

Board Agenda

Regular Meeting

Thursday, July 14, 2022

Camrosa Board Room

5:00 P.M.

TO BE HELD IN PERSON

The Board of Directors meeting will be held in person.

There will be no virtual access.

The public and guests are welcome to attend at the District office:

7385 Santa Rosa Road

Camarillo, CA 93012

Call to Order

Public Comments

At this time, the public may address the Board on any item not appearing on the agenda which is subject to the jurisdiction of the Board. Persons wishing to address the Board should fill out a white comment card and submit it to the Board Chairman prior to the meeting. All comments are subject to a 5-minute time limit.

Matters appearing on the Consent Agenda are expected to be non-controversial and will be acted upon by the Board at one time, without discussion, unless a member of Board or the Staff requests an opportunity to address any given item. Items removed from the Consent Agenda will be discussed at the beginning of the Primary Items. Approval by the Board of Consent Items means that the recommendation of the Staff is approved along with the terms and conditions described in the Board Memorandum.

Consent Agenda

1. **Approve Minutes of the Special Meeting of June 16, 2022**
2. **Approve Minutes of the Special Meeting of June 20, 2022**
3. **Approve Minutes of the Regular Meeting of June 23, 2022**
4. **Approve Minutes of the Special Meeting of June 29, 2022**

5. **Approve Vendor Payments

Objective: Approve the payments as presented by Staff.

Action Required: Approve accounts payable in the amount of \$1,492,563.86.

6. Manhole Rehabilitation

Objective: Maintain the District sewer collection system.

Action Required: Authorize the General Manager to issue a purchase order to Zebron, Inc. in an amount not to exceed \$150,000.00 from the Fiscal Year 2022-23 operating budget for the rehabilitation and coating of District sewer manholes.

7. Biosolids Removal at CWRP

Objective: Remove biosolids from the Camrosa Water Reclamation Facility (CWRP).

Action Required: Authorize the General Manager to issue a purchase order to Liberty Composting, Inc. in an amount not to exceed \$80,000.00 from the Fiscal Year 2022-23 operating budget for the removal of biosolids from the CWRP.

Primary Agenda

8. **Contracting Geographical Information System (GIS) Services

Objective: Outsource management of GIS services.

Action Required: Authorize the General Manager to enter into an annual agreement and issue a purchase order with ZWORLD GIS in an amount not to exceed \$54,000.00 for GIS services and tasks.

9. ** Status Report of AllConnected Managed Service Provider Performance

Objective: Provide an overview of the performance of AllConnected Inc., for contracted IT/OT Managed Services.

Action Required: No action necessary; for information only.

10. Drought Update

Objective: Receive an update on the drought.

Action Required: No action necessary; for information only.

11. **Master Plan

Objective: Begin the master planning process.

Action Required: Authorize the General Manager to enter into an agreement with and issue a purchase order to Woodard & Curran in an amount not to exceed \$557,046.00 for support in developing a near-term Capital Improvement Plan for repair, rehabilitation, and replacement needs of the District's infrastructure.

12. **Rate Adjustments

Objective: Adopt the proposed July 2022 rate adjustments.

Action Required: Adopt Resolution 22-11 of the Board adopting a Schedule of Rates, Fees and Charges for Water and Sanitary Service.

CLOSED SESSION: The Board may enter into a closed session to confidentially discuss personnel matters as authorized by Government Code 54957.

13. Closed Session Conference with Legal Counsel – Personnel

Objective: Conduct a performance review of the General Manager.

Action Required: No action necessary; for information only.

Primary Agenda (cont.)

14. General Manager's Performance and Salary Review

Objective: Review the General Manager's performance and compensation.

Action Required: Consider the General Manager's performance review and salary adjustment.

15. **Salary and Classification Schedule

Objective: Adopt the Salary and Classification Schedule.

Action Required: Adopt Resolution 22-12 Adjusting the District's Salary and Classification Schedule for Employees.

Comments by General Manager; Comments by Directors; Adjournment

PLEASE NOTE: The Board of Directors may hold a closed session to discuss personnel matters or litigation, pursuant to the attorney/client privilege, as authorized by Government Codes. Any of the items that involve pending litigation may require discussion in closed session on the recommendation of the Board's Legal Counsel.

Note: ** indicates agenda items for which a staff report has been prepared or backup information has been provided to the Board. The full agenda packet is available for review on our website at: www.camrosa.com/board-agendas/

July 14, 2022

Board of
Directors
Agenda Packet

Board Minutes

Special Meeting

Thursday, June 16, 2022

5:00 P.M.

Call to Order The meeting was convened at 5:00 P.M.

Present: Eugene F. West, President
Terry L. Foreman, Vice-President
Al E. Fox, Director
Jeffrey C. Brown, Director
Timothy H. Hoag, Director

Staff: Tony Stafford, General Manager (via teleconference)
Ian Prichard, Assistant General Manager
Jozi Zabarsky, Customer Service Manager

Public Comments

None

Primary Agenda

1. Drought Response

Staff briefed the Board on the latest mandates from Metropolitan Water District.

No action was taken.

CLOSED SESSION: CANCELLED

Comments by General Manager

None

Comments by Directors

- Director Fox discussed the potential use and benefit of hot water circulating pumps at Leisure Village
- President West stated JPIA property insurance premium has increased due to the restricted number of carriers.

Adjournment

There being no further business, the meeting was adjourned at 6:18 P.M.

Tony L. Stafford, Secretary/Manager
Board of Directors
Camrosa Water District

(ATTEST)
Eugene F. West, President
Board of Directors
Camrosa Water District

Board Minutes

Special Meeting: Virtual Town Hall

Monday, June 20, 2022

6:00 P.M.

Call to Order The meeting was convened at 6:00 P.M.

Present: Eugene F. West, President (via teleconference)
Terry L. Foreman, Vice-President (via teleconference)
Al E. Fox, Director (via teleconference)
Jeffrey C. Brown, Director (via teleconference)
Timothy H. Hoag, Director (via teleconference)

Staff: Tony Stafford, General Manager (via teleconference)
Ian Prichard, Assistant General Manager (via teleconference)
Terry Curson, District Engineer (via teleconference)
Jozi Zabarsky, Customer Service Manager (via teleconference)

Public Comments

None

Primary Agenda

1. Drought Response

A virtual "town-hall" meeting was held to provide information to and receive feedback from the community. The General Manager gave a presentation on the current drought situation. President West opened the forum for questions and answers with the public in attendance.

No action was taken.

Comments by General Manager

None

Comments by Directors

None

Adjournment

There being no further business, the meeting was adjourned at 7:32 P.M.

Tony L. Stafford, Secretary/Manager
Board of Directors
Camrosa Water District

(ATTEST)
Eugene F. West, President
Board of Directors
Camrosa Water District

Board Minutes

Regular Meeting

Thursday, June 23, 2022

5:00 P.M.

Call to Order The meeting was convened at 5:00 P.M.

Present: Eugene F. West, President
Terry L. Foreman, Vice-President
Al E. Fox, Director
Jeffrey C. Brown, Director
Timothy H. Hoag, Director

Staff: Tony Stafford, General Manager
Ian Prichard, Assistant General Manager
Tamara Sexton, Finance Manager
Kevin Wahl, Superintendent
Greg Jones, Legal Counsel

Guest: Ed McCoy, Fairfield Residential
Grant Williams, Fairfield Residential
Chuck Kiskaden, Leisure Village

Public Comments

None

Consent Agenda

1. Approve Minutes of the Regular Meeting of June 9, 2022

The Board approved the Minutes of the Regular Meeting of June 9, 2022.

Motion: Fox **Second:** Foreman

Motion carried unanimously.

2. Approve Vendor Payments

A summary of accounts payable in the amount of \$2,275,269.63 was provided for Board information and approval. The Board approved the payments to vendors as presented by staff in the amount of \$2,275,269.63.

Motion: Fox **Second:** Foreman

Motion carried unanimously.

Primary Agenda

3. Development During Drought

The Board received comments by guests and directed staff to return to the Board with a workable pathway to providing Water Will Serve Letters for developers that can demonstrate no net impact on existing ratepayers.

No action necessary; for information only.

4. Ordinance 40-22

Agenda Item was pulled.

5. Stage Two Water Supply Shortage

The Board adopted Resolution 22-08 Declaring a Stage Three Water Supply Shortage.

Motion: Hoag **Second:** Brown

Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

6. Fiscal Year 2022-2023 Operating and Capital Budget

The Board adopted Resolution 22-09 Adopting the Operating and Capital Budget for Fiscal Year 2022-2023.

Motion: Brown **Second:** Fox

Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

7. Ventura Regional Sanitation District Sewer Maintenance

The Board pointed out typographical errors to be corrected and authorized the General Manager to enter into a five-year agreement with Ventura Regional Sanitation District (VRSD) and issue a purchase order in an amount not to exceed \$250,000.00 for Fiscal Year (FY) 2022-23 sewer maintenance and cleaning services.

Motion: Hoag **Second:** Brown

Motion carried unanimously.

8. Consolidation of the District's General Election

The Board adopted Resolution 22-10 Requesting Consolidation of the General District Election, Scheduled for November 8, 2022, with Other Elections Called to be Held on the Same Day and in the Same Territory.

Motion: Fox **Second:** Foreman

Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

9. Board Meeting and Agenda Management

The Board authorized the General Manager to enter into a three-year agreement with Granicus, in the amount of \$13,524.23, to subscribe to their meeting and agenda management platform.

Motion: Fox **Second:** Brown

Motion carried unanimously.

CLOSED SESSION: The Board cancelled the closed session to confidentially discuss litigation matters as authorized by Government Codes 54956.9(d)(4).

10. Closed Session Conference with Legal Counsel – Pending Litigation

CANCELLED

Comments by General Manager

- Mr. Stafford provided an update on PV Well #3 and informed the Board that a Special Meeting will be scheduled to discuss the Tierra Rejada Well.

Comments by Directors

- Director Foreman provided a handout regarding per-unit cost conversion.
- Director Hoag commented that his water quality has greatly improved.

Adjournment

There being no further business, the meeting was adjourned at 7:12 P.M.

Tony L. Stafford, Secretary/Manager
Board of Directors
Camrosa Water District

Eugene F. West, President
Board of Directors
Camrosa Water District (ATTEST)

Board Minutes

Special Meeting

Wednesday, June 29, 2022

4:30 P.M.

Call to Order The meeting was convened at 4:30 P.M.

Present: Eugene F. West, President
Terry L. Foreman, Vice-President
Al E. Fox, Director
Jeffrey C. Brown, Director
Timothy H. Hoag, Director

Staff: Tony Stafford, General Manager
Ian Prichard, Assistant General Manager
Terry Curson, District Engineer
Greg Jones, District Counsel

Public Comments

None

Primary Agenda

1. Tierra Rejada Well Rehabilitation Project, Specification No. PW21-03

The Board appropriated additional funding of \$150,000.00 for the Tierra Rejada Well Rehabilitation Project from the potable capital replacement fund and authorized a change order to General Pump Company in the amount of \$139,733.00 for additional out-of-scope work for the cleaning and redevelopment of the well.

Motion: Foreman; **Second:** Brown; the motion carried unanimously.

Comments by General Manager

Mr. Stafford informed the Board that Metropolitan Water District accepted Camrosa's Resolution 2022-08 Declaring a Stage Three Water Supply Shortage and deems Camrosa in compliance with the Emergency Water Conservation Program for the period starting July 1, 2022.

Comments by Directors

Director Fox relayed information from Ventura County Association of Water Agencies regarding the edge-of-field testing agricultural properties will have to engage in to comply with the latest Ag Waiver from the Los Angeles Regional Water Quality Control Board.

President West commended staff on the nonpotable filling station recently established on Gerry Road in the Santa Rosa Valley, in particular Jude Kieswetter for his energy, professionalism, and enthusiasm.

Adjournment

There being no further business, the meeting was adjourned at 4:45 P.M.

Tony L. Stafford, Secretary/Manager
Board of Directors
Camrosa Water District

(ATTEST)
Eugene F. West, President
Board of Directors
Camrosa Water District

Board Memorandum

July 14, 2022

To: General Manager
From: Sandra Llamas, Sr. Accountant
Subject: Approve Vendor Payments

Objective: Approve the payments as presented by Staff.

Action Required: Approve accounts payable in the amount of \$1,492,563.86.

Discussion: A summary of accounts payable is provided for Board information and approval.

Payroll PR 6-2, 6-3 & ME	\$ 143,122.28
Accounts Payable 06/16/2022-07/06/2022	<u>\$ 1,349,441.58</u>
Total Disbursements	<u>\$ 1,492,563.86</u>

DISBURSEMENT APPROVAL

_____ BOARD MEMBER	_____ DATE
_____ BOARD MEMBER	_____ DATE
_____ BOARD MEMBER	_____ DATE

Tony L. Stafford, General Manager

Month of : June-22

CAL-Card Monthly Summary

Date Purchased	Statement Date	Vendor Name	Purchase Total	Item Description	Staff
05/31/22	06/22/22	Amazon	\$13.18	Backhoe Keys	KW
05/26/22	06/22/22	Amazon	\$149.08	Amazon Prime	KW
06/20/22	06/22/22	Amazon	\$66.02	Dry-erase markers/erasers RMWTP, Sunscreen for truck	JS
06/21/22	06/22/22	CWEA Tri Counties	\$30.00	June Workshop	GM
06/17/22	06/22/22	Troemner	\$230.09	Calibration Services for standard weights	GM
06/17/22	06/22/22	UPS Store	\$29.21	Ship Standard Weights	GM
06/10/22	06/22/22	Thomas Scientific	\$58.19	Calmagite Indicator	GM
06/08/22	06/22/22	Ready Refresh	\$27.12	Laboratory water	GM
06/03/22	06/22/22	CVS	\$9.20	Isopropal alcohol	GM
05/25/22	06/22/22	CWEA	-\$675.00	Credit	GM
05/25/22	06/22/22	Thomas Scientific	\$119.68	TSB Broth	GM
05/12/22	06/22/22	Thomas Scientific	\$257.69	Indicator for Chloride titrations	GM
06/01/22	06/22/22	Amazon	\$27.14	board room videoconference equipment	IP
06/16/22	06/22/22	The Acorn	\$121.80	advertising for Town Hall	IP
06/01/22	06/22/22	Thinking2	\$80.00	web site hosting	IP
06/10/22	06/22/22	Facilitron	-\$115.92	ACHS reservation for Town Hall CREDIT (ACHS cancelled)	IP
06/01/22	06/22/22	Facilitron	\$115.92	ACHS reservation for Town Hall	IP
06/13/22	06/22/22	FedEx Office	\$2,359.20	postcard for Town Hall (20 charges, 20 receipts attached)	IP
06/16/22	06/22/22	Capitol Directories	\$95.80	directories for CA legislature (receipt missing; directories on my desk)	IP
06/13/22	06/22/22	zoom	\$62.31	webinar for Town Hall	IP
06/13/22	06/22/22	zoom	\$340.00	teleconferencing for Board & staff meetings	IP
05/31/22	06/22/22	zoom	\$89.94	teleconferencing for Board & staff meetings	IP
05/23/22	06/22/22	Old NY Deli & Bakery	\$404.89	food for strategic plan workshops 5/23, 5/26, 6/1	IP
06/17/22	06/22/22	FSP OIL Changers	\$85.41	Oil Change for unit 34	CP
06/16/22	06/22/22	CWEA	\$50.00	Collection Maintenance Grade 3 exam webinar training	JK
06/15/22	06/22/22	Home Depot	\$17.66	Bug Spray for CWRF	JK
05/26/22	06/22/22	Home Depot	\$100.77	Wheel replacement for equipment at CWRF	JK
05/24/22	06/22/22	Home Depot	\$26.78	Tools for CWRF/work truck 38	JK
05/25/22	06/22/22	Red Wing	\$321.73	Safety Boots	JN
05/23/22	06/22/22	Central Communications	\$397.75	After-Hours Call Center	JZ
06/14/22	06/22/22	Staples	\$117.95	Mailing labels	JZ
06/08/22	06/22/22	Amazon	\$248.40	Service kits for Honda generators	BB
05/27/22	06/22/22	Thompson building material	\$338.03	Concrete for Ballards - Leak Moorpark Rd	CC
05/30/22	06/22/22	Thompson building material	\$99.98	Concrete for Ballards - Leak Moorpark Rd	CC
06/07/22	06/22/22	Jiffy Lube	\$133.15	Oil Change Vehicle 6	CC
06/16/22	06/22/22	McMaster-Carr	\$73.65	Parts for CSUCI Flow Restrictor	BR
06/10/22	06/22/22	McMaster-Carr	\$291.35	Parts for Pennywell Pilot Test	BR
06/08/22	06/22/22	The UPS Store	\$17.78	SWRCB D3 Certificate Application	BR
06/04/22	06/22/22	LogixPro	\$36.00	Training	BR
06/04/22	06/22/22	Swagelok	\$124.56	Tools For unit 36	BR
05/31/22	06/22/22	Valvoline Instant Oil Change	\$120.27	Oil change for unit 36	BR
05/27/22	06/22/22	Amazon	\$193.00	Work Boots	BR
05/26/22	06/22/22	Lowe's	\$129.77	Salt for Pennywell	BR
06/13/22	06/22/22	Ace Hardware	\$38.95	Leak Repair Parts- Cust. Backside	MS
06/19/22	06/22/22	Covid Clinic	\$129.00	Test to return to work	TS
06/07/22	06/22/22	Cracker Barrel	\$63.63	Business Meeting w/Calleguas	TS
06/06/22	06/22/22	SushiWay	\$45.12	Business Meeting w/Oxnard	TS
06/04/22	06/22/22	CarWashClub	\$56.99	monthly vehicle wash	TS
05/31/22	06/22/22	TST Blvd Brgr	\$30.49	Business Meeting w/City	TS
05/26/22	06/22/22	Spectrum	\$1,249.00	Spectrum Internet	JW
06/03/22	06/22/22	Google.com	\$132.00	google corporate email domain - camrosawaterdistrict.org monthly charges - currently 11 seats	JW
06/10/22	06/22/22	Newegg	\$56.83	External SATA 1TB HD for Stella's Office PC	JW
06/11/22	06/22/22	Calfire	\$99.00	online IVR - Delinquent Call Out (Monthly Service Fee)	JW
06/13/22	06/22/22	Newegg	\$32.10	Keyboard and mouse for Stella's Office PC	JW
06/16/22	06/22/22	Mailchimp	\$59.00	Drought awareness outreach	JW
06/19/22	06/22/22	Spectrum	\$86.56	Spectrum Cable	JW
06/17/22	06/22/22	Calfire	\$400.00	Drought awareness outreach	JW
05/24/22	06/22/22	Michaels	\$14.97	signage for conejo wells	KK
05/25/22	06/22/22	B&B hardware	\$23.88	tools for vehicle 31	KK
05/24/22	06/22/22	B&B hardware	\$25.71	tools for vehicle 31	KK
05/24/22	06/22/22	B&B hardware	\$24.84	signage for conejo wells	KK
05/25/22	06/22/22	GFOA	\$160.00	GFOA Membership Tsexton	TDS
06/01/22	06/22/22	Backgrounds Online	\$31.50	Background Screening (RM)	DA
05/25/22	06/22/22	Staples	\$337.89	Office Supplies	DA
02/21/22	06/22/22	VC Metals	\$86.20	Metal For 4B Tower	CS
06/15/22	06/22/22	Big 5	\$126.23	EZ UP - Rosita Fill Up Station	CS
06/01/22	06/22/22	CWEA	\$176.00	Membership Fee	CS
05/31/22	06/22/22	Lowe's	\$240.17	Tables & Tape Trucks 23/36/39	CS
05/30/22	06/22/22	Harbor Freight	\$37.53	Wheel Barrel - Diversion	CS
			\$10,583.12		

Camrosa Water District

Accounts Payable Period:

06/16/2022-07/06/2022

Expense	Account Description	Amount
11100	Accounts Rec-Other	
15773	Deferred Outflows-UAL Prep.	
11700	Meter Inventory	
11900	Prepaid Insurance	
11905	Prepaid Maintenance Ag	
13000	Land	
13400	Construction in Progress	1022459.38
20053	Current LTD Bond 2016	
20052	Current LTD Bond 2012	
20400	Contractor's Retention	-17555.41
20250	Non-Potable Water Purchases	
23001	Refunds Payable	5885.68
50110	Payroll FLSA Overtime-Retro	
50010	Water Purchases & SMP	
50020	Pumping Power	
50100	Federal Tax 941 1 st QTR	
50012	CamSan Reclaimed Water	61612.58
50153	Social Security Tax	
50200	Utilities	22.42
50210	Communications	2881.72
50220	Outside Contracts	46271.70
50230	Professional Services	2200.00
50240	Pipeline Repairs	21438.92
50250	Small Tool & Equipment	3899.24
50260	Materials & Supplies	64392.72
50270	Repair Parts & Equip Maint	128763.63
50280	Legal Services	4546.00
50290	Dues & Subscriptions	2593.00
50300	Conference & Travel	30.00
50310	Safety & Training	
50330	Board Expenses	
50340	Bad Debt	
50350	Fees & Charges	
50360	Insurance Expense	
50500	Misc Expense	
50600	Fixed Assets	
50700	Interest Expense	
TOTAL		\$1,349,441.58

Expense Approval Report

By Vendor Name

Payable Dates 6/16/2022 - 7/6/2022 Post Dates 6/16/2022 - 7/6/2022

Camrosa Water District, CA

Payment Number	Post Date	Vendor Name	Payable Number	Description (Item)	Account Name	Purchase Ord	Amount
Vendor: BON01 - BONDY GROUNDWATER CONSULTING, INC.							
58	07/05/2022	BONDY GROUNDWATER CONSULTING, INC.	077-09 GSA	PM: Santa Rosa GSP	Prof services	FY22-0137-R1	4632.5
TOTAL VENDOR PAYMENTS-GSA						\$	4,632.50
Vendor: *CAM* - DEPOSIT ONLY-CAMROSA WTR							
3337	06/23/2022	DEPOSIT ONLY-CAMROSA WTR	6-23-22-AP2	Transfer to Disbursements Account	Transfer to disbursements-holding ac		197000
3338	06/23/2022	DEPOSIT ONLY-CAMROSA WTR	6-23-22-AP	Transfer to Disbursements Account	Transfer to disbursements-holding ac		863000
3339	06/23/2022	DEPOSIT ONLY-CAMROSA WTR	6-23-22-PR	Transfer to Disbursements Account	Transfer to disbursements-holding ac		235000
Vendor *CAM* - DEPOSIT ONLY-CAMROSA WTR Total:							1295000
58128	07/06/2022	ALEXANDER'S CONTRACT SERVICES, INC	104166	Meter Reading Service	Outsd contracts		1466.2
58129	06/21/2022	ALISYN YAMAMOTO	00004386	Deposit Refund Act 4386 - 1831 Danbury Dr	Refunds payable		32.87
Vendor: ALL06 - ALLCABLE							
58130	06/27/2022	ALLCABLE	4032524	4B Radio Tower	Construction in progress		160.6
58130	06/27/2022	ALLCABLE	4032586	4B Radio Tower	Construction in progress		740.17
58130	06/30/2022	ALLCABLE	4032603	Cat6 Cable	Construction in progress	FY22-0345	2731.25
58130	06/30/2022	ALLCABLE	4032605	Radio Tower 4B	Construction in progress		191.19
Vendor ALL06 - ALLCABLE Total:							3823.21
58131	07/01/2022	ALLCONNECTED INC	43136	AllConnected - Managed IT/OT Services	Outsd contracts	FY22-0219-R1	3750
Vendor: ALL07 - ALLIED ELECTRONICS, INC							
58132	06/27/2022	ALLIED ELECTRONICS, INC	9016400576	4B Radio Tower - Parts	Construction in progress	FY22-0355	2845.23
58132	06/27/2022	ALLIED ELECTRONICS, INC	9016400577	4B Radio Tower - Power Converters	Construction in progress		817.76
Vendor ALL07 - ALLIED ELECTRONICS, INC Total:							3662.99
58133	07/01/2022	ANKURA CONSULTING GROUP LLC	CI-059188	PC Endpoint Monitoring	Outsd contracts	FY22-0180	12812.5
1022	07/05/2022	AQUEOUS VETS	22-0285	GAC Vessels for Conejo Wellfield Treatment Plant	Construction in progress	FY22-0038-R1	657783.15
58134	06/30/2022	AWA	06-14245	AWA Training Course (TC)	Conf. & travel		30
58135	07/01/2022	AWWA	7002027519	Membership 2022-2023 Mmber#00074781 (FY22: Dues & subscrip			2443
Vendor: BAD02 - BADGER METER INC							
58136	06/30/2022	BADGER METER INC	1504630	Potable Meters	Repair Parts & Equipment Maintenar	FY22-0284	4613.9
58136	06/30/2022	BADGER METER INC	1508379	Potable Meters	Repair Parts & Equipment Maintenar	FY22-0284	5234.87
58136	06/30/2022	BADGER METER INC	1509625	Potable Meters	Repair Parts & Equipment Maintenar	FY22-0284	4729.73
58136	06/30/2022	BADGER METER INC	1513008	Potable Meters	Repair Parts & Equipment Maintenar	FY22-0284	3320.46
58136	06/30/2022	BADGER METER INC	1513626	Potable Meters	Repair Parts & Equipment Maintenar	FY22-0284	72509.58
Vendor BAD02 - BADGER METER INC Total:							90408.54
58137	06/30/2022	BLACK MAGIC METAL ART INC.	900	Repair Parts - Antenna Mounts	Repair parts & equipment		960
58138	06/27/2022	BSWLOT 2019, LLC.-Barton Hornstein	00000095	Deposit Refund Act 95 - ADHOR LN	Refunds payable		253.4

