked with dams.
- The lead agencies will serve as Sector Risk Management Agencies (SRMAs) based upon expertise and understanding of the "unique" characteristics, operating models, and risk profiles related to cybersecurity.

Water Resources Development Act (WRDA)

On May 22, the Senate Environment and Public Works (EPW) Committee voted to pass the bipartisan Water Resources Development Act (WRDA) of 2024 by a unanimous vote.

Committee Chairman, Sen. Tom Carper (D-DE) said, "With strong, bipartisan support of WRDA 2024, the EPW Committee has come together to address the diverse water infrastructure needs of the American people. This year's reauthorization of the Water Resources Development Act directs the Corps to construct critical water infrastructure projects and continue vital flood risk management and ecosystem restoration programs – all while making our communities more resilient to extreme weather and creating good paying jobs. I look forward to the work ahead to get this important legislation to the President's desk." See [this committee document](#) for a full section-by-section overview of the bill.

Legislative Calendar

May 25- June 2: District Work Period (House).

May 27-31: State work period (Senate).



YUIMA MUNICIPAL WATER DISTRICT
2023-24 Capital Projects
As of April 30, 2024

	Approved 2023-24 Budget	Approved Budget Carry Forward	Current Year Expenditures 2023-24	Prior Year Expenditures Forward	Total Project Expenditures
GENERAL DISTRICT 10-600-60					
McNally Tank 2 Interior and Exterior Recoating		\$ 450,000		\$ -	\$ -
AMR Meter Replacement			\$ 2,254	\$ 6,112	\$ 8,365
Line Locator			\$ 5,041	\$ -	\$ 5,041
T-Y Well 1 Pump Station <small>10-600-60-6300-614</small>			\$ 384,316	\$ 184,683	\$ 569,000

Total General District Capital Projects - 2023-24		\$ 450,000	\$ 391,610	\$ 190,795	\$ 582,405
----------------------------------------------------------	--	-------------------	-------------------	-------------------	-------------------

IMPROVEMENT DISTRICT A 20-600-60					
Pump Station 4 Pump Cover		\$ 20,000	\$ -	\$ -	\$ -
Pump Station 4 Bypass Valve		\$ 9,764	\$ -	\$ -	\$ -
Dunlap CL2 Analyzer Building Replacement		\$ 10,000	\$ -	\$ -	\$ -
Well 14 Pump			\$ 29,920	\$ -	\$ 29,920
Well 22 Pump			\$ 15,725	\$ -	\$ 15,725
AMR Meter Replacement			\$ 3,751	\$ 5,557	\$ 9,308

Total IDA Capital Projects - 2023-24		\$ 39,764	\$ 49,396	\$ 5,557	\$ 54,953
---------------------------------------------	--	------------------	------------------	-----------------	------------------

Total General District & IDA Capital Projects 2023-24	\$ -	\$ 489,764	\$ 441,006	\$ 196,352	\$ 637,358
------------------------------------------------------------------	-------------	-------------------	-------------------	-------------------	-------------------