Vendor: CAN03 - Cannon Corporation

58139	06/28/2022	Cannon Corporation	80570	Engineering Support Services during construction	Construction in progress	FY21-0035-R1	223
58139	06/28/2022	Cannon Corporation	80627	Design Camsprings new waterline under Conejo Cr	Construction in progress	FY22-0273	11022.04
58139	06/28/2022	Cannon Corporation	80653	Construction Services	Construction in progress	FY20-0256-R2	1947.05
58139	06/28/2022	Cannon Corporation	80805	Contract Inspection Services	Outsd contracts	FY22-0081	1223.5
58139	06/28/2022	Cannon Corporation	80806	Engineering Support Services during construction	Construction in progress	FY21-0035-R1	3228
58139	06/28/2022	Cannon Corporation	80807	Contract Inspection Services	Outsd contracts	FY22-0081	4527
58139	06/28/2022	Cannon Corporation	80808	Contract Inspection Services	Outsd contracts	FY22-0081	1156
58139	06/28/2022	Cannon Corporation	80809	Out of Scope	Construction in progress	FY20-0130-R4	652.5
58139	06/28/2022	Cannon Corporation	80810	Construction Services	Construction in progress	FY20-0256-R2	1205.5
Vendor CAN03 - Cannon Corporation Total:							25184.59

58140	07/01/2022	CENTRAL COAST PROPERTY MANAGEMENT	00002490	Deposit Refund Act 2490 - 1087 Old Ranch Rd	Refunds payable		16.54
58141	07/06/2022	Central Courier LLC	51369	Courier Service	Outsd contracts		860.52
58142	06/30/2022	CITY OF CAMARILLO	29538	Recycled Water from CamSan per June 2017 agrrrr CamSan Water			61612.58

Vendor: CLI01 - CLIFTON LARSON ALLEN LLP

58143	06/30/2022	CLIFTON LARSON ALLEN LLP	3332619	Profesional Auditing Services FY2021-22	Prof services	FY22-0369	600
58143	06/30/2022	CLIFTON LARSON ALLEN LLP	3332619-2	GASB 87 Lease Accounting Implementation Assista	Prof services	FY22-0368	1600
Vendor CLI01 - CLIFTON LARSON ALLEN LLP Total:							2200

58144	06/27/2022	E.J. HARRISON & SONS INC	9975	Trash Removal - CWRF	Outsd contracts		494.59
1023	06/27/2022	ENTERPRISE FLEET SERV INC	FBN4492997	Vehicle Lease June 2022	Outsd contracts		6917.01
58145	06/21/2022	ESQUIRE PROPERTY MANAGEMENT	00001156-2	Deposit Refund Act 1156 - 6149 Paseo Encantada	Refunds payable		26.37

Vendor: FAM01 - FAMCON PIPE & SUPPLY, INC

58146	06/28/2022	FAMCON PIPE & SUPPLY, INC	S100079092-001	Angle Meter Stops - Repair Parts	Repair parts & equipment	FY22-0358	2104.25
58146	06/28/2022	FAMCON PIPE & SUPPLY, INC	S100081374-001	Meter Station 5 & 7 - Parts	Construction in progress	FY22-0357	1901.01
58146	06/27/2022	FAMCON PIPE & SUPPLY, INC	S100081478-001	Repair Parts - Break Away Bolt Kits	Repair parts & equipment		418.28
58146	06/28/2022	FAMCON PIPE & SUPPLY, INC	S100081612-001	Hit fire Hydrant	Pipeline repairs	FY22-0356	2342.34
58146	06/27/2022	FAMCON PIPE & SUPPLY, INC	S100081727-001	Leak Repair Villa 26-118 WO#16205469	Pipeline repairs		127.63
Vendor FAM01 - FAMCON PIPE & SUPPLY, INC Total:							6893.51

58147	06/27/2022	FERGUSON WATERWORKS #1083	0801277	Leak Repair Parts - 24" Dresser Couplings	Pipeline repairs	FY22-0331	9491.63
58148	06/28/2022	Frontier Communications	June 2022	VOIP - Land Lines June 2022	Communications		429.22

Vendor: FRU01 - FRUIT GROWERS LAB. INC.

58149	06/27/2022	FRUIT GROWERS LAB. INC.	206102A	Outside Lab Work CWRF	Outsd contracts		150
58149	06/27/2022	FRUIT GROWERS LAB. INC.	206103A	Outside Labwork	Outsd contracts		385
58149	06/21/2022	FRUIT GROWERS LAB. INC.	207514A	Outside Lab Analysis	Outsd contracts		245
58149	06/21/2022	FRUIT GROWERS LAB. INC.	207515A	Outside Lab Analysis	Outsd contracts		265
58149	06/21/2022	FRUIT GROWERS LAB. INC.	207517A	Outside Lab Analysis	Outsd contracts		40
58149	06/21/2022	FRUIT GROWERS LAB. INC.	207518A	Outside Lab Analysis	Outsd contracts		40
58149	06/27/2022	FRUIT GROWERS LAB. INC.	208009A	Outside Lab Analysis	Outsd contracts		920
58149	06/29/2022	FRUIT GROWERS LAB. INC.	208505A	RMWTP Outside Lab Work	Outside Contracts		40
58149	06/27/2022	FRUIT GROWERS LAB. INC.	208968A	Outside Lab for RMWTP	Outside Contracts		75
58149	06/30/2022	FRUIT GROWERS LAB. INC.	209752A	Outside Lab Analysis	Outsd contracts		107
Vendor FRU01 - FRUIT GROWERS LAB. INC. Total:							2267

58150	07/01/2022	GENERAL PUMP COMPANY, INC	29483	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	Construction in progress	FY22-0163-R1	58714
58151	06/27/2022	GUOHUI HU	00007312	Deposit Refund Act 7312 - 4505 Calle Argolla	Refunds payable		76.8

Vendor: HAC01 - HACH COMPANY

58152	06/27/2022	HACH COMPANY	13087071	HACH Sequential Chlorination CIP	Construction in progress	FY22-0329	9737.48
58152	06/27/2022	HACH COMPANY	13101255	Chemical Reagents- Woodcreek	Materials & supplies		2972.15
58152	06/27/2022	HACH COMPANY	13104688	HACH Sequential Chlorination CIP	Construction in progress	FY22-0329	3403
58152	06/30/2022	HACH COMPANY	13121243	Chemicals Reagents	Materials & Supplies-RMWTP		915.31
58152	06/30/2022	HACH COMPANY	13121309	HACH Sequential Chlorination CIP	Construction in progress	FY22-0329	511.71

Vendor HAC01 - HACH COMPANY Total: 17539.65

58153	06/30/2022	HADRONEX INC.	22294	Smart Covers - Field Repai	Outsd contracts		135
58154	06/27/2022	HILARY PANZICA	00003517	Deposit Refund Act 3517 - 5085 Laurel Park	Refunds payable		36.16
58155	06/28/2022	HOPKINS GROUNDWATER CONSULTING	11892	Additional Scope task 2 & 3	Construction in progress	FY22-0133	4480
58156	06/27/2022	HOSE-MAN, INC.	5296313-0001-05	Hose for Non Potable Filling Station	Repair parts & equipment		404.83
58157	06/21/2022	IDEXX LABORATORIES, INC	3108449588	Lab Supplies	Materials & supplies		760.15
58158	06/28/2022	INFOSEND, INC.	214626	Printing & Mailing June 2022 Statements and Insert	Outsd contracts		5596.47
58159	06/21/2022	IRENE ARDITO	00004043	Deposit Refund Act 4043 - 1810 Hillridge Dr	Refunds payable		153.85
58160	06/21/2022	JILL SYLVAIN	00000794	Deposit Refund Act 794 - 1184 Itamo St	Refunds payable		90.57
58161	06/21/2022	JIM BASSETT	00003358	Closed Acct Overpayment Refund - 896 Creekside C	Refunds payable		51.63
58162	07/01/2022	JOSHUA LAW	00001529	Deposit Refund Act 1529 - 738 Hillcrest Dr	Refunds payable		67.35
58163	06/30/2022	LIFE TECHNOLOGIES CORPORATION	81480478	Laboratory Supplies	Materials & supplies		208.15
58164	06/27/2022	LINDE GAS & EQUIPMENT INC	11111617	Acetylene Gas Cylinders	Materials & supplies		65.8

Vendor: MCM01 - McMASTER-CARR SUPPLY CO

58165	06/27/2022	McMASTER-CARR SUPPLY CO	79926009	Materials & Supplies - SS Hardware	Materials & supplies		625.14
58165	06/27/2022	McMASTER-CARR SUPPLY CO	79931276	Repair Parts - Band Saw	Repair parts & equipment		75.46
58165	06/27/2022	McMASTER-CARR SUPPLY CO	80224580	Materials & Supplies - SS Hardware	Materials & supplies		946.72
58165	06/27/2022	McMASTER-CARR SUPPLY CO	80389226	Materials & Supplies - SS Hardware	Materials & supplies		523.65

Vendor MCM01 - McMASTER-CARR SUPPLY CO Total: 2170.97

58166	06/28/2022	MCR TECHNOLOGIES, INC.	40803	Conejo Well 3 Production Meter	Construction in progress	FY22-0257	6766.73
58167	07/01/2022	MELINDA SELLER	00005106	Closed Account Overpayment - 2033 Vista Alcedo	Refunds payable		243.31
58168	06/27/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	100757	Preparation of Unidirectional Flushing RFP	Outsd contracts	FY22-0155	2413.81

Vendor: NOH01 - NOHO CONSTRUCTORS

58169	06/29/2022	NOHO CONSTRUCTORS	Paymt 7-Project-PS 20-06	Pump Station 2 - Generator Installation	Construction in progress	FY21-0219-R1	41785.06
58169	06/29/2022	NOHO CONSTRUCTORS	Retention-Pymt7	Retention Pymt7 Project PS20-06	Contractor's retention		-2089.25

Vendor NOH01 - NOHO CONSTRUCTORS Total: 39695.81

58170	06/30/2022	NORTHSTAR CHEMICAL	227280	Materials and Supplies - Chemicals RMWTP	Materials & Supplies-RMWTP		2341.7
58171	06/29/2022	PROVOST & PRITCHARD CONSULTING GROUP	92992	GAC Engineering	Construction in progress	FY20-0326-R2	2700

Vendor: PUR01 - PURETEC INDUSTRIAL WATER

58172	06/27/2022	PURETEC INDUSTRIAL WATER	1980883	Chemicals RMWTP	Materials & Supplies-RMWTP		13095.69
58172	06/27/2022	PURETEC INDUSTRIAL WATER	1982870	Chemicals RMWTP	Materials & Supplies-RMWTP		12307.58
58172	06/27/2022	PURETEC INDUSTRIAL WATER	1988854	Chemicals RMWTP	Materials & Supplies-RMWTP		13029.15

Vendor PUR01 - PURETEC INDUSTRIAL WATER Total: 38432.42

58173	06/28/2022	RINCON PROPERTY MGMT	00000676	Deposit Refund Act 676 - 6189 Gitana Ave	Refunds payable		67.76
-------	------------	----------------------	----------	--	-----------------	--	-------

Vendor: RON01 - RON'S PORTABLE WELDING

58174	06/30/2022	RON'S PORTABLE WELDING	6859	Materials & Supplies - Pipe Back	Materials & supplies		1000
58174	06/30/2022	RON'S PORTABLE WELDING	6860	Repair Parts - Bumper Mods for Hitch	Repair parts & equipment		375
58174	06/30/2022	RON'S PORTABLE WELDING	6861	Materials & Supplies - Pipe Rack	Materials & supplies		375
58174	06/30/2022	RON'S PORTABLE WELDING	6869	Materials & Supplies - Pipe Rack	Materials & supplies		625

Vendor RON01 - RON'S PORTABLE WELDING Total: 2375

Vendor: ROY03 - ROYAL INDUSTRIAL SOLUTIONS

58175	06/27/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1017223	Read Road MCC	Construction in progress		262.24
58175	06/28/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1017697	Repair Parts - Power Supplies	Repair parts & equipment		765.81
58175	07/01/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1018064	CSUCI Recycled VFD 2	Repair parts & equipment	FY22-0246-R1	15878.69
58175	06/27/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1019944	Repair Parts - VFD#3	Repair parts & equipment		369.67
58175	06/27/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1019945	Repair Parts - VFD#2	Repair parts & equipment		369.67
58175	06/27/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1021833	Read Rodad MCC	Construction in progress		747.63
58175	06/27/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1022185	4B Radio Tower	Construction in progress		999.27
58175	06/28/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1022200	Repair Parts - Power Supplies	Repair parts & equipment		510.54
58175	06/28/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1022201	Repair Parts - Power Supplies	Repair parts & equipment		765.81
58175	06/28/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1022202	Repair Parts - Power Supplies	Repair parts & equipment		510.54
58175	06/27/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1022259	4B Radio Tower	Construction in progress		417.68
58175	06/27/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1022581	4B Radio Towe	Construction in progress		903.53

Vendor ROY03 - ROYAL INDUSTRIAL SOLUTIONS Total: 22501.08

58176	06/27/2022	RP Barricade, Inc	61415	Engineered TCP Cal Trans Permit-WO#15513094	Pipeline repairs		700
58177	06/28/2022	RT LAWRENCE CORPORATION	47298	Processing June 2022 Payments-Lockbox Servcs	Outsd contracts		741.52
58178	07/05/2022	SAM HILL & SONS, INC.	4212	Leak Repair - 1 1/2 Service	Pipeline repairs	FY22-0367	7686.09
58179	07/01/2022	SARAH HINDMARSH	00007506	Overpayment Refund Act 7506 - 4491 Via Marques Refunds payable			4485.77

Vendor: SCF01 - SC Fuels

58180	06/27/2022	SC Fuels	2152720IN	Materials & Supplies -Fuel Seminary Lift Station	Materials & supplies		7081
58180	06/27/2022	SC Fuels	2153034IN	Material & Supplies -Fuel	Materials & supplies		670.47
58180	06/27/2022	SC Fuels	2153034IN	Material & Supplies -Fuel	Materials & supplies		618.89
58180	06/27/2022	SC Fuels	2153034IN	Material & Supplies -Fuel	Materials & supplies		694.27
58180	07/01/2022	SC Fuels	2157882IN	Material & Supplies - Fuel	Materials & supplies		1793.3
58180	07/01/2022	SC Fuels	2163991IN	Material & Supplies - Fuel	Materials & supplies		2036.79

Vendor SCF01 - SC Fuels Total: 12894.72

58181	06/28/2022	S-MT SALES, INC.	16109	EQ Pond Screens	Construction in progress	FY22-0363	5712.69
-------	------------	------------------	-------	-----------------	--------------------------	-----------	---------

Vendor: SCG01 - SOUTHERN CALIFORNIA GAS

1024	06/30/2022	SOUTHERN CALIFORNIA GAS	June2022	June 2022 Usage Charges - Act 17001399009	Utilities		6.64
1024	06/30/2022	SOUTHERN CALIFORNIA GAS	June2022-A	June 2022 Usage Charges- Acct #12378717941	Utilities		15.78

Vendor SCG01 - SOUTHERN CALIFORNIA GAS Total: 22.42

58182	06/21/2022	SVETLANA GULOTTA	00000105	Deposit Refund Act 105 - 6311 Upland Rd	Refunds payable		139.32
58183	06/21/2022	TANNIS L MCLAUGHLIN	00006449-2	Deposit Refund Act 6449 - 4708 Via Cupertino	Refunds payable		83.92

Vendor: TOT02 - TRAFFIC TECHNOLOGIES LLC

58184	06/27/2022	TRAFFIC TECHNOLOGIES LLC	41209	Signs for Non Potable Filling Station	Repair parts & equipment		897.38
58184	06/30/2022	TRAFFIC TECHNOLOGIES LLC	41317	Conejo GAC Signage	Construction in progress		391.39

Vendor TOT02 - TRAFFIC TECHNOLOGIES LLC Total: 1288.77

Vendor: TRA02 - TRAVIS AGRICULTURAL, INC

58185	06/28/2022	TRAVIS AGRICULTURAL, INC	211360-P2	Trench plate Rental - Travis AG	Pipeline repairs	FY22-0360	1091.23
58185	06/30/2022	TRAVIS AGRICULTURAL, INC	22580-F	Raise Pump Pedestals - Conejo Wells	Construction in progress	FY22-0362	18282.63
58185	06/30/2022	TRAVIS AGRICULTURAL, INC	22643-F	Radio Tower 4B - Concete pad	Construction in progress	FY22-0359	15910
58185	06/28/2022	TRAVIS AGRICULTURAL, INC	22668F	Sewer Lift 1A MCC	Construction in progress	FY22-0361	10392.83

Vendor TRA02 - TRAVIS AGRICULTURAL, INC Total: 45676.69

58186	06/30/2022	UNDERGROUND SERVICE ALERT OF SOUTHERN C.620220206		Dig Alert Montly Tickets	Outsd contracts		414.25
-------	------------	---	--	--------------------------	-----------------	--	--------

Vendor: UNI12 - UNIFIED FIELD SERVICES CORPORATION

58187	06/28/2022	UNIFIED FIELD SERVICES CORPORATION	Pynt 10-Project PW21-01	PV Well No. 2 Construction Services	Construction in progress	FY22-0010	154661.55
58187	06/28/2022	UNIFIED FIELD SERVICES CORPORATION	Retention-Pynt10-Proj-PV	Retention Pynt10-Project PW21-01	Contractor's retention		-15466.16

Vendor UNI12 - UNIFIED FIELD SERVICES CORPORATION Total: 139195.39

Vendor: UNIO8 - UNIFIRST CORPORATION						
58188	06/27/2022	UNIFIRST CORPORATION	328-1382217	Uniform Cleaning Service	Outsd contracts	382.89
58188	06/27/2022	UNIFIRST CORPORATION	328-1382225	Office Cleaning Supplies - Towel-Mat Service	Outsd contracts	85.4
58188	06/30/2022	UNIFIRST CORPORATION	328-1384155	Uniform Cleaning Service	Outsd contracts	393.58
58188	06/30/2022	UNIFIRST CORPORATION	328-1384162	Office Cleaning Supplies- Towel-Mat Service	Outsd contracts	75.85
58188	06/30/2022	UNIFIRST CORPORATION	328-1386148	Uniform Cleaning Service	Outsd contracts	275.28
58188	06/30/2022	UNIFIRST CORPORATION	328-1386156	Office Cleaning Supplies- Towel-Mat Service	Outsd contracts	75.85
Vendor UNIO8 - UNIFIRST CORPORATION Total:						1288.85
Vendor: USA01 - USA BLUE BOOK						
58189	06/21/2022	USA BLUE BOOK	012124	Lab Supplies	Materials & supplies	612.93
58189	06/27/2022	USA BLUE BOOK	015327	Laboratory Supplies	Materials & supplies	50.19
58189	06/27/2022	USA BLUE BOOK	016354	Ph and Conductivity probe	Repair parts & equipment FY22-0189	3622.11
58189	06/28/2022	USA BLUE BOOK	016355	Ph and Conductivity Probe	Repair parts & equipment FY22-0190	3622.11
58189	06/27/2022	USA BLUE BOOK	016356	Ph and Conductivity Probe	Repair Parts & Equipment-RMWTP FY22-0191	3622.11
58189	06/27/2022	USA BLUE BOOK	018240	Materials & Supplies - RMWTP	Materials & Supplies-RMWTP	916.19
58189	06/30/2022	USA BLUE BOOK	950234	Lab Supplies	Materials & supplies	127.5
Vendor USA01 - USA BLUE BOOK Total:						12573.14
58190	06/21/2022	VARDAN EDZHURYAN	00003496	Deposit Refund Act 3496 - 5245 Laurel Park Dr	Refunds payable	60.06
58191	07/06/2022	VCSDA	2022-2023	VCSDA Annual Dues FY 2022-23	Dues & subscrip	150
58192	06/28/2022	VENTURA COUNTY OVERHEAD DOOR	436202	Repair - Front Gate	Repair parts & equipment	195
58193	07/01/2022	VENTURA SECURITY SYSTEMS	7296954	Security System Maintenace	Outsd contracts	207.48
58194	06/30/2022	VERIZON WIRELESS	9909413155	Cell Phone's	Communications	2452.5
Vendor: WWG01 - W W GRAINGER, INC.						
58195	06/27/2022	W W GRAINGER, INC.	9351311080	Small Tools	Small tools & equipment	951.91
58195	06/30/2022	W W GRAINGER, INC.	9360653936	Small Tools	Small tools & equipment	979.35
58195	06/30/2022	W W GRAINGER, INC.	9360653944	Small Tools	Small tools & equipment	994.7
58195	06/30/2022	W W GRAINGER, INC.	9362558547	Small Tools	Small tools & equipment	973.28
Vendor WWG01 - W W GRAINGER, INC. Total:						3899.24
58196	06/30/2022	WESCO DISTRIBUTION, INC	892889	Replacement VFD's CWRf Bar Screen	Repair parts & equipment FY22-0254	2887.83
58197	06/29/2022	WHITE BRENNER LLP	45567	Legal Services	Legal services	4546
58198	06/27/2022	YSI Incorporated	942213	YSI Sequential Chlorination CIP	Construction in progress FY22-0328	231.51
TOTAL VENDOR PAYMENTS-CAMROSA						\$ 1,349,441.58
1020	07/01/2022	ACWA JOINT POWERS INS	2ndQTR2022	Worker's Compensation Premium 2nd QTR 2022	P/R-worker comp	9210.68
1006	07/01/2022	ACWA/JPIA	INV0011701	Dental Insurance	Dental ins.	46590.24
Vendor: PER05 - CAL PERS 457 PLAN						
DFT0004058	06/16/2022	CAL PERS 457 PLAN	INV0011742	Deferred Compensation	Deferred comp - ee paid	3366.46
DFT0004085	06/30/2022	CAL PERS 457 PLAN	INV0011806	Deferred Compensation	Deferred comp - ee paid	3366.46
Vendor PER05 - CAL PERS 457 PLAN Total:						6732.92
DFT0004054	06/16/2022	COLONIAL SUPPLEMENTAL INS	INV0011738	Colonial Benefits	Colonial benefits	279.22
Vendor: EDD01 - EMPLOYMENT DEVELOP. DEPT.						
DFT0004073	06/16/2022	EMPLOYMENT DEVELOP. DEPT.	INV0011766	Payroll-SIT	P/R-sit	3791.87
DFT0004099	06/30/2022	EMPLOYMENT DEVELOP. DEPT.	INV0011822	Payroll-SIT	P/R-sit	3954.15
Vendor EDD01 - EMPLOYMENT DEVELOP. DEPT. Total:						7746.02