RAINFALL RECORD 2023/2024 YUIMA SHOP

Location: 34928 Valley Center Road, Pauma Valley @ 1050' elevation

	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	
1				0.06				1.24	0.32				
2								0.65	0.20				
3							0.29	0.01	0.03				
4								0.01		0.03			
5								1.21	0.25	0.41			
6								0.80	0.53	0.01			
7								0.27					
8								0.10					
9								0.22					
10													
11				0.03									
12													
13			0.01							0.13			
14			0.01							0.07			
15					0.62		0.08		0.30	0.01			
16									0.03				
17					0.47								
18						0.01							
19					0.01	0.01							
20		1.72				0.03	0.38	0.34					
21							0.53	0.15					
22						0.46	1.28			0.01			
23				0.01			0.01		0.22	0.07			
24					0.02				0.15				
25				0.01						0.02			
26				0.01									
27													
28													
29					0.16								
30			0.14		0.13	0.07			1.43				
31						0.01			1.32				TOTAL YEAR
TOTALS	0.00	1.72	0.16	0.12	1.41	0.59	2.57	5.00	4.78	0.76	0.00	0.00	17.11
1987/88 (B)	0.00	0.00	0.00	2.60	4.17	1.20	2.97	2.23	0.97	6.95	0.40	0.00	21.49
1988/89 (B)	0.00	1.25	0.00	0.00	1.36	4.78	1.38	3.25	0.60	0.25	0.43	0.00	13.30
1989/90 (B)	0.00	0.00	1.03	0.50	0.00	0.55	4.45	2.65	0.92	3.22	0.95	1.10	15.37
1990/91	0.32	0.93	0.00	0.16	0.83	0.85	1.30	2.60	13.10	0.20	0.00	0.00	20.29
1991/92	0.70	0.00	0.40	0.85	0.30	1.90	3.25	5.60	5.30	0.15	0.50	0.00	18.95
1992/93	0.00	1.75	0.00	1.55	0.00	5.10	17.25	8.60	1.55	0.00	0.00	0.70	36.50
1993/94	0.00	0.00	0.00	0.25	2.35	0.90	1.20	4.60	5.30	2.00	0.20	0.00	16.80
1994/95	0.00	0.00	0.00	0.40	0.80	0.75	9.35	3.00	9.40	2.00	0.75	1.10	27.55
1995/96	0.10	0.00	0.00	0.00	0.20	0.85	1.50	3.50	2.30	0.50	0.00	0.00	8.95
1996/97	0.00	0.00	0.00	0.00	4.55	2.40	6.35	0.75	0.00	0.00	0.00	0.00	14.05
1997/98	0.00	0.00	2.10	0.10	2.45	2.10	3.70	10.95	4.05	3.30	3.05	0.15	31.95
1998/99	0.00	0.00	1.15	0.00	2.45	1.36	1.93	1.00	0.80	2.32	0.05	0.50	11.56
1999/2000	0.25	0.00	0.10	0.00	0.10	0.25	0.60	5.20	1.55	0.95	0.45	0.00	9.45
2000/2001	0.00	0.00	0.05	0.98	0.45	0.00	2.80	6.20	1.70	1.70	0.50	0.00	14.38
2001/2002	0.00	0.00	0.00	0.00	1.35	1.90	0.60	0.15	1.80	0.65	0.00	0.00	6.45
2002/2003	0.00	0.00	0.20	0.00	2.85	3.60	0.25	6.40	3.45	2.10	0.65	0.00	19.50
2003/2004	0.00	0.40	0.00	0.00	1.55	1.55	0.70	4.25	0.75	1.05	0.00	0.00	10.25
2004/2005	0.00	0.40	0.00	7.20	1.55	4.55	8.70	6.60	1.75	1.05	0.10	0.00	31.90
2005/2006	0.50	0.00	0.10	1.85	0.00	0.50	1.75	2.45	3.55	2.65	0.50	0.00	13.85
2006/2007	0.00	0.20	0.30	0.40	0.05	1.40	0.50	2.70	0.30	0.80	0.10	0.00	6.75
2007/2008	0.00	0.25	0.00	0.20	0.50	5.30	5.80	3.80	0.60	0.00	1.00	0.00	17.45
2008/2009	0.00	0.00	0.00	0.00	1.60	4.95	0.05	4.45	0.30	0.75	0.00	0.00	12.10
2009/2010	0.00	0.00	0.00	0.00	1.10	3.65	7.45	4.00	0.55	2.60	0.00	0.00	19.35
2010/2011	0.20	0.00	0.00	3.15	1.45	8.60	1.25	4.40	2.65	0.30	0.40	0.05	22.45
2011/2012	0.00	0.00	0.15	0.65	2.65	1.20	1.15	2.05	2.25	3.15	0.10	0.00	13.35
2012/2013	0.00	0.00	1.50	0.40	0.45	2.70	1.50	1.25	1.70	0.10	0.40	0.00	10.00
2013/2014	0.28	0.00	0.00	1.48	0.15	0.40	0.25	0.95	2.95	0.80	0.00	0.00	7.26
2014/2015	0.00	0.20	1.00	0.00	1.00	4.90	0.70	0.90	1.60	0.75	1.20	0.50	12.75
2015/2016	1.90	0.30	1.70	0.35	0.90	2.65	3.40	1.15	1.50	0.75	0.40	0.00	15.00
2016/2017	0.00	0.00	1.00	0.16	1.75	4.37	7.17	6.05	0.20	0.00	1.34	0.00	22.04
2017/2018	0.07	0.12	0.13	0.00	0.00	0.00	3.18	0.88	2.55	0.01	0.12	0.00	7.06
2018/2019	0.00	0.00	0.00	1.27	2.51	1.63	2.34	7.98	1.68	0.40	1.83	0.12	19.76
2019/2020	0.00	0.00	0.30	0.00	4.17	2.46	0.17	0.64	5.39	5.96	0.03	0.20	19.32
2020/2021	0.00	0.00	0.00	0.07	1.52	0.79	1.09	0.06	1.55	0.51	0.10	0.02	5.71
2021/2022	1.27	0.30	0.17	0.99	0.00	4.16	0.31	0.53	2.26	0.20	0.19	0.00	10.38
2022/2023	0.00	0.00	1.31	0.55	1.96	1.48	8.01	1.02	5.87	0.04	0.67	0.33	21.24
35 Year Average	0.16	0.17	0.36	0.75	1.40	2.45	3.27	3.51	2.65	1.38	0.47	0.14	16.70

Yuima Municipal Water District - Production/Consumption Report

YUIMA GENERAL DISTRICT	FISCAL				CALENDAR	
	Apr-24	Mar-24	2023-24	2022-23	2024	2023
Produced and Purchased Water						
11-1590 IDA	0.0	0.0	0.0	22.0	0.0	0.0
10-1009 SDCWA	101.9	17.4	2822.5	3729.0	273.7	3450.9
10-2101 TY WELL 1	57.3	48.0	108.9	0.0	108.9	0.0
Total Produced and Purchased	159.2	65.4	2931.4	3768.3	382.6	3451.1
Consumption						
CUSTOMERS GENERAL DISTRICT	103.8	51.4	1215.5	1393.0	239.1	1326.1
10-2100 TAP 1	9.3	3.0	630.2	803.8	44.0	804.7
10-1590 TAP 2	27.1	2.4	548.9	983.7	38.8	667.9
10-1200 TAP 3	25.3	9.7	580.0	656.8	70.8	709.3
Total Consumption - Yuima	165.5	66.5	2974.6	3837.3	392.7	3508.0
Storage Level Changes	8.5	0.7	14.8	-3.2	8.6	6.3
Slippage - Acre Feet	2.2	-0.4	-28.4	-72.2	-1.5	-50.6
Slippage %	1.4	-0.6	-1.0	-1.9	-0.4	-1.5
IMPROVEMENT DISTRICT "A"						
Produced Strub Zone Wells						
20-2012 RIVER WELL 12	17.5	9.3	238.0	240.5	50.8	285.3
20-2091 RIVER WELL 19A	22.9	12.2	278.9	242.1	62.7	324.3
20-2020 RIVER WELL 20A	20.6	10.9	279.7	248.0	60.0	338.9
20-2025 RIVER WELL 25	0.0	0.0	167.8	137.3	0.0	184.8
20-2022 FAN WELL 22	11.1	4.3	109.7	157.5	15.4	154.3
Total Produced Strub Zone Wells	72.1	36.7	1074.1	1025.4	188.9	1287.6
Produced Fan Wells						
20-2014 WELL 14	0.3	0.0	67.4	105.8	0.5	68.2
20-2017 WELL 17	0.1	0.1	66.8	55.4	4.8	85.6
20-2023 WELL 23	0.0	0.0	0.0	0.0	0.0	0.0
20-2024 WELL 24	0.0	0.2	0.6	42.5	0.2	0.7
20-2029 WELL 29	0.1	0.1	81.1	86.0	3.2	106.0
20-20410-500 HORIZONTAL WELLS	14.2	13.7	130.2	146.7	54.1	163.3
Code K Usage WELL USE AGREEMENTS ("K")	9.4	1.6	207.7	204.7	20.3	263.9
Total Produced Fan Wells	24.1	15.7	553.8	656.6	83.1	687.7
Total Produced Strub and Fan Wells	96.2	52.4	1627.9	1682.0	272.0	1975.3
Purchased Water						
10-2100 TAP 1	9.3	3.0	630.2	803.8	44.0	804.7
90 minus 20-2008 TAP 2	27.1	2.4	548.9	983.5	38.8	667.7
10-1200 TAP 3	25.3	9.7	580.0	656.8	70.8	709.3
Total Purchased Water	61.7	15.1	1759.1	2444.1	153.6	2181.7
Total Produced and Purchased	157.9	67.5	3387.0	4126.1	425.6	4157.0
Consumption						
CUSTOMERS IDA	124.5	46.3	3101.2	3820.0	339.0	3825.2
Interdepartmental to Y	0.0	0.0	0.0	22.0	0.0	0.0
Total Consumption - IDA	124.5	46.3	3101.2	3842.0	339.0	3825.2
Storage Level Changes	-5.2	-0.1	-1.1	0.6	-2.9	2.5
Slippage - Acre Feet	28.2	21.1	284.7	284.7	83.7	334.3
Slippage %	17.9	31.3	8.4	6.9	19.7	8.0
Combined General District and IDA						
PRODUCED YUIMA	159.2	65.4	2931.4	3768.3	382.6	3451.1
PRODUCED IDA	96.2	52.4	1627.9	1682.0	272.0	1975.3
Total Produced and Purchased	255.4	117.8	4559.3	5450.3	654.6	5426.4
Consumption	228.3	97.7	4316.7	5235.0	578.1	5151.3
Storage Level Changes	3.3	0.6	13.7	-2.6	5.7	8.9
Slippage - Acre Feet	30.4	20.7	256.3	212.5	82.2	283.8
Slippage %	11.9	17.6	5.6	3.9	12.6	5.2