Vendor: HEA02 - HealthEquity

DFT0004061	06/16/2022	HealthEquity	INV0011747	HSA-Employee Contribution	HSA Contributions Payable	438.46
DFT0004062	06/16/2022	HealthEquity	INV0011748	HSA Contributions	HSA Contributions Payable	200
DFT0004088	06/30/2022	HealthEquity	INV0011810	HSA-Employee Contribution	HSA Contributions Payable	438.46
DFT0004089	06/30/2022	HealthEquity	INV0011811	HSA Contributions	HSA Contributions Payable	200
Vendor HEA02 - HealthEquity Total:						1276.92

Vendor: LNL01 - LINCOLN FINANCIAL GROUP

1012	06/16/2022	LINCOLN FINANCIAL GROUP	INV0011743	Deferred Compensation	Deferred comp - ee paid	2058
1018	06/30/2022	LINCOLN FINANCIAL GROUP	INV0011807	Deferred Compensation	Deferred comp - ee paid	2058
Vendor LNL01 - LINCOLN FINANCIAL GROUP Total:						4116

Vendor: RFS01 - LINCOLN FINANCIAL GROUP

1011	06/16/2022	LINCOLN FINANCIAL GROUP	INV0011761	Profit Share Contribution	Profit share contributions	2618.42
1019	06/30/2022	LINCOLN FINANCIAL GROUP	INV0011819	Profit Share Contribution	Profit share contributions	2618.42
Vendor RFS01 - LINCOLN FINANCIAL GROUP Total:						5236.84

Vendor: PER01 - PUBLIC EMPLOYEES

DFT0004059	06/16/2022	PUBLIC EMPLOYEES	INV0011745	PERS-Classic Employee Portion	P/R-state ret.	16678.71
DFT0004086	06/30/2022	PUBLIC EMPLOYEES	INV0011808	PERS-Classic Employee Portion	P/R-state ret.	16678.71
Vendor PER01 - PUBLIC EMPLOYEES Total:						33357.42

DFT0004063	06/16/2022	SYMETRA LIFE INS CO.	INV0011749	Life Insurance	Life ins.	270.25
------------	------------	----------------------	------------	----------------	-----------	--------

Vendor: UNI10 - UNITED STATES TREASURY

DFT0004031	06/16/2022	UNITED STATES TREASURY	INV0011704	FIT	P/R-fit	10129.66
DFT0004032	06/16/2022	UNITED STATES TREASURY	INV0011705	Payroll-Social Security Tax	P/R - ee social security	545.6
DFT0004033	06/16/2022	UNITED STATES TREASURY	INV0011706	Payroll- Medicare Tax	P/R - ee medicare	2848.46
DFT0004097	06/30/2022	UNITED STATES TREASURY	INV0011820	FIT	P/R-fit	10536.69
DFT0004098	06/30/2022	UNITED STATES TREASURY	INV0011821	Payroll- Medicare Tax	P/R - ee medicare	2834.92
Vendor UNI10 - UNITED STATES TREASURY Total:						26895.33

Vendor: UWA01 - UNITED WAY OF VENTURA CO.

58117	06/16/2022	UNITED WAY OF VENTURA CO.	INV0011737	Charity-United Way	P/R-charity	20
58127	06/30/2022	UNITED WAY OF VENTURA CO.	INV0011805	Charity-United Way	P/R-charity	20
Vendor UWA01 - UNITED WAY OF VENTURA CO. Total:						40

Vendor: UNU01 - UNUM LIFE INSURANCE

1016	07/01/2022	UNUM LIFE INSURANCE	INV0011750	Lont Term Disability	Ltd ins.	1111.72
1016	07/01/2022	UNUM LIFE INSURANCE	INV0011762	Short Term Disability	P/R-std ins.	258.72
Vendor UNU01 - UNUM LIFE INSURANCE Total:						1370.44

TOTAL PAYROLL VENDOR PAYMENTS-CAMROSA**\$ 143,122.28**

Board Memorandum

July 14, 2022

To: General Manager

From: Kevin Wahl, Superintendent of Operations

Subject: Manhole Rehabilitation

Objective: Maintain the District sewer collection system.

Action Required: Authorize the General Manager to issue a purchase order to Zebron, Inc. in an amount not to exceed \$150,000.00 from the Fiscal Year 2022-23 operating budget for the rehabilitation and coating of District sewer manholes.

Discussion: As part of maintaining a sewer collection system, manholes and wet wells need to be systematically rehabilitated. Manholes can be physically damaged by road traffic and agricultural work, but they also deteriorate over time due to sewer gases and root intrusion. All of this leads to unnecessary infiltration that puts an undue demand on the Camrosa Water Reclamation Facility.

Zebron, Inc. repairs the internal concrete damage with gunite or hand-applied mortar and then applies a proprietary epoxy topcoat of polyurethane. This protects the repaired concrete from damage caused by sewer gases and reduces infiltration. Zebron, Inc., has been the contractor for past rehabilitation work.

This is an approved operations line item in the Fiscal Year 2022-23 budget.

Board Memorandum

July 14, 2022

To: General Manager

From: Kevin Wahl, Superintendent of Operations

Subject: Biosolids Removal at CWRF

Objective: Remove biosolids from the Camrosa Water Reclamation Facility (CWRF).

Action Required: Authorize the General Manager to issue a purchase order to Liberty Composting, Inc. in an amount not to exceed \$80,000.00 from the Fiscal Year 2022-23 operating budget for the removal of biosolids from the CWRF.

Discussion: The CWRF produces over 1,600 tons of biosolids throughout the year that need to be hauled off site and properly recycled. This service is carried out on an as-needed basis. Camrosa currently has a five-year contract with Liberty Composting, Inc. that is set to expire December 31, 2026.

This is an approved operations line item in the Fiscal Year 2022-23 budget.

Board Memorandum

July 14, 2022

To: General Manager

From: Joe Willingham

Subject: Contracting Geographical Information System (GIS) Services

Objective: Outsource management of GIS services.

Action Required: Authorize the General Manager to enter into an annual agreement and issue a purchase order with ZWORLD GIS in an amount not to exceed \$54,000.00 for GIS services and tasks.

Discussion: With the departure of the District's full time GIS Specialist in March of this year, staff recommends outsourcing these services for an evaluation period of one year, 20 hours per week. Tasks and service would include, but not be limited to:

- GIS Data Development: Migration of GIS data from NAD27 to NAD83 geodetic referencing system
- GIS Maintenance/Program Support: Maintenance of the District's online and on-premise GIS environments
- GIS Application Support: ArcGIS Desktop, ArcGISPro, Collector, FieldMaps, and 3rd party apps (Workflow Management, DigSmart/DigAlerts)
- Mapping Support: Staff reports, publications & documents, project plans, media presentations as needed

At the end of the fiscal year (FY2022-23), staff will evaluate the performance of the GIS consultant and determine whether to renew the contract for subsequent years.

This is an approved operations line item in the Fiscal Year 2022-23 budget.

**Camrosa Water District
7385 Santa Rosa Rd.
Camarillo, CA 93012
Telephone (805) 482-4677 - FAX (805) 987-4797**

Some of the important terms of this agreement are printed on pages 2 through 3. For your protection, make sure that you read and understand all provisions before signing. The terms on Page 2 through 3 are incorporated in this document and will constitute a part of the agreement between the parties when signed.

TO: ZWORLD GIS
27 West Anapamu Street Suite 191
Santa Barbara, CA 93101

DATE: July 1, 2022
Agreement No.: 2023-60

The undersigned Consultant offers to furnish the following: GIS Support Services per proposal dated May 13, 2022 (attached).

Contract price \$: Not to exceed \$54,000 annually per proposal.

Contract Term: July 1, 2022 – June 30, 2023

Instructions: Sign and return original. Upon acceptance by Camrosa Water District, a copy will be signed by its authorized representative and promptly returned to you. Insert below the names of your authorized representative(s).

Accepted: Camrosa Water District

Consultant: ZWORLD GIS

By: _____
Tony L. Stafford

By: _____
Zacharias Hunt

Title: General Manager

Title: GIS Manager

Date: _____

Date: _____

Other authorized representative(s):

Other authorized representative(s):

Consultant agrees with Camrosa Water District (District) that:

- a. Indemnification: To the extent permitted by law, Consultant shall hold harmless, defend at its own expense, and indemnify the District, its directors, officers, employees, and authorized volunteers, against any and all liability, claims, losses, damages, or expenses, including **reasonable attorney's fees and costs, arising from** negligent acts, errors or omissions of Consultant or its officers, agents, or employees in rendering services under this contract; excluding, however, such liability, claims, losses, damages or expenses arising from the District's sole negligence or willful acts.
- b. Minimum Insurance Requirements: Consultant shall procure and maintain for the duration of the contract insurance against claims for injuries or death to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of that work by the Consultant, his agents, representatives, employees or subcontractors.
- c. Coverage: Coverage shall be at least as broad as the following:
 1. Commercial General Liability (CGL) - Insurance Services Office (ISO) Commercial General Liability Coverage (Occurrence Form CG 00 01) including products and completed operations, property damage, bodily injury, personal and advertising injury with limit of at least two million dollars (\$2,000,000) per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location (coverage as broad as the ISO CG 25 03, or ISO CG 25 04 endorsement provided to the District) or the general aggregate limit shall be twice the required occurrence limit.
 2. Automobile Liability - (If applicable) Insurance Services Office (ISO) Business Auto Coverage (Form CA 00 01), covering Symbol 1 (any auto) or if Consultant has no owned autos, Symbol 8 (hired) and 9 (non-owned) with limit of one million dollars (\$1,000,000) for bodily injury and property damage each accident.
 3. Workers' Compensation Insurance - as required by the State of California, with Statutory Limits, and **Employer's Liability Insurance with limit of no less than \$1,000,000 per** accident for bodily injury or disease.
 4. Waiver of Subrogation: The insurer(s) named above agree to waive all rights of subrogation against the District, its directors, officers, employees, and authorized volunteers for losses paid under the terms of this policy which arise from work performed by the Named Insured for the District; but this provision applies regardless of whether or not the District has received a waiver of subrogation from the insurer.
 5. Professional Liability - (also known as Errors & Omission) Insurance appropriate to the Consultant profession, with limits no less than \$1,000,000 per occurrence or claim, and \$2,000,000 policy aggregate.
 6. Cyber Liability Insurance (Technology Professional Liability – Errors and Omissions), with limits not less than \$2,000,000 per occurrence or claim, and \$2,000,000 aggregate or the full per occurrence limits of the policies available, whichever is greater. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in this Agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.
- d. If Claims Made Policies:
 1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.
 2. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of the contract of work.

3. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, the Consultant **must purchase “extended reporting”** coverage for a minimum of five (5) years after completion of contract work.

If the Consultant maintains broader coverage and/or higher limits than the minimums shown above, the District requires and shall be entitled to the broader coverage and/or higher limits maintained by the Consultant. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the District.

Other Required Provisions: The general liability policy must contain, or be endorsed to contain, the following provisions:

- a. Additional Insured Status: District, its directors, officers, employees, and authorized volunteers are to be given insured status (at least as broad as ISO Form CG 20 10 10 01), with respect to liability arising out of work or operations performed by or on behalf of the Consultant including materials, parts, or equipment furnished in connection with such work or operations.
- b. Primary Coverage: For any claims related to this project, the Consultant's **insurance coverage shall be primary** at least as broad as ISO CG 20 01 04 13 as respects to the District, its directors, officers, employees, and authorized volunteers. Any insurance or self-insurance maintained by the District, its directors, officers, employees, and authorized volunteers shall be excess of the Consultant's insurance and shall not contribute with it.

Notice of Cancellation: Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to the District.

Self-Insured Retentions: Self-insured retentions must be declared to and approved by the District. The District may require the Consultant to provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. The policy language shall provide, or be endorsed to provide, that the self-insured retention may be satisfied by either the named insured or the District.

Acceptability of Insurers: Insurance is to be placed with insurers having a current A.M. Best rating of no less than A:VII or as otherwise approved by the District.

Verification of Coverage: Consultant shall furnish the District with certificates and amendatory endorsements or copies of the applicable policy language effecting coverage required by this clause. All certificates and endorsements are to be received and approved by the District before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive the **Consultant's** obligation to provide them. The District reserves the right to require complete, certified copies of all required insurance policies, including policy Declaration and Endorsements pages listing all policy endorsements. If any of the required coverages expire during the term of this agreement, the Consultant shall deliver the renewal certificate(s) including the general liability additional insured endorsement to Camrosa Water District at least ten (10) days prior to the expiration date.

Subcontractors: Consultant shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Consultant shall ensure that the District, its directors, officers, employees, and authorized volunteers are an additional insured on Commercial General Liability Coverage.

Other Requirements:

- a. Consultant shall not accept direction or orders from any person other than the General Manager or the person(s) **whose name(s) is (are) inserted on Page 1 as “other authorized representative(s).”**
- b. Payment, unless otherwise specified on Page 1, is to be 30 days after acceptance by the District.
- c. **Permits required by governmental authorities will be obtained at Consultant's expense, and Consultant will comply** with applicable local, state, and federal regulations and statutes including Cal/OSHA requirements.

- d. Any change in the scope of the professional services to be done, method of performance, nature of materials or price thereof, or to any other matter materially affecting the performance or nature of the professional services will not be paid for or accepted unless such change, addition or deletion is approved in advance, in writing by the District. **Consultant's "other authorized representative(s)"** has/have the authority to execute such written change for Consultant.

The District may terminate this Agreement at any time, with or without cause, giving written notice to Consultant, specifying the effective date of termination.

CAMROSA WATER DISTRICT
GIS SUPPORT SERVICES

May 13, 2022



Submitted to:

Joe Willingham
Information Technology Manager
Camrosa Water District
7385 Santa Rosa Road
Camarillo, CA 93012

Submitted by:

ZWORLD GIS
27 West Anapamu Street Suite #191
Santa Barbara, CA 93101
Tel 805.448.1726
info@zworldgis.com

May 13, 2022

Camrosa Water District
7385 Santa Rosa Road
Camarillo, CA 93012

Re: GIS SUPPORT SERVICES

ZWORLD GIS is honored to provide a solution for the District's need for ongoing GIS Support. The attached submittal contains details on the GIS Support Services we provide and the particular approach we have designed for the District's GIS Program. The Camrosa Water District having developed GIS data within its various operations identifies the need for ongoing GIS Support Services for all District Mapping/GIS needs.

The Camrosa Water District has identified the need to continue deploying GIS solutions and maintain GIS data in support of the various operations within the District. These tasks include: GIS data development, GIS data maintenance, GIS application support, Mapping support, and District GIS program support. ZWORLD GIS works with supporting the Esri Products and Applications the District has in place, and can provide a cost effective solution for providing core functions and tasks for ongoing District GIS support.

ZWORLD GIS has proposed staff supplement services that provide a solution that addresses the immediate tasks of the District, while providing a solution for on-going support for maintenance of the GIS data and applications that provide the District with business GIS data that is updated and reliable for operational use. The fixed cost of the proposed contract services and not to exceed is \$54,000 for the annual on-going support of the District GIS.

Thank you for the opportunity to provide you with this proposal. ZWORLD GIS would welcome any opportunity to meet with District officials to discuss any District specific questions related to this proposal. We understand the importance of this project to the District and the local community. We look forward to talking with you at your convenience.

Sincerely,



Zacharias Hunt, MPA
Project Manager
ZWORLD GIS



Table of Contents

About ZWORLD GIS.....	2
Background	3
Scope of Work.....	5
Service Tasks.....	5
Cost and Schedule.....	7
Support Team.....	8
References.....	11

About ZWORLD GIS



GEOSPATIAL INFORMATION SYSTEMS

- Mapping**
- Needs Assessment & Strategic Planning**
- GIS Data Development**
- GIS Training**
- GIS Database Design & Development**
- GIS Application Development**
- Systems Integration**
- Project Management**
- Staff Supplement**
- Emergency Preparedness**

"Zacharias is highly expertised in GIS, but never ceases the exploration of new techniques and applications. He's got that rare capability to take control of the details while remaining flexible and creative, and always with the customer foremost in mind." - Lauren Moore, County of Santa Barbara

As a one of the leading service providers of geospatial data products and services in the Santa Barbara/Ventura region, we are cognizant of the crucial role that such information and technology plays in key decisions at all levels of government. ZWORLD GIS is committed to the highest quality and technical standards in this industry, and to supplying decision makers with reliable, accurate information that empowers decision making. This commitment is what sets ZWORLD GIS above others in the industry.

Our goal has been to combine cutting-edge technology with a team of key technical personnel with impressive career achievements and extensive experience in the field of Geospatial Technology and Mapping. ZWORLD GIS will be utilizing the latest approaches and best practices developed in the industry. ZWORLD GIS draws upon the 25 years of experience deploying GIS services, which included developing a GIS Strategic Plan for the County of Santa Barbara as well as the Channel Islands Regional Geographic Information System Collaborative. Being familiar with asset management, mobile field applications, engineering and design processes, legal policies and procedures, and GIS solutions, ZWORLD GIS is uniquely qualified to produce GIS data that is realistic and will assist with achieving business success for the Camrosa Water District.

ZWORLD GIS is a GIS consulting business located in Santa Barbara, California. We provide GIS services and solutions to both private and public organizations. ZWORLD GIS is an Environmental Systems Research Institute, Inc. (ESRI) centered business utilizing the ESRI suite of desktop, database, web, mobile and cloud product solutions and integration strategies related to geospatial data. We support small business needs of basic GIS data development, analyses, and cartographic needs, as well as large scale organizations that require enterprise advanced solutions to capture, store and disseminate information through a variety of application types and portals. With over 25 years of experience in the geospatial technology industry, ZWORLD GIS understands today's business needs within local government and municipalities. Whether the focus is on infrastructure and utility management, planning and land use, law enforcement, environmental and natural resource, emergency preparedness, or public safety, ZWORLD GIS has the experience and resources to meet your challenges with cost effective and scalable GIS solutions.

Background

The Camrosa Water District, organized under the California Water Code, was established on July 24, 1962. Construction of the initial waterworks facilities occurred from 1966 through 1969, and this installation forms the backbone of the potable water system in place today. The District's first customers were ranchers who took delivery of imported water directly from the newly constructed Calleguas pipeline that traversed the area. From these few irrigation customers in the sixties, the potable water distribution system has expanded steadily to serve approximately 35,000 residents, more than 3,000 acres of agriculture, and a host of businesses and light industry.

In 1981, potable water service was extended to the Camarillo State Hospital, and the District assumed the hospital's wastewater treatment plant. When first constructed in 1930, the wastewater plant was the first full-scale bio-filtration plant in the world. In 1997, the plant was rebuilt and expanded to a 1.5 million gallons per day (water reclamation facility). The CWRF, as it is known, produces tertiary-treated recycled water for irrigation use at California State University Channel Islands (CSUCI), the entity that inherited the hospital campus after it was closed in 1997.

In 1991, Camrosa's service area, like all of California, was in the midst of a severe drought. Imported water for agricultural use had diminished and groundwater levels were dropping. Treated wastewater from the City of Thousand Oaks's Wastewater Treatment Plant along Conejo Creek was envisioned to be a long-term solution to local shortages, and in 2002 construction was completed on the Conejo Creek Diversion Project, designed to provide 10,000 acre-feet a year of new non-potable surface water to meet irrigation needs. The area served by non-potable water has gradually increased to include deliveries to agricultural use in the Pleasant Valley County Water District (PVCWD) service area, to agricultural irrigators in the lower elevations of Santa Rosa Valley, and to community landscape areas in Leisure Village.

In 2014, after nearly a decade of planning, Camrosa completed construction on the Round Mountain Water Treatment Plant, a desalination facility that treats brackish (very salty) groundwater to drinking water levels. This desalter produces a million gallons of drinking water a day, offsetting about ten percent of the water Camrosa was importing when the plant came online. Camrosa

received \$2.3 million in state grant funding to help pay for this facility.



CAMROSA

WATER DISTRICT

Incorporation Date: 1962

District Size: .31 sq. miles

DISTRICT PROGRAMS

The five District Departments include:

[Customer Accounts and Billing](#)

[Engineering and Operations](#)

[Finance](#)

[Water Resources and Regulatory Compliance](#)

The District serves more than 30,000 people and delivers more than 14,400 acre-feet of water each year. Camrosa delivers potable water, non-potable surface water and water reclaimed at its Water Reclamation Facility.

Wastewater collection services are provided in the central portion of the District and to CSUCI and County of Ventura.



Significance of Project

A District GIS can provide a framework for organizing data from many sources that relate to the District strategy development. GIS, with its data integration and visualization capabilities that foster collaboration, is the natural vehicle for an intra-organizational and interagency development of strategic plans. GIS improves operational response by centralizing data in many formats and from many sources and integrating it with other technologies such as web map applications. In addition, improved workflows create efficiencies in the decision making capability. A District GIS can strengthen the success of achieving and supporting many of the tasks and goals the District has established. In particular, the following tasks and goals can achieve a positive impact from GIS:

District Goals

To meet the current and future needs for water and sanitary services

District Goals

To deliver high quality products that are reliable, affordable and responsive

District Goals

To prudently manage and maintain the District's assets, and finally

District Goals

To maintain public awareness and confidence and honor the public's trust

Scope of Work – Mapping/GIS Services

GIS Data Development

This task will entail generating new GIS data from past databases for past calls and incidents on an internal Web Map. ZWORLD GIS is experienced with the necessary techniques needed to adequately capture the new GIS data and successfully create corresponding attribute (tabular) information. Either importing the scanned document and georeferencing for a digitizing process or projecting the correct vector data, ZWORLD GIS will create the new GIS format data, making it ready for applications and maps.

ZWORLD GIS can also generate new GIS data from using other source resources. If aerial imagery meets the agencies positional requirements, then structures that are photo-identifiable can be digitized. Survey documents that contain Coordinate Geometry (COGO) information, such as distance and bearings of pipes, can be used to develop the vector GIS data. Tabular data that contains X,Y values such as northing and eastings, or longitude and latitude can be used to position GIS data. GIS data can also be created using a GPS device, occupying the location of the asset in the field.

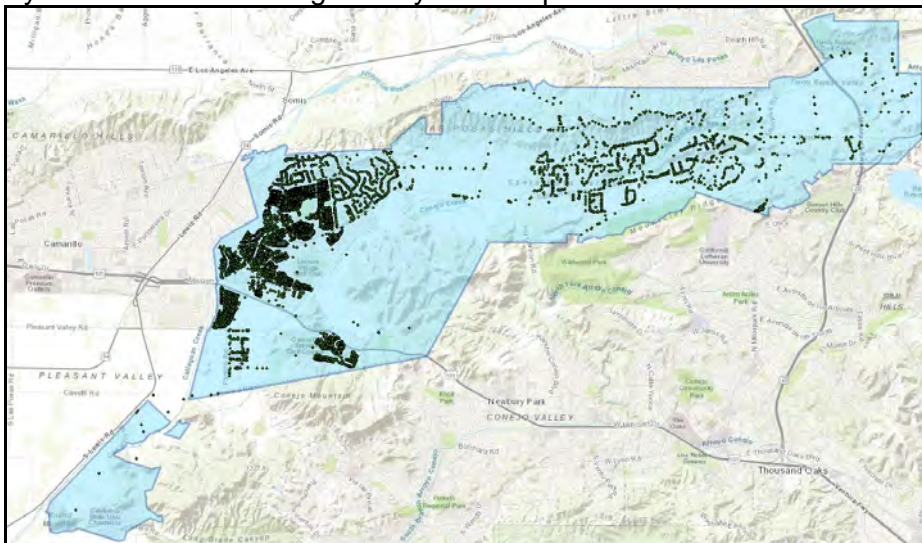
GIS Data Maintenance

This task will focus on maintaining the GIS data once it has been created and where GIS data needs to be updated based on operational changes. This task ensures that the data is kept current and provides the most up to date information is available to staff and application users. ZWORLD GIS will become the data steward of the District GIS data maintaining both new assets and modifying existing features. ZWORLD GIS will be working closely with District staff to perform the required edits to features and attributes.