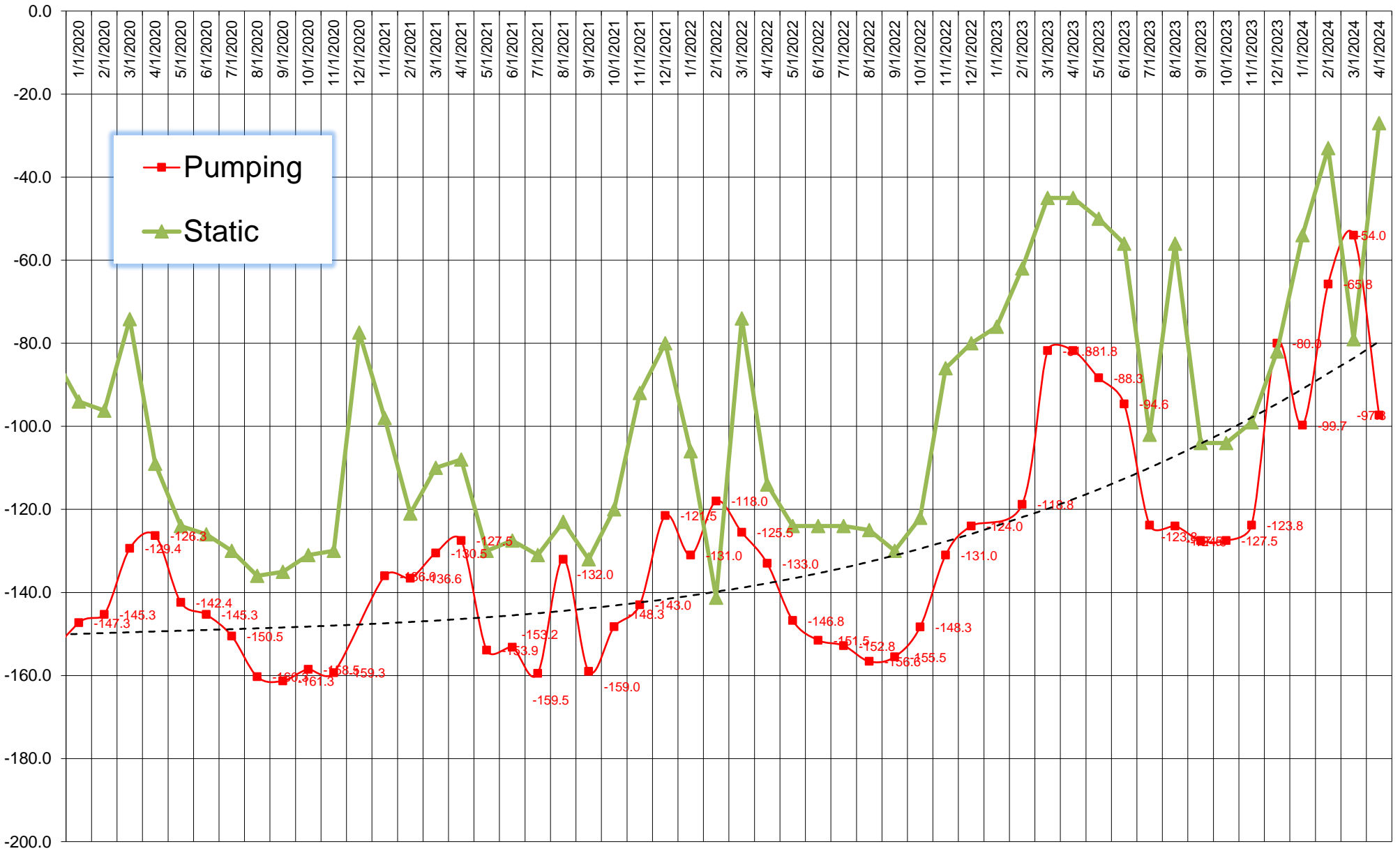
Notes: Horizontal Well to the creek 14.2 acft Dunlap Tank leak 7.5 acft Tank 1 flush 0.3 acf Wells 14,17,29 flushed 0.5 acft

YUIMA MUNICIPAL WATER DISTRICT

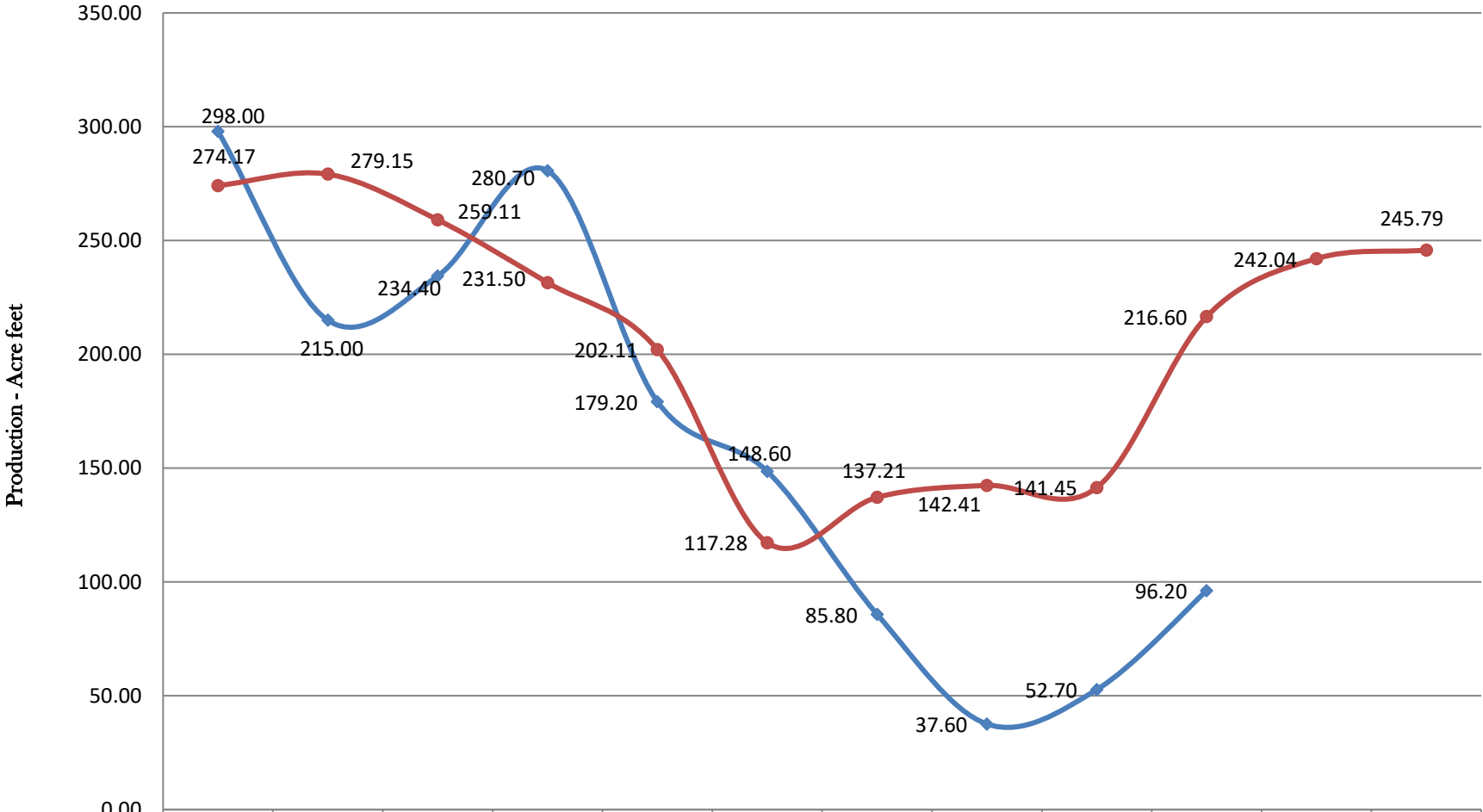
Well Level Report

(* static level with surrounding wells off 24 hrs)	January 2024			February 2024			March 2024			April 2024			May 2024			June 2024		
	Static Level	Pumping Level	GPM	Static Level	Pumping Level	GPM	Static Level	Pumping Level	GPM	Static Level	Pumping Level	GPM	Static Level	Pumping Level	GPM	*Static Level	Pumping Level	GPM
TY Well 1 Elev 800' Depth 330'							156			157	176	523.8						
Monitor Well No. 21A Elev 800' Depth 251'	54			33			54			27								
Well No. 12 (River) Elev 800' Depth 207'	47	108	261	29	97	261	28	92	299	22	105	276						
Well No. 19A (River) Elev 800' Depth 215'	52	98	336	34	86	374	36	77	374	25	91	374						
Well No. 20A (River) Elev 800' Depth 225'	48	93	299	30	80	299	32	72	337	22	83	336						
Well No 25 (River) Elev 805' Depth 210'	51						57	75		23.5	110							
Well No. 3 (Fan) Elev 1220' Depth 547'																		
Well No. 7A (Fan) Elev 1240' Depth 554'																		
Well No. 8 (Fan) Elev 1227' Depth 1000'																		
Well No. 9 (Fan) Elev 1252' Depth 436'																		
Well No. 10 (Fan) Elev 1210' Depth 405'																		
Well No. 13 (Fan) Elev 1280' Depth 403'																		
Well No. 14 (Fan) Elev 1310' Depth 542'	308						110			211								