GIS Application Support

This task will provide support for internal Web Map applications for staff to track and analysis previous site data, system assets and base district data. An additional Web Map for the Public can be developed and, limited data just for public need can be shown.

Additionally, a field application can be developed for field staff to use and document the Water System Valve Exercising and Hydrant Inspections.



Mapping Support

ZWORLD GIS can assist with providing custom mapping and cartographic images for:

- Staff Reports
- Publications & Documents
- Project Plans
- Operational meetings
- Public Sessions & Media Presentation

District GIS Program Support

ZWORLD GIS will work closely with staff to make sure that all of the various operations and resources that integrate with GIS are supported and maintained. This includes

ZWORLD GIS can assist with providing custom mapping and cartographic images for:

- Esri ArcGIS Online Organization Account
 - Web Map Applications
 - Users and Roles
 - Field Mobile Applications
 - Data Publishing and Services
 - Dashboard & Story Map Integrations
- Esri ArcGIS Enterprise Server
 - Rest URL Services
 - Geodatabases
- Esri Desktop Licenses
- District Esri User Accounts
- District Mapping Products
 - Atlas Maps
 - Wall Maps
- GPS Field Collection
 - On-Site Field collection of District Assets



Cost and Schedule

It is proposed that the services involved in the scope of work be conducted by ZWORLD GIS staff as shown on the following page. ZWORLD GIS will be the primary contractor for the proposed scope of work. Deliverables from GIS Professional Services is proposed at an annual cost and not to exceed \$54,000, and all work under this proposal would be invoiced monthly. Services could be started immediately.

Total Weekly Support Hours: 20 hours

ZWORLD GIS will provide dedicated on-site staff for two days a week for the first two months of providing GIS support before transitioning to providing GIS support remotely. On-site support will continue for routine field GPS updates and various on-site needs.

Camrosa Water District– GIS Support Services

Annual GIS Support Cost: \$72,000

With Local Business Partnership Discount (25%): - \$18,000

Total GIS Support	\$54,000
--------------------------	-----------------

Support Team

Zacharias Hunt
Project Manager



Overview

Mr. Hunt is the founding principal of ZWORLD GIS. He has been working in the GIS/Mapping and local government industry since 1999 and holds a Master's degree in Public Administration as well as a Bachelor Degree in Geography. Mr. Hunt also has certification in the use of Global Positioning Systems (GPS) from Ventura College, California. Mr. Hunt has been involved in all aspects of deploying GIS for local government special districts. As the Geographic Information Officer (GIO) for Santa Barbara County, Mr. Hunt managed all aspects of a County Enterprise GIS program which included: developed and implemented a County GIS Strategic Plan; managed GIS web based applications for both internal County staff as well as the public; implemented GIS policy and standards; participated in annual budgeting and procurement process for GIS; developed sustainable GIS revenue opportunities; recruited and trained GIS staff; managed the County GIS Internship program; and coordinated GIS based systems for the County Office of Emergency Services (OES). Mr. Hunt also participates with the Channel Island Regional GIS Collaborative, and served as President from 2010-2016.

Education & Qualifications

- Masters of Science Degree – Public Administration, California State University of Northridge, 2011
- Bachelor of Arts Degree – Geography, University of California, Santa Barbara, 1999

Career Experience

Owner, ZWORLD GIS
June 2011 – Present

CIRGIS President, CIRGIS Collaborative
Mar. 2010 – Jan. 2016

Geographic Information Officer (GIO), Santa Barbara County, CA
Feb. 2007 – June 2011

Public Works GIS Supervisor, Santa Barbara County, CA
Aug. 2004 – Feb. 2007

Lead GIS Analyst, Nellis Air Force Base (USAFE Geobase)
Feb. 2004 – Aug. 2004

Public Works GIS Analyst, Santa Barbara County, CA
Apr. 2000

QUICK FACTS

Previously Managed Projects:

CHANNEL ISLANDS BEACH COMMUNITY SERVICES DISTRICT

Created & upgraded the GIS data for the District Water system which included:

- * Water Pipe Mains / Laterals
- * Water Meters
- * System Valves
- * Fire Hydrants
- * Pressure Zones

VENTURA RIVER WATER DISTRICT

Created & upgraded the GIS data for the District Water system which included:

- * Water Pipe Mains / Laterals
- * Water Meters
- * System Valves
- * Fire Hydrants
- * Pressure Zones

MONTECITO WATER DISTRICT

Created & upgraded the GIS data for the District Water system which included:

- * Water Pipe Mains / Laterals
- * System Valves
- * Fire Hydrants
- * Pressure Zones

CITY OF SOLVANG

Developed new City Water GIS system which included:

- * Water Pipe Mains / Laterals
- * System Valves
- * Fire Hydrants
- * Pressure Zones

Support Team

Gavin Leavitt
GIS Analyst



QUICK FACTS

Recent Projects:

CITY OF SALINAS

Handled city employee, contractor, and public requests for spatial data, maps, and web applications using a variety of formats. Built out the City Sanitary Sewer and Storm Drain system GIS datasets using historic engineering plans. Built City Sewer Utility Network for ArcMap.

Published ArcGIS for Server:

- * WFS
- * WMS
- * Geoprocessing Services
- * Feature Services

GOLETA STORM DRAIN GIS

Developed advanced GIS data for the City of Goleta Storm Drain system which included creating system GIS layers from field GPS collection and as-built research.

- * Inlets
- * Outlets
- * Maintenance Holes
- * Surface Drainage
- * Underground Drainage

CHANNEL ISLANDS BEACH COMMUNITY SERVICES DISTRICT

Created & upgraded the GIS data for the District Water system which included:

- * Water Pipe Mains / Laterals
- * Water Meters
- * System Valves
- * Fire Hydrants
- * Pressure Zones

Overview

Mr. Leavitt is the lead GIS Analyst of ZWORLD GIS.

He has been working in the Geospatial Science Industry and assisting with local government agencies since 2015 and holds a Bachelor of Science degree in Marine Sciences and a Master of Science Degree in Applied Marine Science from California State University, Monterey Bay. Mr. Leavitt also has obtained certifications in the use of Esri GIS Desktop software, and is qualified on mapping grade GPS collection processes in the field. Mr. Leavitt is also a UAV Operator with a Part 107 Certified Remote Commercial Pilot license. Mr. Leavitt has been involved in the many aspects of mapping and data development of GIS for local government and special district agencies. As the Geospatial Information Systems Analyst for ZWORLD GIS, Mr. Leavitt provides core functions of a GIS data development project which can include developing a technical strategy for data creation; development of GIS data with advanced digitization techniques; create accurate and reliable data from field collection using GPS equipment; integrate GIS data into various third party databases systems; and produce final data reports describing technique, statistical analysis, and metadata documentation. Mr. Leavitt also assists in supporting Web Map applications for agencies that need a common tool to use for all staff. Mr. Leavitt enables agencies by preparing custom training guides for on-site training sessions so staff become more aware of the functionality of the GIS Web Map application deployed by their organization, as well as maintaining core base data for each application to ensure that the GIS is kept relevant and reliable.

Education & Qualifications

- Masters of Science Degree – Applied Marine Science, California State University, Monterey Bay, 2017
- Bachelor of Science Degree – Marine Sciences, California State University, Monterey Bay, 2015
- UAV Operator – Part 107 Certified Remote Commercial Pilot License

Career Experience

GIS Analyst, ZWORLD GIS
December 2020 – Present

GIS Technician, City of Salinas
January 2017 – July 2020

Research Assistant, Monterey Bay Aquarium Research
Institute June 2016 – November 2016

Support Team

Caroline Conrad
GIS Technician



QUICK FACTS

Recent Projects:

COUNTY OF SANTA BARBARA TRANSPORTATION DIVISION

Assist with the design and development of the major capital assets for the County Transportation Division to include into the GIS system in support of their various operations and staging for an enterprise asset management program. Critical GIS assets included:

- * **Street Signs**
- * **Storm Water Infrastructure**
- * **Maintained Road System**

GOLETA SANITARY DISTRICT

Developed advanced GIS data for the District which included creating a custom indexing layer for the entire Easement library, as well as produce cartographic operational maps for the District field staff.

The GIS support services included:

- * **As-Built / Record Drawing Index**
- * **Integration to Mobile Web Map**
- * **Update District GIS Data**

CITY OF BUELLTON

Created & upgraded the GIS data for the City Water system which included:

- * **Water Pipe Mains / Laterals**
- * **Water Meters**
- * **System Valves**
- * **Fire Hydrants**
- * **Pressure Zones**

Overview

Ms. Conrad is the lead GIS Technician of ZWORLD GIS. She has been working in the Geospatial Science Industry and assisting with local government agencies since 2019 and holds a Bachelor of Arts degree in Geography/GIS from the University of California, Santa Barbara. Ms. Conrad also has obtained certifications in the use of Esri GIS Desktop software, and is qualified on mapping grade GPS collection processes in the field. Ms. Conrad has been involved in the many aspects of mapping and data development of GIS for local government and special district agencies. As the Geospatial Information Systems Technician (GIST) for ZWORLD GIS, Ms. Conrad provides core functions of a GIS data development project which can include developing a technical strategy for data creation; development of GIS data with advanced digitization techniques; create accurate and reliable data from field collection using GPS equipment; integrate GIS data into various third party databases systems; and produce final data reports describing technique, statistical analysis, and metadata documentation. Ms. Conrad also assists in maintaining core base data for each client application to ensure that the GIS is kept relevant and reliable.

Education & Qualifications

- Bachelor of Arts Degree – Geography, University of California, Santa Barbara, June 2019

Career Experience

GIS Technician, ZWORLD GIS
January 2022 – Present

GIS Technician, Santa Barbara County Fire
October 2021 – February 2022

Technical Contractor, US Geological Survey
June 2019 – January 2022

Operations Coordinator, University of California, Santa Barbara
September 2018 – June 2019

References

City of Solvang, California



Company Address: 411 Second Street, Solvang CA 93463
Contact Phone: 805.588.4424
Contact Person: Mike Matthews
Date: 2011-Current

Goleta Sanitary District, California



Company Address: 1 Moffett Place, Goleta, CA 93117
Contact Phone: 805.760.4426
Contact Person: Luis Asorga
Date: 2015-Current

City of Goleta, California



Company Address: 130 Cremona Drive, Goleta, CA 93117
Contact Phone: 805.618.5768
Contact Person: Andrea Dransfield
Date: 2013-Current

Montecito Water District, California



Company Address: 583 San Ysidro Road, Montecito, CA 93108
Contact Phone: 805.969.2271
Contact Person: Adam Kanold
Date: 2013-Current

City of Carpinteria, California



Company Address: 5775 Carpinteria Avenue, Carpinteria, CA 93013
Contact Phone: 805.684.5405
Contact Person: John Ilasin
Date: 2015-Current

Ventura River Water District, California



Company Address: 409 Old Baldwin Rd, Ojai, CA 93023
Contact Phone: 805.646.3403
Contact Person: Bert Rapp
Date: 2019-Current

County of Santa Barbara, Public Works Department – Transportation Division



Company Address: 123 East Anapamu Street, Santa Barbara, CA 93101
Contact Phone: 805.896.6296
Contact Person: Kurt Klucher
Date: 2011-Current

Board Memorandum

July 14, 2022

To: General Manager

From: Joe Willingham

Subject: Status Report of AllConnected Managed Service Provider Performance

Objective: Provide an overview of the performance of AllConnected Inc., for contracted IT/OT Managed Services.

Action Required: No action necessary; for information only.

Discussion: At the January 27, 2022 meeting of the Camrosa Board of Directors, the Board approved a support contract with AllConnected Inc. (ACI), of Simi Valley, CA, to provide application, computer, and network support services through the end of FY2025 (June 30, 2025). This two-part contract includes:

- 1) SmartConnect: Normal recurring IT services such as help desk support, security & performance monitoring, preventive maintenance, advanced threat protection, data backup, and end-user security training.
- 2) Auxiliary support as needed: Mainly to assist in IT upgrades, enhancements, and out-of-scope tasks that would otherwise fall under SmartConnect services.

To date, the onboarding phase for these contract components has been successfully completed. ACI has collected system and network configurations, established usage baselines, and gathered performance statistics of all critical IT/OT infrastructure. Camrosa staff has been instructed on accessing and using the help desk, which is accessible via phone, email, or ACI's web portal. Nightly cloud and on-premise backups for all application servers are in place. Weekly updates of critical security patches on all servers and workstations have been configured.

Advanced Email and DNS security features have also been put in place. Per contract, ACI provides monthly cybersecurity awareness training and testing for all staff members. These brief, web-based training sessions include a wide variety of topics such as phishing, password security, ransomware, privacy, and information protection. Camrosa's IT Manager has exercised the use of the auxiliary support services component of the contract by having ACI's designated Camrosa System Administrator on-site at the District office twice a week for four hours a day to assist in system and network anomalies as they arise and to address any out-of-scope end-user issues. Additional benefits of on-site support include Camrosa staff developing a rapport with their eventual full time "Sys Admin" and the support contractor developing a fuller understanding of the IT/OT operations of the District.

Lastly, a collaboration of IT staff and ACI personnel has produced a comprehensive draft IT Plan with policies and procedures to address the handling of IT procurements and cybersecurity at the District. The draft is attached for Board review, with the intent to return to the Board at a later date for adoption.

Camrosa Water District Information Technology Policies and Procedures Manual

Table of Contents

1.	Introduction	14
1.1	Camrosa IT Department.....	14
2.	Information Technology Procurement, Acquisition, and Support Policy	16
2.1	Overview	16
2.2	IT Procurement Categories	16
2.2.1	Standard Items.....	16
2.2.2	Non-Standard Items.....	16
2.2.3	IT Capital Project Expenses	16
2.2.4	Employee Purchases	17
2.2.5	IT Emergency Procurements.....	17
2.2.6	IT Planned Maintenance and IT Outside Contract Support Costs.....	17
2.3	New System Implementation and Support.....	17
2.3.1	Centralized vs. Departmental Acquisition and Support Responsibilities.....	18
2.3.2	Software Licensing	18
2.4	IT Asset Management	18
2.5	IT Lifecycle Management.....	18
2.6	Roles and Responsibilities.....	18
2.6.1.1	Policies	18
2.6.2	Short- and Long-Term Technology Road Maps.....	19
2.6.3	Resources	19
2.6.4	Organization.....	19
2.6.5	Information Technology Steering Committee	19
2.6.5.1	Responsibilities	19
2.6.5.2	Membership.....	19
2.6.5.3	Meetings	20
3.	Cyber Security Policies	21
3.1	Acceptable Use of Information Systems Policy	21
3.1.1	Overview	21
3.1.2	Purpose	22
3.1.3	Scope.....	22
3.1.4	Policy Detail.....	22

3.1.4.1	Ownership of Electronic Files.....	22
3.1.4.2	Privacy	22
3.1.4.3	General Use and Ownership	23
3.1.4.4	Security and Proprietary Information	23
3.1.4.5	Unacceptable Use	24
3.1.4.6	System and Network Activities	24
3.1.4.7	Incidental Use	25
3.1.4.8	Review and Acceptance	25
3.2	User Account/Password Management Policy.....	27
3.2.1	Overview	27
3.2.2	Purpose	27
3.2.3	Audience	27
3.2.4	Policy Detail.....	27
3.2.4.1	Account Names and Passwords	27
3.2.4.2	Account Management.....	27
3.2.4.3	System-Level/Administrator Passwords	28
3.2.4.4	Password Protection	28
3.3	Anti-Malware/Endpoint Detection and Response (EDR) Policy.....	30
3.3.1	Definitions	30
3.3.1.1	Virus	30
3.3.1.2	Trojan Horse.....	30
3.3.1.3	Worm	30
3.3.1.4	Spyware.....	30
3.3.1.5	Malware	30
3.3.1.6	Adware	30
3.3.1.7	Keyloggers.....	30
3.3.1.8	Ransomware	30
3.3.1.9	Server	31
3.3.1.10	Security Incident	31
3.3.1.11	Email.....	31
3.3.2	Overview	31
3.3.3	Purpose	31
3.3.4	Audience	31

3.3.5	Policy Detail.....	31
3.4	Email Policy	33
3.4.1	Definitions	33
3.4.1.1	Anti-Spoofing	33
3.4.1.2	Antivirus	33
3.4.1.3	Electronic mail system	33
3.4.1.4	Electronic mail (e-mail)	33
3.4.1.5	Email spoofing.....	33
3.4.1.6	Inbound filters.....	33
3.4.1.7	Quarantine	33
3.4.1.8	SPAM.....	33
3.4.2	Overview	34
3.4.3	Purpose	34
3.4.4	Audience	34
3.4.5	Legal	34
3.4.6	Policy Detail.....	34
3.4.6.1	Incidental Use	36
3.4.6.2	Email Retention.....	36
3.4.6.3	Email Archive.....	36
3.5	Firewall Policy	37
3.5.1	Definitions	37
3.5.1.1	Firewall.....	37
3.5.1.2	Firewall Configuration.....	37
3.5.1.3	Firewall Ruleset/Access Control List (ACL).....	37
3.5.1.4	Host Firewall	37
3.5.1.5	Internet Protocol (IP)	37
3.5.1.6	Local Area Network (LAN)	37
3.5.1.7	Network Firewall.....	37
3.5.1.8	Network Topology.....	37
3.5.1.9	Simple Mail Transfer Protocol (SMTP)	37
3.5.1.10	Virtual private network (VPN).....	37
3.5.2	Overview	37
3.5.3	Purpose	37

3.5.4	Policy Detail.....	38
3.5.4.1	Rulesets.....	38
3.5.4.2	Protection.....	38
3.5.4.3	Configuration Management.....	39
3.5.4.4	Responsibilities	39
3.6	Hardware and Electronic Media Disposal Policy.....	41
3.6.1	Definitions.....	41
3.6.1.1	Beyond reasonable repair.....	41
3.6.1.2	Chain of Custody (CoC)	41
3.6.1.3	Disposition	41
3.6.1.4	Non-leased	41
3.6.1.5	Obsolete.....	41
3.6.1.6	Surplus.....	41
3.6.2	Overview	41
3.6.3	Purpose	41
3.6.4	Policy Detail.....	42
3.6.5	Disposal Standard	42
3.7	Security Incident Management Policy	43
3.7.1	Definitions.....	43
3.7.2	Overview	43
3.7.3	Purpose	43
3.7.4	Policy Detail.....	43
3.7.4.1	Program Organization.....	43
3.7.4.1.1	Computer Emergency Response Plans	43
3.7.4.1.2	Incident Response Plan Contents	43
3.7.4.1.3	Incident Response Testing	44
3.7.4.1.4	Incident Response and Recovery	44
3.7.4.1.5	Intrusion Response Procedures	44
3.7.4.1.6	Malicious Code Remediation	45
3.7.4.1.7	Data Breach Management	45
3.7.4.1.8	Incident Response Plan Evolution.....	45
3.7.4.2	Program Communication.....	45
3.7.4.2.1	Reporting to Third Parties.....	45

3.7.4.2.2	Display of Incident Reporting Contact Information	45
3.7.4.2.3	Customer Notification.....	45
3.8	Internet Use Policy.....	47
3.8.1	Definitions	47
3.8.1.1	Internet	47
3.8.1.2	Intranet	47
3.8.1.3	User	47
3.8.1.4	World Wide Web (www).....	47
3.8.2	Overview	47
3.8.3	Purpose	47
3.8.4	Audience	47
3.8.5	Policy Detail.....	47
3.8.5.1	Accessing the Internet	47
3.8.5.2	Expectation of privacy.....	48
3.8.5.3	File downloads and virus protection.....	48
3.8.5.4	Monitoring of computer and Internet usage.....	48
3.8.5.5	Frivolous use	48
3.8.5.6	Content	49
3.8.5.7	Transmissions.....	49
3.8.5.8	Incidental use	49
3.9	Log Management Policy.....	50
3.9.1	Definitions	50
3.9.1.1	End points	50
3.9.1.2	Flow	50
3.9.1.3	IP	50
3.9.1.4	Packet.....	50
3.9.2	Overview	50
3.9.2.1	Purpose	50
3.9.3	Policy Detail.....	51
3.9.3.1	Log generation	51
3.9.3.2	Application logs.....	51
3.9.3.3	System logs	51
3.9.3.4	Network logs	51

3.9.3.5	Time synchronization	51
3.9.3.6	Use of log information	52
3.9.3.7	Baseline behavior	52
3.9.3.8	Investigation.....	52
3.9.3.9	Log record life-cycle management.....	52
3.9.3.10	Retention	52
3.9.3.11	Log management infrastructure	52
3.10	Safeguarding Customer Information Policy	53
3.10.1	Definitions	53
3.10.1.1	Customer.....	53
3.10.1.2	Service provider	53
3.10.1.3	Personally Identifiable Information (PII).....	53
3.10.1.4	Sensitive PII	53
3.10.1.5	Non-sensitive PII	53
3.10.1.6	Customer information system	53
3.10.2	Overview	53
3.10.2.1	Purpose	54
3.10.3	Policy Detail.....	54
3.10.3.1	Information Security Program	54
3.10.3.2	Risk Assessment	54
3.10.3.3	Management and Control of Risk	54
3.10.3.4	Customer information security controls.....	55
3.10.3.4.1	Vendor management review program	55
3.10.3.4.2	Software inventory	55
3.10.3.4.3	Hardware inventory.....	56
3.10.3.4.4	Critical systems list.....	56
3.10.3.4.5	Records management	56
3.10.3.4.6	Clean desk policy.....	56
3.10.3.4.7	Hardware and electronic media disposal procedure.....	56
3.10.3.4.8	IT acquisition policy	56
3.10.3.4.9	Incident response plan.....	56
3.10.3.5	Summary of Actions	57
3.10.3.5.1	Training	57

3.10.3.5.2	Testing.....	57
3.11	Network Security and Virtual Private Network (VPN) Acceptable Use Policy	58
3.11.1	Definitions	58
3.11.1.1	Demilitarized Zone (DMZ).....	58
3.11.1.2	Virtual Private Network (VPN)	58
3.11.1.3	User Authentication.....	58
3.11.1.4	Multi-Factor/Two-Factor Authentication (MFA/2FA).....	58
3.11.1.5	Dual Homing	58
3.11.1.6	Remote Access	58
3.11.1.7	Split-tunneling.....	58
3.11.1.8	IPSec Concentrator	59
3.11.1.9	Secure Socket Layer (SSL)	59
3.11.2	Overview	59
3.11.3	Purpose	59
3.11.4	Audience	59
3.11.5	Policy Detail.....	59
3.11.5.1	Network Security	59
3.11.6	Remote Access	60
3.11.7	Requirements.....	60
3.11.8	Virtual Private Network (VPN)	61
3.11.9	VPN Encryption and Authentication	62
3.11.10	VPN Approval, Acceptable Use Review and Acceptance	62
3.11.11	Wireless Communications	62
3.11.12	Register Access Points and Cards.....	62
3.11.13	Approved Technology	62
3.11.14	Setting the Service Set Identifier (SSID)	62
3.12	Bring Your Own Device (BYOD) Policy and Agreement	63
3.12.1	Definitions	63
3.12.1.1	Bring Your Own Device (BYOD).....	63
3.12.1.2	Guest Network.....	63
3.12.2	Overview	63
3.12.3	Purpose	63
3.12.4	Audience	63