Well No. 17 (Fan) Elev 1375' Depth 597'	317			293			299			295								
Well No 22 (Fan) Elev 997.4' Depth 1100'	170			158			172	199	195	160	198	192						
Well No. 23 (Fan) Elev 1587' Depth 963'	120			118			121			121								
Well No. 24 (Fan) Elev 1530' Depth 582'	242			238			246			246								
Well No. 29 (Fan) Elev 1314' Depth 450'	268			246			247			244								
Well No. 41 (Horizontal) Elev 2627' Depth 555'			14.7			14.4			14			14.4						
Well No. 42 (Horizontal) Elev 2632' Depth 675'			28.5			29.6			15			30.4						
Well No. 44 (Horizontal) Elev 3040' Depth 465'			7.9			5.7			6			4.5						
Well No. 46 (Horizontal) Elev 3050' Depth 870'			8.5			18.5			15			14.5						
Well No. 47 (Horizontal) Elev 3050' Depth 1007'			4.6			9.6			2			8.2						
Well No. 48 (Horizontal) Elev 3160' Depth 785'			14.7			12.9			7			13.7						
Well No. 49 (Horizontal) Elev 3160' Depth 905'			10.2			10.2			5			10.1						
Well No. 50 (Horizontal) Elev 3120' Depth 1215'			19.7			22.7			12			5.4						

Yuima Municipal Water District
River Well Static (21A) and Pumping Levels
For Yuima Wells No. 12, 19A, 20A and 25
(Increasing Inverse = improving water levels)
Pumping and Static Levels (feet below ground level)
(Updated April 2024) 2020-Current



Yuima Municipal Water District
 Monthly Production of District Owned Wells
 Updated April 2024



	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN
◆ FY 2023/24	298.00	215.00	234.40	280.70	179.20	148.60	85.80	37.60	52.70	96.20		
● 15-Yr Avg.	274.17	279.15	259.11	231.50	202.11	117.28	137.21	142.41	141.45	216.60	242.04	245.79

YUIMA MUNICIPAL WATER DISTRICT

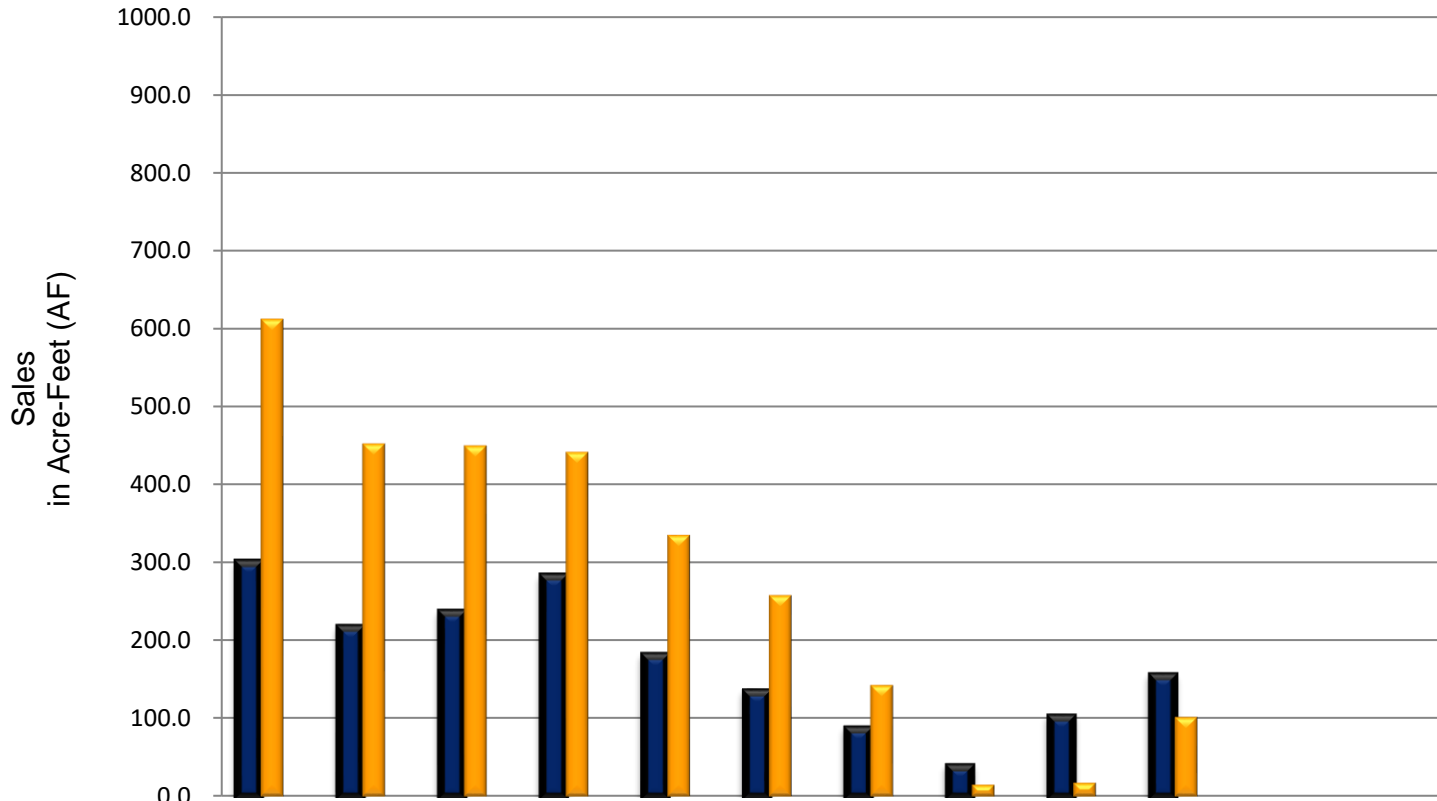
REPORT OF DISTRICT WATER PURCHASED AND PRODUCED

	Month Comparative One (1) Year Ago			Fiscal Year to Date Comparatives		
	Apr-24	Apr-23	%CHANGE	2023/24	2022/23	%CHANGE
LOCAL SUPPLY	153.5	94.9	61.7%	1736.8	1312.4	32.3%
AUTHORITY	101.9	136.2	0.0%	2822.5	3027.9	-6.8%
TOTAL PRODUCED & PURCHASED	255.4	231.1	10.5%	4559.3	4340.3	5.0%
CONSUMPTION	228.3	203.7	12.1%	4316.7	4169.4	3.5%
% LOCAL	60.1%	41.1%	19.0%	38.1%	30.2%	7.9%
%AUTHORITY	39.9%	58.9%	-19.0%	61.9%	69.8%	-7.9%