3.12.5	Policy Detail.....	63
3.12.5.1	Accessing the Internet from the Camrosa Guest Network.....	63
3.12.5.2	Responsibilities of the District	64
3.12.5.3	Responsibilities of BYOD Participants.....	65
3.12.5.4	Help and Support	66
3.13	Patch Management Policy	67
3.13.1	Overview	67
3.13.2	Purpose	67
3.13.3	Audience	67
3.13.4	Policy Detail.....	67
3.13.4.1	Common Vulnerabilities and Exposures	67
3.13.4.2	Responsibility	67
3.14	Physical Access Control Policy.....	69
3.14.1	Overview	69
3.14.2	Purpose	69
3.14.3	Policy Detail.....	69
3.15	Cloud Computing Policy	70
3.15.1	Definitions.....	70
3.15.1.1	Cloud computing.....	70
3.15.1.2	Public cloud.....	70
3.15.1.3	Private Cloud.....	70
3.15.1.4	Financial information	70
3.15.1.5	Intellectual property	70
3.15.1.6	Other non-public data or information	70
3.15.1.7	Other public data or information.....	70
3.15.1.8	Personally Identifiable Information (PII).....	70
3.15.2	Overview	70
3.15.3	Purpose	70
3.15.3.1	Security	71
3.15.3.2	Data Governance	71
3.15.3.3	Encryption.....	71
3.15.3.4	Antivirus Detection	71
3.15.3.5	User Authentication.....	71

3.15.3.6	Regulatory Compliance	71
3.15.3.7	Certifications & Standards	71
3.15.3.8	Other Service Level Agreement (SLA) Criteria	71
3.15.4	Policy Detail.....	72
3.15.4.1	Cloud Computing Services	72
3.15.4.2	Privacy Concerns.....	72
3.15.4.3	Exit Strategy	73
3.15.4.4	Diligence.....	73
3.15.5	Approved and Non-approved Cloud Services	73
3.16	Server Security Policy.....	74
3.16.1	Overview	74
3.16.2	Purpose	74
3.16.3	Policy Detail.....	74
3.16.3.1	Responsibilities	74
3.16.3.2	Supported Technology.....	75
3.16.4	Social Media Acceptable Use Policy.....	76
3.16.4.1	Definitions.....	76
3.16.4.1.1	Anonymous content	76
3.16.4.1.2	District Official	76
3.16.4.1.3	Facebook.....	76
3.16.4.1.4	LinkedIn.....	76
3.16.4.1.5	Microblogging	76
3.16.4.1.6	Social Media.....	76
3.16.4.1.7	Twitter.....	76
3.16.4.1.8	YouTube	76
3.16.4.2	Overview	76
3.16.4.3	Purpose of Using Social Media.....	77
3.16.5	Policy Detail.....	77
3.16.5.1	Terms and Conditions of Use	77
3.16.5.2	Representing the Camrosa Water District.....	78
3.16.5.3	Personal Blogs and Posts	78
3.16.5.4	Rules of Engagement	79
3.16.5.5	Rules of Composition	79

3.17	System Monitoring and Auditing Policy.....	81
3.17.1	Overview	81
3.17.2	81
3.17.3	Policy Detail.....	81
3.18	Vulnerability Assessment Policy	82
3.18.1	Overview	82
3.18.2	Purpose	82
3.18.3	Policy Detail.....	82
3.19	Website Operation Policy	83
3.19.1	Overview	83
3.19.2	Purpose	83
3.19.3	Policy Detail.....	83
3.19.3.1	Responsibility	83
3.19.3.2	Links	83
3.19.3.3	Security	84
3.19.3.4	Website Changes	84
3.19.3.5	Regulatory Compliance	84
3.19.3.6	Website Design	84
3.20	Workstation Configuration Security Policy.....	85
3.20.1	Definitions	85
3.20.1.1	Domain.....	85
3.20.2	Overview	85
3.20.3	Purpose	85
3.20.4	Policy Detail.....	85
3.20.4.1	Responsibilities	85
3.20.4.2	Supported Technology.....	86
3.21	Wireless (WiFi) Connectivity Policy.....	87
3.21.1	Definitions	87
3.21.1.1	Wireless Access Point (AP).....	87
3.21.1.2	Guest Network.....	87
3.21.1.3	Keylogger	87
3.21.1.4	WiFi	87
3.21.1.5	Wireless.....	87

3.21.2	Overview	87
3.21.3	Policy Detail.....	87
3.21.3.1	District Guest WiFi Network	87
3.21.3.2	Public WiFi Usage.....	88
3.22	Telecommuting Policy and Agreement.....	90
3.22.1	Definitions.....	90
3.22.1.1	Telecommuting	90
3.22.1.2	Telecommuting Agreement (TA)	90
3.22.2	Overview	90
3.22.3	Purpose	90
3.22.4	Policy Detail.....	90
3.22.4.1	Eligibility Criteria	90
3.22.4.2	Telecommuting Assignment	91
3.22.4.3	General Duties, Obligations and Responsibilities	92
3.23	Data Backup and Recovery Policy	94
3.23.1	Definitions.....	94
3.23.1.1	Data Backup	94
3.23.1.2	Data Recovery	94
3.23.1.3	Archive	94
3.23.1.4	Full Backup	94
3.23.1.5	Differential Backup	94
3.23.1.6	Incremental Backup	94
3.23.1.7	GFS Backup.....	94
3.23.1.8	Recovery Point Objective (RPO).....	94
3.23.1.9	Recover Time Objective (RTO)	94
3.23.2	Overview	94
3.23.3	Purpose	95
3.23.3.1	Scope.....	95
3.23.4	Policy Detail.....	95
3.23.4.1	Backup Schedule	95
3.23.4.2	Recover Point Objective (RPO)	95
3.23.4.3	Recovery Time Objective (RTO)	95
3.23.4.4	Retention	95

3.23.4.5	Responsibility	95
3.23.4.6	Backup and Restoration Testing	95
3.23.4.7	Storage Locations.....	95
3.23.4.8	Restoration.....	96
3.24	Personal Storage Backup and Recovery Policy and Procedure.....	97
3.24.1	Overview	97
3.24.2	Accessing files	97
3.24.3	File Revision Retention.....	97
3.24.4	Access to OneDrive	98
3.25	Internet Of Things Policy.....	99
3.25.1	Definitions	99
3.25.1.1	Internet of Things (IoT)	99
3.25.1.2	Data points.....	99
3.25.2	Overview	99
3.25.3	Purpose	99
3.25.4	Policy Detail.....	99
3.25.4.1	IoT Device Procurement	99
3.25.4.2	Cybersecurity Risks and Privacy Risk Considerations	99
APPENDIX A	Receipt of Acceptable Use of the Camrosa Water District’s Information Systems.....	i
APPENDIX B	Camrosa Water District – Notice of Data Breach	ii
APPENDIX C	Virtual Private Network (VPN) Use Agreement.....	iv
APPENDIX D	Bring Your Own Device (BYOD) Agreement	v
Appendix E	Cloud Computing Adoption	vii
APPENDIX F	Telecommuting Agreement	viii
APPENDIX G	Telecommuting Equipment Checkout Sheet	x
APPENDIX H	IoT Device Usage Request Form.....	xi

1. Introduction

The Camrosa Water District Information Technology Policies and Procedure Manual provides the policies and procedures for selection and use of IT within the District institution which must be followed by all staff and/or contractors who use the District's data and communication systems. It also provides guidelines the District will use to administer these policies, with the correct procedures to follow. The District will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

The District fully leverages on technology when possible. This includes servers, storage, networking, and other devices that are typically referred to as "Information Technology" (IT). But it also includes industrial controls such and Programmable Logic Controllers (PLC's) and automation of Supervisory Control and Data Acquisition (SCADA) tasks that monitor reservoir levels, which in turn, control drinking water wells and booster pump production. This field of technology is typically referred to as "Operational Technology" (OT). For brevity, the term IT will often be used to in this document to include both IT and OT environments. When distinction is necessary, either or both terms will be used.

1.1 Camrosa IT Department

Management of Camrosa's IT environment is divided into functional areas that include, but are not limited to, administration of local/wide area networks, servers, security, domain, applications, industrial controls, data management, telephony, and other forms of voice communications. While there is some overlap in administration of these duties, the definition of roles and structure of the IT Department is provided. The IT Department at Camrosa consists of the following entities:

- IT Manager - An employee of the District, the duty of the IT Manager is to provide general oversight and administration of the day-to-day operations and activities of the District's data and communications infrastructure. Additional duties of the IT Manager include:
 - Development, maintenance, and adherence of policies, procedures, and standards to protect the privacy and integrity of applications and data.
 - Ensure internal IT security policies, procedures, guidelines, standards, and activities align with all state and/or federal regulatory requirements.
 - Development of the District's short and long-range IT plans and the practical implementation of the District's IT strategies.
 - Oversee the annual preparation and execution of the IT Department's capital improvement and expense budgets.
 - Oversee the use of technology within the organization in order to assess potential risks that could compromise sensitive information.
 - Provide guidance, oversight, and management of IT tasks relegated to the District's IT/OT Managed Service Provider(s).
- Operations Supervisor – An employee of the District, the duties of the Operations Supervisor include oversight and administration of the District's OT network which includes all equipment necessary for the automation of the District's industrial controls systems.

- AllConnected Incorporated, Simi Valley, California - Contracted IT/OT Managed Service Provider (IT/OT MSP) provide the following services for the District:
 - Helpdesk services.
 - Basic and advanced technical support for network, systems, and security infrastructure.
 - 24x7 monitoring, alerting and escalation
 - Repair and upkeep of network, data center and server hardware
 - Firewall/Security
 - IT vendor management
 - Engineering/Consulting
 - Managed backup and disaster recovery
 - IT/OT support as needed

2. Information Technology Procurement, Acquisition, and Support Policy

2.1 Overview

Leveraging on the effective use of information technology is one approach available to the District in achieving its goals of improving organizational productivity, Industrial Control System (ICS) automation, customer service efficiency, public outreach and customer access to account information. However, careful consideration must be given in the procurement and acquisition of new IT systems to control costs, ensure compatibility, future supportability, and determine the impacts and risks these new systems may have to cyber security. The purpose of this policy, and in accordance with District strategic planning, is to define standards, procedures, and restrictions for the procurement and acquisition of all IT hardware, software, computer-related components, and technical services purchased with District funds. Purchase of technology and technical services for the District must be approved and coordinated through the IT Department.

2.2 IT Procurement Categories

Purchasing within the IT Department falls under four general categories. In the event of any inconsistency, conflict, or ambiguity between the District's overarching procurement policy (currently defined under Resolution 20-06) and the procurement categories defined here, then the procurement policy defined under Resolution 20-06 shall take precedence.

2.2.1 Standard Items

Standard items include purchase of items which have been pre-approved by the IT Department and require only a Service Desk request and are limited in costs and/or quantity; typically, one-thousand dollars or less.

2.2.2 Non-Standard Items

Non-standard items are defined as hardware or software not previously approved by the IT Department. Such purchases should be minimized as much as reasonably possible. Requests for non-standard items will go through a formal selection process that will involve thorough vendor sourcing. The IT Department will review non-standard purchases for viability of support and compatibility. The selection process may vary depending on the type, cost, and other significant factors. Before approval will be granted, employees or departments requesting non-emergency specialized software, or components, must describe how this item will be supported. Support options include assigning a staff member (or members) to maintain and/or support the component or arranging for a service-level agreement with the hardware or software vendor. Individuals requesting non-standard items for purchase can suggest a potential vendor, if a pre-existing relationship exists between that vendor and the District.

2.2.3 IT Capital Project Expenses

IT capital project expenses may include purchase of standard and non-standard capitalized hardware, software, or equipment and which are typically above \$1,000.00 with life of 3 years or more and are approved through the standard budgetary process or as specified in the District's Fixed Asset and Capital Asset Policy. Capitalized expenses must go through the General Manager and Board of Directors for approval. IT capital project expenses may only be requisitioned by or at the authorization of the IT Manager and the Finance Manager. The purchase selection process for these expenditures may be evaluated the General Manager.

The procurement and acquisition of major IT systems should be accomplished by working from an established district-wide priority list. These capital expenses should also adhere to the District's short and long range technology road-maps established through strategic planning, management and the Camrosa Water District, Board of Directors.

2.2.4 Employee Purchases

Employee purchases include purchase of IT related hardware and software by individual District staff members. These purchases are typically less than \$250 and are required immediately by an individual to maintain productivity. Such purchases will require no pre-authorization by the IT Department however, post-purchase ratification by the IT Manager shall still be required.

2.2.5 IT Emergency Procurements

Emergency procurements related to IT may be required if and when an unforeseen catastrophic event occurs within the District's IT environment that affect the District's ability to continue to function. While this condition is very rare it should and must be addressed within this policy. For contrast, a shortfall of funds at the end of the fiscal year does not constitute an IT emergency.

The District's IT Manager is responsible for timely reporting to the General Manager if and when an IT catastrophic event occurs and to what extent such an event may impact the operations of the District. The District's IT Manager (with the possible assistance of the District's Finance Manager) will develop a written cost solution that will mitigate the adverse event and present it to the General Manager. The General Manager is responsible for timely reporting to the Camrosa Board of Directors of any unforeseen catastrophic IT events. However, at the discretion of the General Manager, an immediate purchase of IT goods or services to mitigate the catastrophic adverse event may be procured without prior Board approval. The General Manager shall return to the Board for immediate ratification at the next available board meeting.

The District should solicit as much competition as practical for emergency procurements; however, emergency procurements may be conducted without competition.

2.2.6 IT Planned Maintenance and IT Outside Contract Support Costs

This IT cost category includes purchase of goods and services that have been adopted in the Information Systems Program budget of the District's annual Operating & Capital Budget Fiscal Year document.

2.3 New System Implementation and Support

The District will only acquire new equipment, applications or systems if the skills and resources to effectively implement, manage and support them are available. Accordingly, the following issues will be fully considered and evaluated before acquiring or developing new systems:

- Costs (both initial implementation and ongoing support)
- Benefits
- Impacts on cyber security
- Hardware and software compatibility
- Availability of adequate implementation, maintenance, and support resources
- Training requirements

2.3.1 Centralized vs. Departmental Acquisition and Support Responsibilities

In general, District departments (Operations, Customer Service, etc.) are responsible for managing and supporting their applications; and IT is responsible for managing and supporting the technical environment in which these user applications operate (workstations, application servers, printers, data communications, local and wide area networks, operating system, and desktop software).

- **Application Support.** The responsibility for acquiring and supporting applications that meet focused functional requirements – such as operational industrial control systems, geographical information systems, customer service and finance systems – generally lies with their respective departments. This reflects the fact that departmental users are the best suited to evaluate and use the features of new applications and to support them.
- **IT Staff/MSP Technical Support.** In the case of District-wide applications such as word processing, spreadsheets, presentation graphics, and email, responsibility for acquiring and supporting applications generally lies with the IT Department and/or its managed service provider.
- **Third-party Major System/Application Support.** For major system/application support, the District should enter into a Service Level Agreement (SLA) with system/application vendors to clearly define the roles, responsibilities, service scope and performance standards of both parties.

2.3.2 Software Licensing

All software, including application, operating system, or firmware will be used in conformance with license agreements and copyright laws.

2.4 IT Asset Management

Qualified IT assets procured by the IT Department shall be duly managed with the objective of protecting them from misappropriation and unplanned obsolescence. Management of these assets shall adhere to the District's Fixed Asset and Capital Asset Policy with the purpose of identification, location, tracking, lifecycle, reporting, and disposition.

2.5 IT Lifecycle Management

IT lifecycle management is the planning, acquisition, implementation, maintenance, and retirement of key IT infrastructure components that are essential to support the District's business functions. For planning purposes, new procurements of major IT systems, applications and equipment shall have a serviceable life of 3-5 years for system hardware components and 5-10 years for application support. From the date of purchase/procurement, systems shall have a planned end-of-life of no more than 15 years. Consideration will be given to the current age and supportability of IT systems, applications, and equipment as part of the annual budgetary process.

2.6 Roles and Responsibilities

2.6.1.1 Policies

The Camrosa Board of Directors is responsible for adopting district-wide IT policies. These are generally set forth in the IT Strategic Plan. The General Manager recommends to the Board, new policies, and revisions of existing policies.

2.6.2 Short- and Long-Term Technology Road Maps

Camrosa Management is responsible for maintaining a comprehensive IT Master Plan that sets the overall direction, purpose and priorities for the District's development and use of information technology resources. The General Manager has overall responsibility for developing this plan, presenting it to the Board for their approval, and for ensuring implementation after its adoption.

2.6.3 Resources

The Camrosa Board of Directors is responsible for allocating the resources necessary to acquire, manage, operate and maintain the District's information technology systems. The Board also approves specific acquisitions consistent with the District's purchasing policies. Based on an approved priority list, the General Manager makes specific recommendations to the Board regarding the allocation of resources and system acquisitions.

2.6.4 Organization

The General Manager is responsible for the effective management and operation of the District's information technology activities. To assist the General Manager in fulfilling this responsibility, the Information Technology Steering Committee is established under this policy and their responsibilities as well as those of the district departments are identified. The General Manager may modify the membership and responsibilities of the IT Steering Committee and departments as he or she deems appropriate in achieving the overall goals and objectives set forth in this policy as well as in the IT Strategic plan.

2.6.5 Information Technology Steering Committee

2.6.5.1 Responsibilities

The IT Steering Committee is responsible for:

- Coordinating development and implementation of the IT strategic plan; monitoring progress in achieving plan goals and objectives; and recommending long and short range plan updates to the General Manager on a periodic basis or as needed.
- Developing and approving IT standards and policies governing all data systems used by the District that would have significant organizational or budgetary impacts.
- Developing and approving operational policies and procedures, consistent with plans and policies set forth in the adopted IT Strategic Plan.
- Reviewing departmental proposals for new hardware and application and making recommendations to the General Manager for inclusion in the priority list as appropriate.
- Approving organization-wide IT training strategies.
- Monitoring and overseeing the implementation and performance of existing and proposed IT hardware and applications, including major capital projects.
- Facilitating research of new and emerging trends in technologies to ensure future system viability and supportability

2.6.5.2 Membership

The IT Steering Committee consists of the following members:

- District Assistant General Manager, who serves as the Committee Chair

- IT Manager/IT Coordinator
- District Finance Manager
- Operations and Maintenance Supervisor
- Chief Technology Officer – As of this writing, AllConnected Incorporated of Simi Valley, California is providing this service.

2.6.5.3 Meetings

The IT Steering Committee will meet as necessary to fulfill its responsibilities. With the concurrence of their department head, other employees interested in these issues are welcome to attend these meetings and offer their comments and advice.

3. Cyber Security Policies

Cyber security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of services they provide. Effective cyber security is a team effort involving the participation and support of every Camrosa employee and affiliate who deals with the District's information and information systems. It is the responsibility of every District computer user to know these guidelines and to conduct their activities accordingly. The policies and procedures defined in this section segment the somewhat nebulous topic of cyber security into functional areas to address key areas and minimize risk to information systems. These include:

- Acceptable use of Information Systems Policy and Agreement
- User Account/Password Management
- Anti-Malware/Endpoint Detection and Response (EDR)
- Email
- Firewall
- Hardware and Electronic Media Disposal
- Security Incident Management
- Internet Use
- Log Management
- Safeguarding Customer Information
- Network Security and Virtual Private Network (VPN) Acceptable Use Policy and Agreement
- Bring Your Own Device (BYOD) Policy and Agreement
- Patch Management
- Physical Access Control
- Cloud Computing Adoption
- Server Security
- Social Media Acceptable Use
- System Monitoring and Auditing
- Vulnerability Assessment
- Website Operation
- Workstation Configuration Security
- Wireless (WiFi) Connectivity
- Telecommuting
- Data Backup and Recovery
- Internet of Things
- Mobile Device Management (MDM)

3.1 Acceptable Use of Information Systems Policy

3.1.1 Overview

Data, electronic file content, information systems, and computer systems at the Camrosa Water District must be managed as valuable organization resources. The Information Technology (IT) department's intentions are not to impose restrictions that are contrary to the District's established culture of trust, and integrity. IT is committed to protecting the District's authorized users and the organization in whole from illegal or damaging actions by individuals either knowingly or unknowingly. IT related systems, including but not limited to:

- Local Area Networks (LANs)
- Wide Area Networks (WANs)
- Internet
- Intranet
- Computers (Servers and Workstations)
- Operating Systems
- User Accounts
- Email
- Industrial Control Systems (ICS)
- Firewalls/Bridges/Routers
- File Repositories

are the property of the District. These systems are to be used for business purposes in serving the interests of the District.

3.1.2 Purpose

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

3.1.3 Scope

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

All employees, directors, contractors, consultants, temporaries, or any other affiliates conducting business for the District are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Camrosa policies and standards, local laws, and regulations.

3.1.4 Policy Detail

3.1.4.1 Ownership of Electronic Files

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

3.1.4.2 Privacy

All electronic files created, saved, sent, received, printed or stored on Camrosa owned, leased, or administered equipment, or otherwise under the custody and control of the District are not private and may be intercepted, monitored, recorded, and accessed by the Camrosa IT Department for all legal purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access and to verify security procedures any time without knowledge of the user, sender, recipient, or owner. Electronic file content may also be accessed by appropriate personnel in accordance with any/all directives from Human Resources or the General Manager.

3.1.4.3 General Use and Ownership

Access must be authorized and submitted from departmental supervisors 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 corporate systems immediately become the property of Camrosa. Because of the need to protect the District's network and computer systems, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to the District.

For security and network maintenance purposes, authorized individuals within the Camrosa's IT Department may monitor equipment, systems, and network traffic at any time. The IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Further, the IT Department reserves the right to remove any non-business related software or files from any system as they deem appropriate. 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.

3.1.4.4 Security and Proprietary Information

All mobile and computing devices that connect directly or indirectly to the District's internal networks must comply with this policy and the following District cyber security policies:

- Account Management
- Anti-Virus
- Owned Mobile Device Acceptable Use and Security
- E-mail
- Internet
- Safeguarding Member Information
- Bring Your Own Device (BYOD)
- Password
- Cloud Computing
- Wireless (WiFi) Connectivity
- Telecommuting

Domain level and user level passwords must comply with the Password Policy. Authorized users must not share their 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 District 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.

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

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

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

3.1.4.5 Unacceptable Use

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

Under no circumstances is an employee, director, contractor, consultant, temporary, or any other affiliate conducting business for the District authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing district-owned resources.

3.1.4.6 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 Camrosa.
- 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 the District or the end user does not have an active license is prohibited. Users must report unlicensed copies of installed software to the IT Department.
- 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 or remotely through a virtual private network (VPN) connection.
- Using a District 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 district-owned 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 the District’s IT Department.
- Installing or using non-standard shareware or freeware software without the District’s IT Department approval.
- Installing, disconnecting, or moving any district-owned computer equipment and peripheral devices without prior consent of District’s IT Department.
- Purchasing software or hardware, for District use, without prior IT compatibility review.
- Purposely engaging in activity that may degrade the performance of information systems.

- Purposely engaging in activity that may deprive an authorized district user access to a District resource.
- Purposely engaging in activity that may use additional resources beyond those allocated.
- Purposely engaging in activity that may circumvent the District's computer security systems and controls.
- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on district-owned information systems. The District's IT Department is the only department authorized to perform these actions.
- Purposely engaging in activity that may degrade access or employ a 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 connectivity, via any means, locally or via the Internet.
- Access to the Internet at home, from a district-owned computer, must adhere to all the same policies that apply to use from within Camrosa facilities. Authorized users must not allow family members or other non-authorized users to access district-owned computer systems.
- District information systems must not be used for personal benefit.

3.1.4.7 Incidental Use

As a convenience to Camrosa employees, directors, contractors, consultants, temporaries, or any other affiliates conducting business for the District, 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 approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to the District 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 the District.
- Storage of personal email messages, voice messages, files, and documents within the District's information systems must be minimal.
- All messages, files, and documents — including personal messages, files, and documents — located on District information systems are owned by Camrosa, may be subject to open records requests, and may be accessed in accordance with this policy.

3.1.4.8 Review and Acceptance

All Camrosa staff are responsible for review and acceptance of Acceptable Use of Information systems policy upon starting work at the Camrosa Water District (see Appendix A).

New employee onboarding and training shall include this policy 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 the IT Manager.

3.2 User Account/Password Management Policy

3.2.1 Overview

Computer accounts are the means used to grant access to Camrosa's information systems. These accounts provide a means of providing centralized authorization and accountability, and are vital to the cyber security program at the District. This implies the creation, control, and monitoring of all computer accounts is extremely important to an overall security program.

3.2.2 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 the District.

3.2.3 Audience

This policy applies to all employees, directors, contractors, consultants, temporaries, or any other affiliates conducting business for the District, including all personnel affiliated with third parties with authorized access to any District information system.

3.2.4 Policy Detail

3.2.4.1 Account Names and Passwords

- All accounts must be uniquely identifiable using the assigned username.
- Shared accounts on District information systems are not permitted.
- Concurrent connections may be limited for technical or security reasons.
- All accounts must be disabled immediately upon notification of any employee's termination.
- Passwords for the District network access must be implemented according to the following guidelines:
 - Passwords must be changed every 90 days.
 - Passwords must adhere to a minimum length of 10 characters.
 - Passwords must contain a combination of uppercase, lowercase, numeric, and special characters.
 - Passwords must not be easily tied back to the account owner's username, social security number, nickname, relative's names, birth date, etc.
- Passwords must not be dictionary words or acronyms.
- Passwords cannot be reused for 1 year.

3.2.4.2 Account Management

The following items apply to System Administrators or 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 District management.
- An independent audit review may be performed to ensure the accounts are properly managed.

3.2.4.3 System-Level/Administrator Passwords

All system-level (or Admin 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 following four items: uppercase, lowercase, 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

3.2.4.4 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 District 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").
- Passwords must not be shared with anyone, including co-workers, managers, or family members.
- 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 IT 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 IT. 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.
- Security tokens (i.e. smartcards, hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with the District.

3.3 Anti-Malware/Endpoint Detection and Response (EDR) Policy

3.3.1 Definitions

3.3.1.1 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.

3.3.1.2 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.

3.3.1.3 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.

3.3.1.4 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.

3.3.1.5 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.

3.3.1.6 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.

3.3.1.7 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).

3.3.1.8 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.

3.3.1.9 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.

3.3.1.10 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.

3.3.1.11 Email

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

3.3.2 Overview

Malware threats must be managed to minimize the downtime of Camrosa systems and prevent risk to critical systems and customer data. This policy is established to:

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

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

3.3.3 Purpose

This policy is established to help prevent infection of District 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.

3.3.4 Audience

This policy applies to all computers connecting to the District 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 District network.

3.3.5 Policy Detail

All computer devices, including servers, workstations, laptops, tablets, cell phones, or mobile devices of any kind that are connected to the District network or 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 IT 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.

Anti-virus software used by the District shall incorporate both traditional signature-based anti-virus protection and next-generation anti-virus features, commonly known as Endpoint Detection and Response (EDR) which include halting of: data exfiltration; the use of legitimate operating system executable such as MS Powershell and Windows Management Instrumentation (WMI) for malicious purposes; and other non-malware attacks that may otherwise go undetected by traditional signature-based, anti-virus algorithms.

All e-mail services including on-premise or hosted implementations (e.g. MS Exchange Online) must utilize Advanced Threat Protection that will preemptively monitor, quarantine, and delete emails containing harmful attachments and links. Users, prior to accessing or connecting to email services of any kind from the District network, including personal email accounts, must obtain IT approval.

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 District's IT Manager.

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 District network until the infection has been removed.

3.4 Email Policy

3.4.1 Definitions

3.4.1.1 Anti-Spoofing

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

3.4.1.2 Antivirus

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

3.4.1.3 Electronic mail system

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

3.4.1.4 Electronic mail (e-mail)

Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

3.4.1.5 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.

3.4.1.6 Inbound filters

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

3.4.1.7 Quarantine

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

3.4.1.8 SPAM

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

3.4.2 Overview

E-mail at Camrosa 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.

3.4.3 Purpose

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

3.4.4 Audience

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

3.4.5 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

3.4.6 Policy Detail

District email is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on District computer systems. Camrosa can, but is not obliged to, monitor emails without prior notification. All emails, files, and documents – including personal emails, files, and documents – are owned by the District and 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 District systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, the IT Department 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 IT Department 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.

Email 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 virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm the District'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 email for conducting personal business.
- Using email for the purposes of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.
- Sending email using another person's email account, except when authorized as a delegate to send messages for another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- Forging or attempting to forge email messages.
- Using unauthorized email software.
- Knowingly disabling the automatic scanning of attachments on any District personal computer.
- Knowingly circumventing email security measures.
- Sending or forwarding joke emails, chain letters, or hoax letters.
- Sending unsolicited messages to large groups, except as required to conduct District business.
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding email with computer viruses.
- Setting up or responding on behalf of the District without proper approval.

All confidential or sensitive District material transmitted via email, outside the District network, must be encrypted. Passwords to decrypt the data should not be sent via email.

Email is not secure. Users must not email passwords, social security numbers, account numbers, PIN numbers, dates of birth, mother's maiden name, etc. to parties outside the District network without encrypting the data. All user activity on Camrosa information system assets is subject to logging and review. The District has software and systems in place to monitor email usage.

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

Users must not send, forward, or receive confidential or sensitive District information through non-District email accounts unless appropriately authorized (explicitly or implicitly) to do so. Examples of

non-District email 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-District owned mobile devices must adhere to the Bring Your Own Device (BYOD) Policy for sending, forwarding, receiving, or storing confidential or sensitive District information.

3.4.6.1 Incidental Use

Incidental personal use of sending e-mail is restricted to District 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 the District. 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 the District. Storage of personal files and documents within the District's information systems should be minimal.

3.4.6.2 Email Retention

- Messages are retained for 36 months. Emails older than 36 months are subject to automatic purging.
- Deleted and archived emails are subject to automatic purging.
- Appointments, Tasks, and Notes older than the retention period are subject to automatic purging.

3.4.6.3 Email Archive

- Only the owner of a mailbox and the system administrator has access to the archive.
- Messages will be deleted from the online archive 36 months from the original send/receive date.

3.5 Firewall Policy

3.5.1 Definitions

3.5.1.1 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.

3.5.1.2 Firewall Configuration

The system setting affecting the operation of a firewall appliance.

3.5.1.3 Firewall Ruleset/Access Control List (ACL)

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

3.5.1.4 Host Firewall

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

3.5.1.5 Internet Protocol (IP)

Primary network protocol used on the Internet.

3.5.1.6 Local Area Network (LAN)

A grouping of network enabled devices that communicate on the datalink layer of the Open Standard Interconnect (OSI) model and are logically grouped to share a set of functions (e.g., a server LAN or workstation LAN)

3.5.1.7 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).

3.5.1.8 Network Topology

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

3.5.1.9 Simple Mail Transfer Protocol (SMTP)

An Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

3.5.1.10 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.

3.5.2 Overview

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

3.5.3 Purpose

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

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

- Control access 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 multifactor authentication.
- Provide virtual private network (VPN) connectivity.

3.5.4 Policy Detail

All network firewalls, installed and implemented, must conform to best management practices and recommendations laid out within the National Institute of Standards and Technology (NIST) Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

3.5.4.1 Rulesets

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

- Outbound traffic from internal sources on the District network to external destinations (internet) will be authorized on an as needed basis by the IT Department.
- Inbound traffic from external sources (internet) to internal destination on the District network will be authorized on an as needed basis by the IT Department
- Packet filtering – selective passing or blocking of data packets as they pass through a network interface will be allowed/denied based on:
 - Source and destination Internet Protocol (IP) address.
 - Source and destination port and/or service.
 - Schedule or time-of-day.
 - Security profiles including anti-virus, web, DNS, application, file, email, and SSL inspection.
 - Stateful Inspection technology that monitors the state of active connections and uses this information to determine which network packets to allow/deny through the firewall.
- Firewalls will be configured to limit inbound and outbound traffic, to the fullest extent possible, with the Internet and between the following Local Area Networks:
 - Servers
 - Workstations
 - SCADA
 - Voice-Over-IP (VOIP)

3.5.4.2 Protection

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 network traffic and the attacker does not care about receiving responses to the attack packets.
- Any traffic that would exploit known Common Vulnerabilities and Exposures (CVE's) in firmware, operating systems or application software listed within the cve.mitre.org database (which also feeds the NIST National Vulnerability Database or NVD)
- Any network information utility that could be used reveal information about the District's internal networks.
- Known anti-virus signatures
- Known malicious websites

3.5.4.3 Configuration Management

A change control process is required before any firewall rules are modified. Prior to implementation, District network administrators are required to have the modifications approved by the IT Manager. All related 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:

The District must review all network firewall rulesets and configurations during the initial implementation process and periodically thereafter.

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.

3.5.4.4 Responsibilities

The IT Department is responsible for implementing and maintaining District 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 District's Password Policy.

The specific guidance and direction for information systems security is the responsibility of IT Department. Accordingly, the IT Department will manage the configuration of the District's firewalls.

The District has contracted with a Third Party Vendor, AllConnected Inc. of Simi Valley, California to manage the external firewalls. This vendor will be responsible for:

- Retention of the firewall rules
- Patch Management
- Review of firewall logs for:

- System errors
- Blocked web sites
- Attacks
- Sending alerts to the IT Manager in the event of attacks or system errors
- Backing up the firewalls

3.6 Hardware and Electronic Media Disposal Policy

3.6.1 Definitions

3.6.1.1 Beyond reasonable repair

Refers to all equipment whose condition requires fixing or refurbishing that is likely to cost as much or more than total replacement.

3.6.1.2 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.

3.6.1.3 Disposition

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

3.6.1.4 Non-leased

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

3.6.1.5 Obsolete

Refers to all equipment that no longer meets requisite functionality.

3.6.1.6 Surplus

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

3.6.2 Overview

Hardware and electronic media disposition is necessary at the District to ensure the proper disposition of all non-leased District IT hardware and media capable of storing customer information. Improper disposition can lead to potentially devastating fines and lawsuits, as well as possible irreparable brand damage.

3.6.3 Purpose

District 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.

The District'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 District upgrade guidelines.

All disposition procedures for retired IT assets must adhere to District approved methods.

3.6.4 Policy Detail

The IT Department is responsible for backing up data from IT assets slated for disposition (if applicable) and removing District tags and/or identifying labels. The IT Department is responsible for selecting and approving external agents for hardware sanitization, reselling, recycling, or destruction of the equipment. The IT Department 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 member of the District's IT Department, with the appropriate authority, to ensure that IT assets are disposed of according to the disposal standards in this Hardware and Electronic Media Disposal Policy. It is imperative that all dispositions are done appropriately, responsibly, and according to IT lifecycle standards, as well as with the District'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)
- Backup tapes
- CDs and DVDs
- Zip and thumb drives
- Hard drives / Flash memory
- Other portable storage device

3.6.5 Disposal Standard

The District will follow all state and federal regulations (or recommendations) for proper disposal of electronic waste in order to protect the environment from toxic elements like battery acid, lead, and mercury. The District will also adhere to all state and federal regulations for ensuring all electronic recordable media has been properly sanitized as part of the disposal process to ensure the confidentiality of any Personally Identifiable Information (PII) that may reside on such media.

3.7 Security Incident Management Policy

3.7.1 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.

3.7.2 Overview

- Security Incident Management at Camrosa is necessary to detect unauthorized access, determine the magnitude of any threat presented by these security incidents, respond to these incidents, and as required, notify District stakeholders (staff, board members, and customers) and law enforcement of the breach.

3.7.3 Purpose

This policy defines the requirement for reporting and responding to incidents related to the District's information systems and operations. Incident response provides the District 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 simply noted and corrected.

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

- Servers and other devices that provide centralized computing capabilities.
- Data repositories and other 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 staff or customer information occurs, the District is required by California state law to notify these individuals as described in California Civil Code 1798.29, Accounting of Disclosures.

3.7.4 Policy Detail

3.7.4.1 Program Organization

3.7.4.1.1 Computer Emergency Response Plans

The District IT Department 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. Examples include internet connectivity is interrupted or an isolated malware discovery.

3.7.4.1.2 Incident Response Plan Contents

The District's incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of any third-party hardware and software support vendor with whom the District maintains a Service Level Support Agreement (SLA) and it could be reasonably believed the security incident affects the support vendor as well. 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

3.7.4.1.3 Incident Response Testing

At least once every year, the IT Department must utilize simulated incidents to mobilize and test the adequacy of response. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with the District's General Manager.

3.7.4.1.4 Incident Response and Recovery

A security incident response capability will be developed and implemented for all District information systems that house or access District 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 appropriate District staff.

3.7.4.1.5 Intrusion Response Procedures

The IT Department 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.

3.7.4.1.6 Malicious Code Remediation

Steps followed will vary based on scope and severity of a malicious code incident as determined by the IT Manager. 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.

3.7.4.1.7 Data Breach Management

The District's IT Department 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 data.

3.7.4.1.8 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 revisions in best-management-practices (BMPs) for protecting Water Utility - Critical Infrastructure (CI) from cyber attacks.

3.7.4.2 Program Communication

3.7.4.2.1 Reporting to Third Parties

Unless required by law or regulation to report information security violations to external authorities, Camrosa management, in conjunction with legal representatives, IT Department must weigh the pros and cons of external disclosure 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.
- If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Security Officer must be notified immediately.

3.7.4.2.2 Display of Incident Reporting Contact Information

The District 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.

3.7.4.2.3 Customer Notification

The notification will be conducted and overseen by the District's General Manager or his/her appointed head of the Risk Management team. Pursuant to California Civil Code 1798.29, the notification must contain, at a minimum, the following elements:

- The Security Breach Notification shall be written in plain language
- The notification shall be titled "Notice of Data Breach"
- Shall present in paragraph (2) of the notification under the following headings:
 - "What Happened?"
 - "What Information Was Involved?"
 - "What We Are Doing"
 - "What You Can Do"
 - "For More Information"

Additionally, the date of the breach (or estimated date of the breach, or a date range of the breach) shall be provided in the notice if it is known at the time the notice is provided. The breach notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. The notice may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. However, the notice must state it was delayed due to these circumstances. The toll-free telephone numbers and addresses of the major credit reporting agencies shall be provided in the notice if the breach exposed a social security number, driver's license, or California identification card number. At the discretion of the District, the notice may also include advice on steps that individuals whose information has been breached may take to protect themselves.

A sample Security Breach Notification can be found in Appendix B of this document.

3.8 Internet Use Policy

3.8.1 Definitions

3.8.1.1 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.

3.8.1.2 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.

3.8.1.3 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.

3.8.1.4 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.

3.8.2 Overview

Internet access and usage at Camrosa must be managed as a 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.

3.8.3 Purpose

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

3.8.4 Audience

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

3.8.5 Policy Detail

3.8.5.1 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. The District 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 District's standard software suite or approved by IT. Such software must incorporate all vendor provided security patches.

Users accessing the Internet through any electronic device connected to the District's network must do so through an approved Internet firewall or other security device. Bypassing the District's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using the District's 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.

3.8.5.2 Expectation of privacy

Users should have no expectation of privacy from District management in anything they create, store, send, or receive using Internet access. Users expressly waive any right of privacy in anything they create, store, send, or receive using the District provided Internet access.

3.8.5.3 File downloads and virus protection

Users are prohibited from downloading and installing software on their PC without proper authorization from the IT Department. 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 District approved virus detection software. If a user suspects a file may be infected, he/she must notify the IT Department immediately.

Users are prohibited from using the Internet to deliberately propagate any virus, worm, Trojan Horse, or other malicious program.

3.8.5.4 Monitoring of computer and Internet usage

All user activity on District IT assets is subject to logging and review. The District 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.

3.8.5.5 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 designated "Break Room PCs" and only in compliance with this policy.

3.8.5.6 Content

The District 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 District PC or electronic device prohibited.

Users are prohibited from attempting to access or accessing inappropriate sites from any District PC or electronic device. If a user accidentally connects to a site containing such material, the user must disconnect at once.

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

No personal or non-District commercial advertising may be made available via the District's advertised web site or social media platforms.

3.8.5.7 Transmissions

All sensitive District material transmitted over the Internet or external network must be encrypted.

Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

3.8.5.8 Incidental use

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

Incidental use must not result in direct costs to the District.

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 the District.

Storage of personal files and documents within the District's data repositories should be minimal.

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

3.9 Log Management Policy

3.9.1 Definitions

3.9.1.1 End points

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

3.9.1.2 Flow

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

3.9.1.3 IP

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

3.9.1.4 Packet

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

3.9.2 Overview

Most components of the IT infrastructure at Camrosa are capable of producing logs which record 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.

3.9.2.1 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. The District 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

3.9.3 Policy Detail

3.9.3.1 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.

3.9.3.2 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.

3.9.3.3 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.

3.9.3.4 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.

3.9.3.5 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 District's IT infrastructure have

synchronized clocks. The District shall use Network Time Protocol (NTP) for time synchronization, offset to Pacific Standard Time (PST).

3.9.3.6 Use of log information

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

3.9.3.7 Baseline behavior

It is essential that a baseline of activity, within the District's 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.

3.9.3.8 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 District's 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.

3.9.3.9 Log record life-cycle management

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

3.9.3.10 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 the District to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.

3.9.3.11 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

3.10 Safeguarding Customer Information Policy

3.10.1 Definitions

3.10.1.1 Customer

An individual who has established a service account for water or sanitary services with the Camrosa Water District.

3.10.1.2 Service provider

A third party that maintains, processes, or otherwise is permitted access to customer information while performing services for the District.

3.10.1.3 Personally Identifiable Information (PII)

Any record that contains information that, when used alone or with other relevant data, can identify an individual.

3.10.1.4 Sensitive PII

Sensitive PII includes, but is not limited to, information such as social security numbers, driver's license numbers, state and federal identification cards, or medical records. Sensitive PII includes all non-public records of information that could cause harm to an individual, if disclosed. All Sensitive PII must be stored or transmitted in secure form, for example, using encryption.

3.10.1.5 Non-sensitive PII

Non-sensitive PII is any information regarding an individual which is readily accessible from public sources and can include zip code, race, gender, and date of birth.

3.10.1.6 Customer information system

Any electronic or physical method used to access, collect, store, use, transmit, protect, or dispose of Customer PII.

3.10.2 Overview

This policy addresses the following topics:

- Board Involvement
- Risk Assessment
- Management and Control of Risk
- Customer Information Security Controls
 - Vendor Management Review Program
 - Software Inventory
 - Hardware Inventory
 - Critical Systems List
 - Records Management
 - Clean Desk Policy
 - Hardware and Electronic Media Disposal Policy
 - IT Acquisition Policy
 - Incident Response Plan
 - Information Sharing
- Training

- Testing

3.10.2.1 Purpose

The purpose of this policy is to ensure that the District complies with existing federal and state laws, and to ensure that information regarding District customers is kept secure and confidential.

3.10.3 Policy Detail

It is the policy of the District to protect the confidentiality, security, and integrity of each customer's non-public personal information in accordance with existing state and federal laws. The District will establish and maintain appropriate standards relating to administrative, technical, and physical safeguards for District customer's sensitive PII.

The District will maintain physical, electronic, and procedural safeguards, which comply with federal standards, to guard District customers' non-public personal information.

The District will not gather, collect, or maintain any information about its customers that is not necessary to offer its services, to complete customer transactions, or for other relevant business purposes.

The District does not sell or provide any user information to third parties, including list services, telemarketing firms, or outside companies for independent use.

The District's IT Manager is responsible for annually reviewing the program, making any needed adjustments, and coordinating staff training. District management is responsible for ensuring that its departments comply with the requirements of the program.

3.10.3.1 Information Security Program

Management is responsible for developing, implementing, and maintaining an effective information security program to:

- Ensure the security and confidentiality of customer non-public records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to, or use of, such records or information that would result in substantial harm or inconvenience to any customer

Management shall report to the Board of Directors, at least annually, on the status of the District's Information Security Program. The Board of Directors will also be notified of any security breaches or violations and the management team's response and recommendations for changes in the Information Security Program.

3.10.3.2 Risk Assessment

The District maintains a risk assessment that identifies potential threats to customer information and evaluates the potential impact of the threats.

On an annual basis, the risk assessment will be reviewed and updated by the IT Manager and reviewed by all District department managers. The District's controls will then be updated accordingly.

3.10.3.3 Management and Control of Risk

In order to manage and control the risks that have been identified, the District will:

- Establish written procedures designed to implement, maintain, and enforce the District's information security program
- Limit access to the District's customer information systems to authorized employees only
- Establish controls to prevent employees from providing customer's non-public information to unauthorized individuals
- Limit access at the District's physical locations containing customer's non-public information, such as building, computer facilities, and records storage facilities, to authorized individuals only
- Provide encryption of electronic customer non-public information including, but not limited to, information in transit or in storage on networks or systems to which unauthorized individuals may have access.
- Ensure that customer information system modifications are consistent with the District's information security program
- Implement dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, customer information
- Monitor the District's IT systems and procedures to detect actual and attempted attacks on, or intrusions into, the customer information systems
- Establish response programs that specify actions to be taken when the District suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies
- Implement measures to protect against destruction, loss, or damage of customer information due to environmental hazards, such as fire and water damage or technical failures
- Regularly test, monitor, evaluate, and adjust, as appropriate, the information security program considering any relevant changes in technology, the sensitivity of customer information, business arrangements, outsourcing arrangements, and internal or external threats to the District's information security systems

3.10.3.4 Customer information security controls

The District has established a series of customer information security controls to manage the threats identified in the risk assessment. The controls fall into ten categories.

3.10.3.4.1 Vendor management review program

All service providers, who may access customer Sensitive PII, must complete a Vendor Confidentiality Agreement requiring the provider to maintain the safekeeping and confidentiality of customer's non-public information in compliance with applicable state and federal laws. Such agreements must be obtained prior to any sharing of customer PII. Once the agreement has been completed, management will, according to risk, monitor service providers by reviewing audits, or other evaluations.

3.10.3.4.2 Software inventory

The District will maintain an inventory of its desktop, server, and infrastructure software. The information from this collection will provide critical information in identifying the software required for rebuilding systems. A template incorporated into the software inventory ensures that the security configuration and configuration standards are enforced. The template will also provide IT personnel with a quick resource in the event of a disaster. The software inventory list will be reviewed and updated on a continual basis.

3.10.3.4.3 Hardware inventory

The District will maintain an inventory of its desktop, server, and infrastructure hardware. The information from this collection will provide critical information in identifying the hardware requirements for rebuilding systems. A template incorporated into the hardware inventory ensures that the District's standards are enforced. The template will also provide IT personnel with a quick resource in the event of a disaster. The hardware inventory list will be reviewed and updated on a continual basis.

3.10.3.4.4 Critical systems list

The District will maintain a listing of its critical systems. This listing will support critical reliability functions, communications, services, and data. The identification of these systems is crucial for securing customer information from vulnerabilities, performing impact analysis, and in preparing for unscheduled events that affect the operations of the District.

3.10.3.4.5 Records management

The District will adhere to policies and procedures for protecting critical records from all outside and unauthorized access. Access to sensitive data will be defined as to who can access which data and under what circumstances. The access will be logged to provide accountability.