FISCAL YEAR ENDING JUNE 30 COMPARATIVES

	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011	2010	2009
LOCAL SUPPLY	1682.0	2295.2	2571.6	2311.7	1688.5	2107.5	2058.1	2334.3	2726.6	3145.7	4199.9	4353.8	3356.5	2858.8	3729.7
AUTHORITY SUPPLY	3768.3	5151.2	5610.9	4684.7	4819.6	4780.9	4470.6	3621.1	4468.4	4596.1	2149.3	1183.6	1617.7	2521.8	2347.0
TOTAL PRODUCED & PURCHASED	5450.3	7446.4	8182.5	6996.4	6508.1	6888.4	6528.7	5955.4	7195.0	7744.8	6349.2	5537.4	4974.2	5380.6	6076.7
CONSUMPTION	5235.0	7176.2	7879.3	6727.3	6351.1	6629.8	6379	5887.8	7175.6	7591.1	6310.3	5486.9	4959.0	5310.8	5909.0
% LOCAL	30.9%	30.8%	31.4%	33.0%	25.9%	30.6%	31.5%	39.2%	37.9%	40.6%	66.1%	78.6%	67.5%	53.1%	61.4%
% AUTHORITY	69.1%	69.2%	68.6%	67.0%	74.1%	69.4%	68.5%	60.8%	62.1%	59.4%	33.9%	21.4%	32.5%	46.9%	38.6%

**YUIMA MUNICIPAL WATER DISTRICT
WATER PRODUCED & PURCHASED
2023-24**



	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24
■ LOCAL SUPPLY PRODUCED	298.0	215.0	234.4	280.7	179.2	133.0	85.8	37.6	101.0	153.5	0.0	0.0
■ AUTHORITY PURCHASED	612.0	452.3	449.8	441.6	335.3	257.8	142.9	15.1	17.4	101.9		
TOTAL PROD/PURCH	910.0	667.3	684.2	722.3	514.5	390.8	228.7	52.7	118.4	255.4		

**YUIMA MUNICIPAL WATER DISTRICT
DELINQUENT ACCOUNTS LISTING
4/30/2024**

YUIMA			
<u>ACCOUNT NUMBER</u>	<u>PAST DUE AMOUNT</u>	<u>ACTION</u>	
01-0688-06	85.69	Notice	
01-0690-08	138.59	Notice	
01-1198-01	234.69	Notice	
01-1351-07	324.96	Notice	
01-1421-06	88.96	Notice	
01-1651-04	381.50	Notice	
01-1655-02	180.87	Notice	
01-2097-00	924.18	Notice	
	\$ 2,359.44		

IDA			
<u>ACCOUNT NUMBER</u>	<u>PAST DUE AMOUNT</u>	<u>ACTION</u>	
02-0051-02	371.27	Notice	
02-0149-02	164.21	Notice	
02-0202-02	208.80	Notice	
02-1797-08	115.12	Notice	
02-2236-02	205.03	Notice	
02-2455-04	110.22	Notice	
02-2984-09	416.25	Notice	
02-3957-04	154.47	Notice	
02-4007-01	75.26	Notice	
02-4175-01	468.10	Notice	
02-4181-00	60.28	Notice	
02-4185-01	233.35	Notice	
02-6500-00	451.98	Notice	
02-6657-00	91.91	Notice	
02-7125-00	71.54	Notice	
02-7246-04	371.27	Notice	
02-7248-02	105.44	Notice	
02-7249-01	61.86	Notice	
	\$ 3,736.36		

LIENS FILED / TRANSFERRED TO TAX ROLL

for liens filed and transfer to tax roll:
 July agenda
 auditor and controller by Aug 10th