The District will adhere to the Camrosa Records Retention Policy for the proper process to dispose of records. Record disposal will be well documented. An inventory will be maintained of the types of records that are disposed of, including certification that the records have been destroyed.

3.10.3.4.6 Clean desk policy

District employees will comply with the Clean Desk Policy. This policy was developed to protect sensitive data from being readily available to unauthorized individuals.

3.10.3.4.7 Hardware and electronic media disposal procedure

The District will take precautions, as outlined in the Hardware and Electronic Media Disposal Policy, to ensure sensitive data cannot be retrieved from retired hardware or electronic media.

3.10.3.4.8 IT acquisition policy

The District will adhere to policies and procedures for acquisition of computer related items. Computer related purchases will be reviewed by designated IT personnel for compliance with security plans and alignment with operational and strategic plans. An annual review of acquisition policies and procedures will occur with input from the IT Manager.

A review of technology needs will occur during the annual budgeting and work planning processes. Needs will be classified into either current year plans or long range needs. The acquisition of technology solutions will be assessed to ensure that both current and future needs are met.

3.10.3.4.9 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 District's Incident Response Plan. The District will assemble a team to handle any incidents that occur. Necessary actions to prepare the District and the Incident Response Team will be conducted prior to an incident as required in the Incident Response Plan.

3.10.3.5 Summary of Actions

Below is a summary of the actionable steps the IT Department, as well as District management, would take:

- The IT Department 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
- The IT Department will notify the General Manager and all department managers of the intrusion. The General Manager will be responsible for notifying the Board of Directors.
- The IT Department 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, DHS, Homeland Security, or the public.
- If applicable, notices will be sent to affected customers in compliance with the District's Security Incident Management policy and the California Civil Code 1798.29, Accounting of Disclosures.

3.10.3.5.1 Training

The District recognizes that adequate training is of primary importance in preventing IT security breaches, virus outbreaks, and other related problems. The District 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 customer information.

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

3.10.3.5.2 Testing

The Information Security Officer, or designee, will annually audit the District's Safeguarding Customer Information Program. The Information Security Officer shall provide a formal report of its findings to the General Manager.

The District will require periodic tests of the key controls, systems, and procedures of the information security program. In accordance with current industry standards, the frequency and nature of such tests shall be determined by the IT Department.

The Information Security Officer will be responsible for reviewing the results of these tests and for making recommendations for improvements where needed.

3.11 Network Security and Virtual Private Network (VPN) Acceptable Use Policy

3.11.1 Definitions

3.11.1.1 Demilitarized Zone (DMZ)

A logical or physical sub-network that holds most of a network's externally combined services which attach to the internet. Its principal purpose is to give another layer of protection to internal protected networks.

3.11.1.2 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 examples of VPN capabilities allow employees to:

- Securely access a corporate intranet while located outside the office
- Remotely access their desktop computers from offsite
- Remotely manage the network given the proper authority and credentials

3.11.1.3 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.

3.11.1.4 Multi-Factor/Two-Factor Authentication (MFA/2FA)

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)

MFA and 2FA are considered synonymous for the purpose of this policy.

3.11.1.5 Dual Homing

Having concurrent connectivity to more than one network from a computer or network device.

Examples include:

- Being logged into the District network via a VPN connection from local Ethernet or WIFI connection, and a second independent connection to an Internet Service Provider (ISP)
- A Server connected to an internal protect District network and a second network connection to a Demilitarized Zone (DMZ) network for access from the internet.

3.11.1.6 Remote Access

Any access to District's corporate network through a non-District controlled network, device, or medium such as the Internet Service Provider (ISP) network or Internet.

3.11.1.7 Split-tunneling

Simultaneous direct access to a non-District network (such as the Internet, or a home network) from a remote PC or mobile device while connected into the District's corporate network via a Virtual Private

network (VPN) tunnel. VPN is a method for accessing a remote network via “tunneling: through the Internet.

3.11.1.8 IPSec Concentrator

A device in which VPN connections are serviced.

3.11.1.9 Secure Socket Layer (SSL)

An encryption-based internet security protocol that provides secure end-to-end communications between two or more end points.

3.11.2 Overview

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

3.11.3 Purpose

The purpose of this policy is to define standards for connecting to the District’s network from any host. These standards are designed to minimize the potential exposure to the District from damages, which may result from unauthorized use of District resources.

Damages include the loss of sensitive customer information or District confidential data, intellectual property, damage to the District’s public image, and damage to critical District internal systems.

Remote access implementations that are covered by this policy include SSL and IPsec VPN implementations only.

3.11.4 Audience

This policy applies to all District employees, contractors, vendors, and agents with a District-owned/District-approved computer or workstation used to connect to the District network. This policy also applies to remote access (VPN) connections used to do work from offsite on behalf of the District.

3.11.5 Policy Detail

3.11.5.1 Network Security

Users are permitted to use only those network addresses assigned to them by the District’s IT Department.

Remote users may connect to District Information Systems using only protocols approved by the IT Department. All remote access to the District network will be through a District approved VPN hardware appliance or software application using either secure SSL or IPsec VPN security protocol from a District-owned, domain joined PC or mobile device that has up-to-date anti-virus software (see the District Owned Mobile Device Acceptable Use and Security Policy and the Bring Your Own Device (BYOD) Policy for more information).

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 District network without the IT Department’s approval.

Users must not install network hardware or software that provides network services without the IT Department's approval. Non-District computer systems that require network connectivity must be approved by the IT Department prior to connection.

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of the District's network. For example, users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the District's network infrastructure. Only the IT Department is permitted to perform these actions.

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

3.11.6 Remote Access

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

General access to the Internet, through the District network is permitted for employees working remotely. These employees are responsible to ensure that they:

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

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

Employees are responsible for reviewing and following all IT and cyber security policies for protecting information when accessing the District corporate network via the following remote access methods:

- Virtual Private Network (VPN)
- Wireless Communications

The District will support VPN connections through broad-band internet service only. Dial-in modem usage is not a supported or acceptable means of connecting to the District's network.

3.11.7 Requirements

Secure remote access must be strictly controlled. Control will be enforced with Multi- Factor Authentication (MFA).

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

District employees, directors, and contractors with remote access privileges:

- Must ensure that their computer, which is remotely connected to District'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-District email accounts (i.e. Hotmail, Yahoo, etc.), or other external resources to conduct District business without prior approval from the District General Manager.

Remote VPN connections to the District network are configured by default with split-tunneling disabled. Reconfiguration of a home user's equipment for split-tunneling or dual homing is not permitted at any time.

For remote access to District hardware, all hardware configurations must be approved by the IT Department.

All hosts that are connected to the District's 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 District's network must obtain prior approval from the IT Department.

3.11.8 Virtual Private Network (VPN)

The purpose of this section is to provide guidelines for Remote Access using IPsec or SSL Virtual Private Network (VPN) connections to the District's corporate network.

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

Authorized remote users are responsible for selecting/obtaining an Internet Service Provider (ISP), coordinating installation, and paying associated fees at their point of connection to the Internet. Further details may be found in the Remote Access section above.

In the event a District owned, WIFI hotspot or other Internet service device is provided to the user, then the authorized user will connect to the District network through the VPN using only this device. This especially applies if the authorized remote user is at a public establishment, such as a coffee shop, hotel, etc., where there exists a higher risk to cyber security.

The following guidelines will also apply:

- It is the responsibility of the authorized remote user, with VPN privileges, to ensure that unauthorized users are not allowed access to District's internal networks.
- VPN use is controlled using multi-factor authentication.
- 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 the District's IT Department.
- All computers connected to the District's 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 District'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.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- To ensure protection from viruses, as well as protection of customer data, only District-owned equipment or non-District devices in accordance with the Bring Your Own Device (BYOD) Policy will have VPN and Remote Access.
- Only IT approved VPN clients may be used.

- By using VPN technology, users must understand that their machines are an extension of District's network and as such are subject to the same rules and regulations, as well as monitoring for compliance with this policy.

3.11.9 VPN Encryption and Authentication

All District approved devices connecting to the District network through a remote VPN connection will be configured to drop all unauthenticated and unencrypted traffic and will be provisioned with split-tunneling disabled. All District approved remote devices will be configured to effectively route all Internet access to the device through the District firewalls and Internet filters.

To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 256 bits, support a hardware address that can be registered and tracked (i.e. a MAC address), and support and employ strong user authentication, which checks against a protected database of authorized user's credentials. Any deviation from this practice will be considered on a case-by-case basis.

3.11.10 VPN Approval, Acceptable Use Review and Acceptance

Approval from a staff director or higher authority is required for a user's VPN access account creation. An acceptable use form is attached to the VPN procedure maintained by the IT Department and shall be reviewed and signed by each approved user to acknowledge having read and understood the policy (see Appendix C). This form shall in turn be approved, collected, and retained by the IT Manager prior to the user's VPN account use.

3.11.11 Wireless Communications

Access to the District's networks is permitted on wireless systems that have been granted an exclusive waiver by the IT Manager for connectivity to the District'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 the District's networks do not fall under the review of this policy.

3.11.12 Register Access Points and Cards

All wireless access points, extenders, or network interface adapters connected to the District network must be registered and approved by the IT Department.

3.11.13 Approved Technology

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

3.11.14 Setting the Service Set Identifier (SSID)

All District wireless SSID's shall be configured as non-advertised and therefore hidden from visibility.

3.12 Bring Your Own Device (BYOD) Policy and Agreement

3.12.1 Definitions

3.12.1.1 Bring Your Own Device (BYOD)

Privately owned wireless and/or portable electronic handheld equipment.

3.12.1.2 Guest Network

A District provided separate Local Area Network (LAN) that can be joined via wireless (WiFi) or wired (Cat5/6 cabling) connection that provides Internet access to connected devices but prevents access to the District's corporate internal networks.

3.12.2 Overview

Acceptable use of BYOD at Camrosa must be managed to ensure that access to the District's Guest Network resource for business are performed in a safe and secure manner for participants of the District's BYOD program. A participant of the BYOD program includes, but is not limited to:

- Employees
- Contractors
- Board of Directors

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.

3.12.3 Purpose

This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access the District's Guest Network using their personal device that fit the following device classifications:

- Laptops
- Notebooks
- Tablets
- Mobile/cellular phones

3.12.4 Audience

This policy applies to all District employees, including full and part-time staff, Board of Directors, contractors, and other agents who utilize personally-owned mobile devices to access the District's Guest Network. Such access to the Guest Network is a privilege, not a right, and forms the basis of a trust agreement the District will share with the BYOD user. Consequently, employment at the District does not automatically guarantee the initial and ongoing ability to use District provided Guest Network for Internet access.

3.12.5 Policy Detail

3.12.5.1 Accessing the Internet from the Camrosa Guest Network

Users are provided access to the Internet from the Camrosa Guest Network as a convenience to the BYOD user. At any time, at the request of management, Internet access may be revoked. The IT Department may restrict access to certain Internet sites that reduce network performance or are known

or found to be compromised with and by malware. The District 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 District's standard software suite or approved by IT. Such software must incorporate all vendor provided security patches.

Users accessing the Internet through any electronic device connected to the District's Guest Network must do so through the Internet firewall or other security devices that are in place. Attempting to bypass the District's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using District provided 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.

3.12.5.2 Responsibilities of the District

The IT Department will centrally manage the BYOD program and devices including, but not limited to, onboarding approved users, monitoring BYOD connections, and terminating BYOD connections to the Guest Network.

The IT Department will manage security policies, network, application, and Internet access centrally using whatever technology solutions it deems suitable.

The IT Department reserves the right to refuse the ability to connect mobile devices to Guest Network infrastructure. The IT Department will engage in such action if it feels such equipment is being used in such a way that puts the District's systems, data, or users at risk.

The IT Department will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to the District's Guest Network. To find out if a preferred device is on this list, an individual should contact the District's IT Department Service Desk. Although the IT Department currently allows only listed devices to be connected to the District's Guest Network, the IT Department reserves the right to update this list in the future.

The IT Department will maintain enterprise IT security standards.

The IT Department will inspect and monitor all mobile devices attempting to connect to the District's Guest Network and Internet.

The District's IT Department reserves the right to:

- Restrict applications.
- Limit use of network resources.
- Provide professional advice for proper provisioning and configuration of BYOD devices before connecting to the Guest Network.
- Through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from the District's protected internal networks.

3.12.5.3 Responsibilities of BYOD Participants

All potential participants will be granted access to the District Guest Network on the condition that they read, sign, respect, and adhere to the District's IT policies concerning the use of these devices and services (see Appendix D).

Prior to initial use on the District's Guest Network, all personally owned mobile devices must be registered with the IT Department.

Participants of the BYOD program and related software for network and data access will, without exception:

Use an approved method of encryption during reception or transmission of data.

The District's Guest Network is not to be accessed on any hardware that fails to meet the District's established enterprise IT security standards.

Utilize a device lock with authentication, such as a fingerprint or strong password, on each participating device. Refer to the District's 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.

Passwords and confidential data should not be stored on unapproved or unauthorized BYOD devices.

Exercise reasonable physical security measures. It is the end user's responsibility to keep their approved BYOD equipment safe and secure.

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 the owner.

The IT Department can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the connection of a BYOD device, and the resulting reports may be used for investigation of possible breaches and/or misuse.

If any BYOD device is lost or stolen, the District IT Department must be immediately contacted so that IT can delete or disable access to any associated District data (e.g., email).

If any BYOD device is scheduled to be upgraded or exchanged, the user must contact IT in advance. IT will disable the BYOD and delete any associated District data.

BYOD equipment that is used to conduct District business will be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's access.

Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with District's overarching security policy.

The user agrees to and accepts that his or her access and/or connection to District Guest Network may be monitored to record dates, times, duration of access, etc. This is done to identify unusual usage patterns or other suspicious activity, and to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains the District's highest priority.

Employees, Board of Directors, contractors, and temporary staff will not reconfigure their BYOD devices with any type of District owned and installed hardware or software without the express approval of the District's IT Department.

The end user agrees to immediately report, to his/her manager and the District's IT Department, any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of District resources, databases, networks, etc.

3.12.5.4 Help and Support

The District will offer the following support for the personal devices: connectivity to the District Guest Network, including email and calendar, and security services, including policy management, password management, and decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), or change of ownership.

The District is not able to provide any additional assistance on any personally owned device and is not responsible for carrier network or system outages that result in a failure of connectivity to the District Guest Network.

3.13 Patch Management Policy

3.13.1 Overview

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 Camrosa at risk. In order to effectively mitigate this risk, software “patches” are made available to remove a given security vulnerability.

3.13.2 Purpose

Given the number of computer workstations and servers that comprise the District 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 District employee.

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

3.13.3 Audience

This policy applies to all equipment that is owned or leased by the District, such as, all electronic devices, servers, application software, computers, peripherals, routers, and switches.

Adherence to this policy is mandatory.

3.13.4 Policy Detail

3.13.4.1 Common Vulnerabilities and Exposures

Many computer operating systems and software application programs may contain security flaws. These are known in the cyber security field as Common Vulnerabilities and Exposures (CVEs). An up-to-date list of CVEs is maintained by the non-profit, federally funded, cyber security firm, Mitre corporation (at <https://cve.mitre.org>) and in the National Institute of Standards and Technology’s (NIST), National Vulnerability Database (NVD).

Occasionally, one or more of these flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the District 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.

- If 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.

3.13.4.2 Responsibility

The IT Manager is responsible for providing a secure network environment for the District. It is District policy to ensure all computer devices (including servers, desktops, printers, etc.) connected to the District’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 IT Department is responsible for ensuring all known and reasonable defenses are in place to reduce network vulnerabilities, while keeping the network operating.

IT Management and Administrators 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:

- Identifying vulnerabilities
- Scheduled third party scanning of the District's network to identify known vulnerabilities.
- Monitoring application web sites for notifications of security updates of all vendors that have hardware or software operating the District's network

The IT Department 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.

The patching process will be well documented and will include the specific systems, groups of systems, and the timeframes associated with patching.

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

3.14 Physical Access Control Policy

3.14.1 Overview

Physical access controls define who is allowed physical access to Camrosa facilities that house information systems within those facilities. Without physical access controls, the potential exists that information systems could be physically accessed by unauthorized groups or individuals and the security of the information they house could be compromised.

3.14.2 Purpose

This policy applies to all facilities of the District, 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.

3.14.3 Policy Detail

Access to facilities that house information systems will be limited to authorized personnel only. Authorization will be demonstrated with authorization credentials (badges, identity cards, etc.) that have been issued by the District.

Access to facilities will be controlled at defined access points with the use of physical locks and/or electronic card readers. Before physical access to facilities and information systems 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 facilities that house information systems, 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.

3.15 Cloud Computing Policy

3.15.1 Definitions

3.15.1.1 Cloud computing

Is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction.

3.15.1.2 Public cloud

Is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

3.15.1.3 Private Cloud

Is based on the standard cloud computing model but uses a proprietary architecture typically at a federal, state, or county level of organization with dedicated facilities (or a partition of a public cloud facility with special access controls) or uses an infrastructure dedicated to a single organization.

3.15.1.4 Financial information

Is any data for the District, its employees, customers, or other third parties.

3.15.1.5 Intellectual property

Is any data that is owned by the District or provided by a third party that would not be distributed to the public.

3.15.1.6 Other non-public data or information

Are assets deemed the property of the District.

3.15.1.7 Other public data or information

Are assets deemed the property of the District.

3.15.1.8 Personally Identifiable Information (PII)

Any record that contains information that, when used alone or with other relevant data, can identify an individual.

3.15.2 Overview

Cloud computing allows the District to take advantage of technologies for storing and sharing of files, and for virtual on-demand computing resources all of which are typically managed by the cloud service provider and/or application specific vendor; for example the District's financial or customer billing applications. Cloud computing can be beneficial in reducing in-house IT staffing requirements by shifting the responsibility of administration and support of application servers and their associated hardware to the cloud service provider.

3.15.3 Purpose

The purpose of this policy is to ensure that the District can make intelligent cloud adoption decisions, weighing both the advantages and potential pitfalls of migrating IT systems to cloud services. In addition

to cost and budget, factors to consider when choosing what should stay on-premise or selecting a cloud service provider should include:

3.15.3.1 Security

Security should be multi-layered, incorporating:

- Physical or perimeter layer, such as controls that allow/prevent employees and contractors from entering the physical location of the provider's facilities.
- Infrastructure layer, which encompasses the data center equipment and systems that keep it running smoothly (e.g. backup power sources).
- Data layer, to restrict access to data, and maintain a separation of privileges for each layer.
- Environmental layer, to ensure a data center isn't built in an area prone to environmental catastrophe.

3.15.3.2 Data Governance

Any prospective cloud service provider of the District must meet or exceed all policies and standards the District has defined for information accessibility, security, and reliability within the entirety of this IT Master Plan.

3.15.3.3 Encryption

Does the cloud service provider automatically encrypt data at the physical layer before it leaves the provider's facilities? Is the data encrypted while in transit and at rest?

3.15.3.4 Antivirus Detection

How are threats detected (e.g. signature based scanning, behavioral-based scanning, or both)? How often are virus signatures updated? Is there a human (or humans) in the loop monitoring suspicious activity from a centralized Security Operations Center (SOC)? If so what are the SOC hours of operation (24/7, 5x8, etc.)?

3.15.3.5 User Authentication

How are legitimate users authenticated on to the system? Does the cloud service provider use Multi-Factor Authentication? If so, what methods are available (biometrics, SMS, email)?

3.15.3.6 Regulatory Compliance

Would a prospective service provider be able to offer additional regulatory security requirements for protecting the critical infrastructure and automated industrial control systems of a water utility?

3.15.3.7 Certifications & Standards

There are multiple standards and certifications within the cloud service provider industry. For prospective service providers, which standards and frameworks does the service provider comply with in order to determine the degree to which they adhere to best practices?

3.15.3.8 Other Service Level Agreement (SLA) Criteria

- Availability & uptime guarantee
- Escalation procedures
- Data center redundancy and/or cloud-to-cloud backup plan
- Computing performance specifications

- Exit plan

3.15.4 Policy Detail

It is the policy of the District to protect the confidentiality, security, and integrity of each customer's non-public personal information. The District will take responsibility for its use of cloud computing services to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the District.

This policy acknowledges the potential use of diligently vetted cloud services, only with:

- Providers who prove, and can document in writing, that they can provide appropriate levels of protection to the District's data in categories that include, but are not limited to, transport, storage, encryption, backup, recovery, encryption key management, legal and regulatory jurisdiction, audit, or privacy
- Explicit procedures defined for all handling of District information regardless of the storage, sharing or computing resource schemes

3.15.4.1 Cloud Computing Services

The category of cloud service offered by the provider has a significant impact on the split of responsibilities between the District and the provider to manage security and associated risks.

- Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. The provider is supplying and responsible for securing basic IT resources such as machines, disks, and networks. The District would be responsible for the operating system and the entire software stack necessary to run applications and is responsible for District data placed into the cloud computing environment. This means that most of the responsibility for securing the applications and the data would fall onto the District.
- Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. The infrastructure, software, and data are primarily the responsibility of the provider since the District would have little control over any of these features. These aspects need appropriate handling in the contract and the Service Level Agreement (SLA).
- Platform as a Service (PaaS) is a cloud computing service that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. Responsibility would likely be shared between the District and provider.

3.15.4.2 Privacy Concerns

Information security and data privacy concerns about the use of cloud computing services for the District include:

- The District may be limited in its protection or control of its data, potentially leading to a loss of security, lessened security, inability to comply with various regulations and data handling protection laws, or loss of privacy of data due to aggregation with data from other cloud consumers.
- The District's dependency on a third party for critical infrastructure and data handling processes.

- The District may have limited SLA options for a given provider's services and the third parties that a cloud vendor might contract with.
- The District is reliant on vendors' services for the security of the computing infrastructure.

3.15.4.3 Exit Strategy

Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. The District must determine how data would be recovered and migrated from the cloud vendor once service has been terminated, and the potential costs for such a migration.

3.15.4.4 Diligence

In evaluating the potential use of a particular cloud platform, the District will pay particular attention to the foregoing, and other privacy concerns, in addition to its documented vendor due diligence program.

3.15.5 Approved and Non-approved Cloud Services

See Appendix E for a list of approved and non-approved services adopted by the District.

3.16 Server Security Policy

3.16.1 Overview

The servers at the District provide a wide variety of services to users, and many servers also store or process sensitive information for Camrosa. These hardware and/or virtual devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the them against such attacks.

3.16.2 Purpose

The purpose of this policy is to define standards and restrictions for the base configuration of server equipment owned or leased and operated by the District's IT Department or IT/OT Managed Service Provider (MSP). This can include, but is not limited to, the following:

- Internet 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 CAMROSA.COM domain or appears to be owned by the District.

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

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

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

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

3.16.3 Policy Detail

3.16.3.1 Responsibilities

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

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

3.16.3.2 Supported Technology

All servers will be centrally managed by the District's IT Department or IT/OT Managed Service Provider (MSP) and will utilize approved server configuration standards. Approved server configuration standards will be established and maintained by the District's IT Department.

All established standards and guidelines for the District's IT environment are documented in an IT storage location. The following outlines the District's minimum system requirements for server equipment supporting District systems:

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the IT 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 the District'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. "Administrator" 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 District servers are to be in access-controlled environments.
- All employees are specifically prohibited from operating production servers in environments with uncontrolled access (i.e., office spaces).

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

It is the responsibility of any employee (or MSP employee) of the District who is installing or operating server equipment to protect the District's technology based resources (including District data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in the loss of customer information, damage to critical applications, loss of revenue, and damage to the District's public image. Procedures will be followed to ensure resources are protected.

3.16.4 Social Media Acceptable Use Policy

3.16.4.1 Definitions

3.16.4.1.1 Anonymous content

A comment, reply, or post submitted to a the District or affiliate site where the user has not registered and is not logged into the site.

3.16.4.1.2 District Official

A District Official is identified as any employee, contracted IT support employee, or Board of Director of the Camrosa Water District who is authorized to post public content on social media sites.

3.16.4.1.3 Facebook

A free social networking website.

3.16.4.1.4 LinkedIn

A social networking site designed specifically for the business community.

3.16.4.1.5 Microblogging

A web service that allows the subscriber to broadcast short messages to other subscribers of the service.

3.16.4.1.6 Social Media

A form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. For purposes of this policy, "Social Media" includes, but is not limited to, online blogs, chat rooms, personal websites, and social networking sites, such as Facebook, Twitter, MySpace, LinkedIn, YouTube, etc. The absence of, or lack of, explicit reference to a specific social networking tool does not limit the extent of the application of this policy. As new online tools are introduced, this policy will be equally applicable without advance notice.

3.16.4.1.7 Twitter

A free social networking microblogging service that allows registered members to broadcast short posts called tweets.

3.16.4.1.8 YouTube

A video-sharing website on which users can upload, share, and view videos.

3.16.4.2 Overview

The use of external social media (i.e. Facebook, LinkedIn, Twitter, YouTube, etc.) within organizations for business purposes is increasing. The District faces exposure of a certain amount of information that can be visible to friends of friends from social media. While this exposure is a key mechanism driving value, it can also create an inappropriate conduit for information to pass between personal and business contacts. Tools to establish barriers between personal and private networks and tools to centrally manage accounts are only beginning to emerge. Involvement by the IT Department for security, privacy, and bandwidth concerns is of utmost importance.

3.16.4.3 Purpose of Using Social Media

- Building a positive image: The District can use social media to promote a positive image and boost customer confidence in the various communities that comprise the Camrosa Water District.
- Increasing mind share: Social media can reach large audiences at very low monetary cost, giving the District another medium for promotion and increasing awareness of District operations.
- Improving customer satisfaction: Customers who receive more timely and personal service, in the medium that they prefer, will be more satisfied.
- Gaining customer insights: Social media can be used to monitor public opinion about the District's services.
- Customer service: Use of social media to respond to customer service issues or post questions quickly and efficiently. The answer to the problem can be made public, making it searchable by other customers who have the same issues or requests.
- Service outages: Use of social media to quickly and efficiently eliminate fears and communicate accurate information regarding recovery actions in the event of a service outage.

3.16.5 Policy Detail

The District encourages the use of social media as a channel for business communication in a manner consistent with its communications strategy. It is the policy of the District to establish guidelines for safe social media usage with respect to protecting District information. The safety and confidentiality of information is vital to the District's success. The District has established this policy to set parameters and controls related to District Official's usage of its social media sites.

3.16.5.1 Terms and Conditions of Use

All requests for use of external social media, on behalf of the District, must be submitted to a designated District Official. The District Official may only access or post to these sites in a manner consistent with District's security protocols and may not circumvent IT Security protocols to access any social media sites.

Use of personal social media accounts and user IDs, for District use, is prohibited.

Use of the District's social media user IDs, for personal use, is prohibited. Use of the District's email addresses to register on social networks, blogs, or other online tools utilized for personal use is prohibited. Examples of prohibited use of company User IDs include:

- Joining groups using a District user ID for personal reasons
- Adding personal friends to a District Official's friends list

District Officials are to acknowledge they have reviewed the social media service's Terms of Service (TOS) or Terms of User (TOU), as applicable. Links for sites are below.

- Facebook: <https://www.facebook.com/terms.php>
- LinkedIn: http://www.linkedin.com/static?key=user_agreement Twitter: <http://twitter.com/tos>
- YouTube: <http://www.youtube.com/t/terms>

3.16.5.2 Representing the Camrosa Water District

The General Manager will designate a person or team to manage and respond to social media issues concerning the District and will determine who will have the authority to contribute content. This person(s)'s responsibilities will include, but are not limited to:

- Managing social media tools and channels
- Responding to questions internally and externally about the social media site
- Addressing problems and provide direction for staff if a user becomes threatening, abusive, or harassing
- Submitting change requests to this District social media policy when warranted
- Working with other staff to make sure opportunities aren't overlooked in use of social media services
- Training staff to ensure they understand how to use the District's social media program.
- Ensuring the District's social media content complies with applicable laws and regulations.

All District Officials who participate in social media, on behalf of the District, are expected to represent the District in a professional manner. Failure to do so could have negative impact on the District and could jeopardize a District Official's ability to participate in social media in the future.

The District owns all authorized social media and networking content. District Officials are prohibited from taking, saving, or sending any District content distributed via social media for personal use while employed, separated, serving on the Board of Directors, or terminated by the District.

New technologies and social networking tools continually evolve. As new tools emerge, this policy will be updated to reflect the changes.

Platforms for online collaboration are fundamentally changing the work environment and offering new ways to engage with members and the community. Guiding principles for participating in social media should be followed:

- Post meaningful, respectful comments and refrain from remarks that are off-topic or offensive.
- Reply to comments quickly when a response is appropriate.
- Know and follow the state and federal laws that protect customer confidentiality at all times.
- Protect proprietary information and confidentiality.
- When disagreeing with others' opinions, keep it professional.
- Know the District's Code of Conduct and apply the standards and principles in social computing.

3.16.5.3 Personal Blogs and Posts

The District takes no position on a District Official's decision to start or maintain a personal blog or website or to participate in other online social media activities outside of work. District Officials, identifying themselves as a District Official on a social network, should ensure their profile and related content is consistent with how they and the District wish for them to present themselves. This includes what the District Official writes about himself/herself and the type of photos he/she publishes.

District Officials must not reveal proprietary information and must be cautious about posting exaggerations, obscenities, or other characterizations that could invite litigation.

District Officials must not make public reference to any District related financial or security procedures.

District Officials who comment on any District business or policy issue must clearly identify themselves as a District Official in their blog or posting and include a disclaimer that the views are their own and not those of District. When generating content that deals with District or individuals associated with the District, District Officials should use a disclaimer such as “The postings on this site are my own and do not necessarily reflect the views of the District.”

District Officials must not use social media websites to harass, threaten, discriminate against, disparage, or defame any other District employees, customers, vendors, Board of Directors, District services, or business philosophy.

District Officials are prohibited from disclosing confidential, proprietary, or otherwise sensitive business or personal information related to the District or any of its employees, vendors, customers, or Board of Directors. District Officials are also prohibited from disclosing any confidential, proprietary, or otherwise sensitive business or personal information that could identify another District employee, vendor, Board of Directors, or customers without that individual’s prior authorization.

District Officials should not take any action via social media websites or personal blogs that would harm, or is likely to harm, the reputation of the District or other District employee, vendors, Board of Directors, or customer.

3.16.5.4 Rules of Engagement

Protecting customer information is everyone’s number one responsibility. Information that can be used to disclose a customer’s personal information in any way should never be posted.

Communications in written, audio, or video form will be around for a long time, so consider the content carefully and be judicious.

What is written, produced, or recorded is ultimately the employee’s responsibility. Participation in social computing on behalf of the District is not a right and, therefore, needs to be taken seriously and with respect. Failure to comply could put an employee’s participation at risk and can lead to discipline. Third-party site’s terms and conditions must be followed.

Denigration of other water agencies, the District, or District affiliates is not permitted. Communication should be respectful when inviting differing points of view. Topics like politics or religion are not appropriate for District communications. Communicate carefully and be considerate; once words or other materials are posted, they cannot be retracted.

3.16.5.5 Rules of Composition

Produce material District customers will value. Social media communication from the District should help its customers, be thought provoking, and build a sense of community. It should help customers improve their knowledge or understand District functions better.

- District Officials should write and post about their areas of expertise, especially as it relates to the District.
- Write in the first person. Talk to the reader as if he/she were a real person in a professional situation.
- Avoid overly composed language.
- Consider content that is open-ended and invites response.

- Encourage comments.
- Use a spell-checker.
- Make the effort to be clear, complete, and concise in the communication. Determine if the material can be shortened or improved.
- If a mistake is made, it must be acknowledged. Be upfront and be quick with the correction. If posting to a blog, make it clear if a modification has been done to an earlier post.

Anonymous content is not allowed on District social media sites.

In general, the District will limit the access of social media sites to District Officials who use it on behalf of the Camrosa Water District.

3.17 System Monitoring and Auditing Policy

3.17.1 Overview

Systems monitoring and auditing capabilities must be implemented at Camrosa to determine when a failure of the information system security has occurred, including details of that failure.

3.17.2

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 the District. Specifically, it includes:

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

3.17.3 Policy Detail

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 and/or an externally contracted Security Operations Center 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 IT Manager.

Devices and appliances that provide information system logging capabilities will maintain sufficient primary (on-line) storage to retain 30-days' worth of log data and secondary (off-line) storage to retain one year's worth of data. If primary storage capacity is exceeded, the information system logging device(s) will be configured to overwrite the oldest logs first. 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 appropriate authentication. Further, access to logs or other system audit information will be logged as well.

3.18 Vulnerability Assessment Policy

3.18.1 Overview

Vulnerability assessments at Camrosa are necessary to manage the increasing number of cyber threats, risks, and common vulnerabilities and exposures.

3.18.2 Purpose

The purpose of this policy is to establish standards for periodic vulnerability assessments. This policy reflects the District's commitment to identify and implement security controls, which will keep risks to information system resources to a minimum.

This policy covers all computer and communication devices owned or operated by the District. This policy also covers any computer and communications device that is present on the District premises, but which may not be owned or operated by the District. Due to its obstructive nature, Denial-of-Service (DoS) testing or activities will not be performed.

3.18.3 Policy Detail

The operating system or environment for all information system resources must undergo a regular vulnerability assessment. This standard will empower the IT Department 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 the District'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.

The IT Department will make vulnerability scan reports and on-going correction or mitigation progress to the General Manager for consideration and reporting to the Board of Directors.

3.19 Website Operation Policy

3.19.1 Overview

The Camrosa internet website provides information to customers and the public, in general, regarding the District. It is designed to provide public information regarding the District. The District's website may also provide links to other websites, that also serve this purpose.

3.19.2 Purpose

The purpose of this policy is to establish guidelines with respect to communication and updates of the District's public facing website. Protecting the information on and within the District website, with the same safety and confidentiality standards utilized in the transaction of all the District business, is vital to the District's success.

3.19.3 Policy Detail

To be successful, the District website requires a collaborative, proactive approach by all District stakeholders working toward common goals and objectives of:

- Supporting the goals and key initiatives of the District
- Developing content that is customer focused, relevant, and valuable, while ensuring the best possible presentation, navigation, interactivity, and accuracy
- Promoting a consistent image and identity to enhance effectiveness
- Periodically assess the effectiveness of web pages

3.19.3.1 Responsibility

The Assistant General Manager is responsible for the website content and ensuring that materials meet legal and policy requirements.

The IT Department is responsible for the security, functionality, and infrastructure of the website. The third party, System Administrators will monitor the District website for response time and to resolve any issues encountered.

3.19.3.2 Links

The District is not responsible for, and does not endorse, the information on any linked website, unless the District's website and/or this policy states otherwise. The following criteria will be used to decide whether to place specific links on the the District website. the District will place a link on the website if it serves the general purpose of the District's website and provides a benefit to its members.

the District's website may contain, but not limited to, links for:

- Secure customer transactions such as bill pay
- Secure methods for customers to receive information such as monthly statements
- Ancillary services that are provided to members through third-parties, such as daily/monthly usage information
- District notices inviting bids or hiring notices
- District disclosures
- The District website will not provide links on its website for:
 - Illegal or discriminatory activities
 - Candidates for local, state, or federal offices

- Political organizations or other organizations advocating a political position on an issue
- Individual or personal home pages

3.19.3.3 Security

When a login is required, various forms of multi-factor authentication are implemented to ensure the privacy of customer information and security of their transactions. This process is to be implemented for access to Online Banking.

The District website, as well as linked sites, may read some information from the users' computers. The website or linked transactional websites may create and place cookies on the user's computer to ensure the user does not have to answer challenge questions when returning to the site. The multi-factor authentication process will still be required at the next login. This cookie will not contain personally identifying information and will not compromise the user's privacy or security.

3.19.3.4 Website Changes

Changes to the website will be authorized by the General Manager and performed by trained and qualified employee, or a specialized firm or individual they may retain, and only with the explicit approval of the General Manager or designated manager. On an annual basis, the District website will be reviewed by management for compliance to District policies. At the time of any significant changes to the website, a compliance review will be conducted by District management, legal counsel, or another reputable 3rd party compliance expert.

3.19.3.5 Regulatory Compliance

It is the policy of the District not to store or transmit customer credit card information on any internal or external District information system. This includes public facing websites owned or operated by the District. However, the District does contract with third-party credit card processing firms which may store or transmit customer credit card information (e.g., online bill pay) and these entities must comply with all regulations dealing with security of customer information, including, but not limited to:

- Payment Card Industry Data Security Standard (PCI DSS)
- Any other applicable security policies of the Camrosa Water District

At a minimum, the following disclosures will appear on all District websites:

- Privacy Policy and Web Privacy Policy
- Web Links Disclaimer

3.19.3.6 Website Design

The District website maintains a cohesive and professional appearance. While a sophisticated set of services is offered on the website, the goal is to maintain relatively simplistic navigation to ensure ease of use. Security on the website and protection of customer information is the highest priority in the layout and functionality of the site.

3.20 Workstation Configuration Security Policy

3.20.1 Definitions

3.20.1.1 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 several network endpoints or addresses.

3.20.2 Overview

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

3.20.3 Purpose

The purpose of this policy is to enhance security while optimizing operational performance of workstations utilized at the District. The IT Department shall implement these guidelines when deploying all new workstation equipment. Workstation users are expected to maintain these guidelines and to work collaboratively with the IT Department to maintain the guidelines that have been deployed.

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

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

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

This policy applies to all district-owned, operated, or controlled workstation equipment. Addition of new workstations, within the District facilities, will be managed at the sole discretion of the IT Manager. Non-sanctioned workstation installations, or use of unauthorized equipment on District facilities, is strictly forbidden.

3.20.4 Policy Detail

3.20.4.1 Responsibilities

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

Other IT staff members, under the direction of the IT Manager, are responsible for following the procedures and policies relating to Information Technology.

3.20.4.2 Supported Technology

All workstations will be centrally managed by the District's IT Department and will utilize approved workstation configuration standards, which will be established and maintained by the District's IT Department.

All established standards and guidelines for the District's IT environment are to be documented in an IT storage location.

The following outlines the District'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 IT Manager.
- All patch management to workstations will be monitored through reporting with effective remediation procedures. the District has deployed a patch management process; reference the Patch Management Policy.
- All workstations joined to the District domain will automatically receive a group policy update configuring the workstation to obtain future security patches and updates from the desktop management system.
- All systems within the District are required to utilize anti-virus, malware, and data leakage protection. IT will obtain alerts of infected workstations and perform certain remediation tasks.
- All workstations will utilize the District 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 to efficiently manage and maintain system security policies and controls.
- Third-party applications need to be updated and maintained. So that software with security updates is not exposed to vulnerabilities for longer than necessary, a quarterly review will be performed.
- Third-party applications, including web browsers, shall be updated and maintained in accordance with the District patch management program.
- Any critical security updates for all applications and operating systems need to be reviewed and appropriate actions taken by the IT Department to guarantee the security of the workstations in accordance with the District patch management program.
- Internet browsers on workstations will remain up to date. To ensure all browsers are up to date, the IT Department will perform quarterly reviews. If there is a reason the browser cannot be updated, due to conflicts with applications, these exceptions will be recorded.
- By default, all workstations joined to the District 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 the District's network.

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

3.21 Wireless (WiFi) Connectivity Policy

3.21.1 Definitions

3.21.1.1 Wireless Access Point (AP)

A device that allows wireless devices to connect to a wired network using WiFi or related standards.

3.21.1.2 Guest Network

A District provided separate Local Area Network (LAN) that can be joined via wireless (WiFi) or wired (Cat5/6 cabling) connection that provides Internet access to connected devices but prevents access to the District's corporate internal networks.

3.21.1.3 Keylogger

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

3.21.1.4 WiFi

A term for certain types of wireless local area networks (WLAN) that use specifications in the IEEE 802.11 specification.

3.21.1.5 Wireless

A term used to describe telecommunications in which electromagnetic waves, rather than some form of cabled (wired) media, carry the signal over all or part of the communication path.

3.21.2 Overview

This policy addresses the wireless connection of the District owned devices in remote locations.

Purpose

The purpose of this policy is to secure and protect the information assets owned by the District and to establish awareness and safe practices for connecting to free and unsecured WiFi, and connecting to secure guest networks provided by the District. The District provides computer devices, networks, and other electronic information systems to meet mission goals, and initiatives. the District grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

3.21.3 Policy Detail

3.21.3.1 District Guest WiFi Network

The District Guest WiFi network is provided on a best-effort basis, primarily as a convenience to employees and others who may receive permission to access it and the Internet. At any time, at the request of management, Internet access may be revoked. The IT Department may restrict access to certain Internet sites that reduce network performance or are known or found to be compromised with and by malware. The District 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 District's standard software suite or approved by IT. Such software must incorporate all vendor provided security patches.

Users accessing the Internet through any electronic device connected to the District's Guest Network must do so through the Internet firewall or other security devices that are in place. Attempting to bypass the District's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using District provided 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.

Microwaves, cordless telephones, neighboring APs, and other Radio Frequency (RF) devices that operate on the same frequencies as the District Guest WiFi network are known sources of signal interference. WiFi bandwidth is shared by everyone connected to a given WiFi access point (AP). As the number of WiFi 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 control of the District, availability, bandwidth, and access is not guaranteed.

The District WiFi 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 use of the WiFi.
- Physically or logically separate from the District's internal network and IT resources.
- Accessed by employees only in accordance with the Acceptable Use policy and its cross-referenced policies seen in this document
- Provided as a convenience for the use of District employees and vendors while visiting the District, and other visitors with the District's express permission via provision of an appropriate passphrase.
- Optionally provided to customers and qualifying visitors, by the District staff, with the provision of an appropriate passphrase and may be accessed with implied consent with the acceptable use policy provided in statement, online or in a written or verbal format.

The District's WiFi 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 the District.

3.21.3.2 Public WiFi Usage

When using WiFi 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 WiFi 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 WiFi link is legitimate. Check the security level of the network by choosing the most secure connection, even if you must 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 setup by a hacker. Inquire of the manager of the establishment for information about their official WiFi access point.
- Avoid free WiFi 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 WiFi connection (such as at Starbuck's, McDonald's, some hotels, etc.).
- Seek out WiFi 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 WiFi, or your own mobile hotspot if you have one or have been provided with one.
- If you must use an open WiFi, 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, postpone 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 District network and are authorized to do so, choose a trusted and encrypted WiFi AP or use your personal hotspot. In every case, you must always use your District-provided VPN. The VPN tunnel encrypts your information and communications. 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.

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 not when connected to an open, unencrypted WiFi.
- Allow automatic connection to WiFi Access Points your device finds, as it may be a rogue AP set up by a thief. Rather, configure automatic connections to known AP's you have reason to trust.

3.22 Telecommuting Policy and Agreement

3.22.1 Definitions

3.22.1.1 Telecommuting

A work arrangement in which employees do not commute or travel by bus or car to a central place of work, such as an office building, warehouse, or store. Telecommuters often maintain a specific office or workspace and usually work from this alternative work site during predefined days of the week. This is differentiated from teleworking or working remotely, that may refer to casual or occasional remote work done by a traditional employee while away from their traditional company office.

3.22.1.2 Telecommuting Agreement (TA)

A Telecommuting Agreement (TA) is a contract whereby employees are allowed to work from home. However, Employees must adhere to the same degree of professionalism in telecommuting as if they are working from office. The Company will provide the equipment for work and the use of the equipment can be constantly monitored. The working hours of the employee can be negotiated with the company. Under this Agreement, the employee uses the equipment provided by the Company and the Company keeps a register detailing the description and quantity of equipment used by the Employee. The employee also protects the equipment against damage and unauthorized use. In this Agreement, the Company agrees for the maintenance of company owned equipment and employee will be responsible for the maintenance of the equipment provided by the employee.

3.22.2 Overview

Telecommuting allows employees to work at home. This is particularly beneficial to the Camrosa Water District to ensure continuity of business if normal operations are disrupted and staff working at alternative locations would be more appropriate.

3.22.3 Purpose

This policy is to ensure that essential District functions continue to be performed if normal operations are disrupted and employees working at alternative locations would be more appropriate. The policy applies to telecommuting employees who regularly perform their work from home. Both the policy and agreement are intended to cover long-term telecommuting typically performed in response to an emergency or other disruption for the duration of the disruption or some specified portion thereof. This policy does not apply to the casual or after-hours telework that may be performed by employees. The policy also focuses on the IT equipment typically provided to a telecommuter, this policy addresses the telecommuting work arrangement and the responsibility for the equipment provided by the District.

3.22.4 Policy Detail

The General Manager or designee has the discretion to implement and withdraw any telecommuting agreements (TA) as necessary. The General Manager or designee shall designate and authorize specific times in which the TA shall apply. Any TA is subject to the terms and conditions set forth below.

3.22.4.1 Eligibility Criteria

Telecommuting is not suitable for all employees and/or positions. The General Manager or designee has the discretion to determine the employees and positions who may telecommute utilizing criteria that includes, but is not limited to:

1. The operational needs of the employee's department and the District.
2. The potential for disruption to District functions.
3. The ability of the employee to perform their specific job duties from a location separate from their District worksite ("Alternate Worksite") without diminishing the quantity or quality of the work performed.
4. The degree of face-to-face interaction with other District employees and the public that the employee's position requires.
5. The portability of the employee's work.
6. The ability to create a functional, reliable, safe, and secure Alternate Worksite for the employee at a reasonable cost.
7. The risk factors associated with performing the employee's job duties from an Alternate Worksite.
8. The ability to measure the employee's work performance from an Alternate Worksite.
9. The employee's supervisory responsibilities.
10. The employee's need for supervision.
11. Other considerations deemed necessary and appropriate by the employee's immediate supervisor and the General Manager.

3.22.4.2 Telecommuting Assignment

Any Telecommuting Agreement (TA) is only valid for the period specified in the Agreement. The Agreement is invalid after this time unless the District approves an extension in writing. The District may, at its discretion, decide to terminate the Agreement earlier.

1. Employee acknowledges and agrees that the TA is temporary and subject to the discretion of management. Telecommuting will be approved on a case-by-case basis consistent with the eligibility criteria above.
2. Non-exempt employees who receive overtime shall be assigned a work schedule in the TA, including rest and meal breaks ("Work Schedule"). Any deviation from the Work Schedule must be approved in advance, in writing, by management. Non-exempt employees must take meal and rest breaks while telecommuting, just as they would if they were reporting to work at their District worksite. Non-exempt employees may not telecommute outside their normal work hours without prior written authorization from their supervisor. A non-exempt employee who fails to secure written authorization before telecommuting outside his or her normal work hours may face discipline in accordance with the District's policy for working unauthorized overtime.
3. Telecommuting employees are required to be accessible in the same manner as if they are working at their District worksite during the established telecommuting Work Schedule, regardless of the designated location for telecommuting, or "Alternate Worksite." Employees must be accessible via telephone, email, and/or network access to their supervisor and other District employees while telecommuting, as if working at their District worksite. Employees shall check their District-related business phone messages and emails on a consistent basis, as if working at their District worksite.
4. Employees shall work on a full-time basis, according to the Work Schedule. If an employee has established an alternative work schedule, approved, and documented by the employee's supervisor, that schedule shall be reflected in the Work Schedule. Employees are required to

maintain an accurate record of all hours worked at the Alternate Worksite and make that record available to his or her supervisor upon request.

5. While telecommuting, employees shall:
 - a. Be available to the department via telephone and/or email during all TA designated work hours.
 - b. Have reliable and secure internet and/or wireless access.
 - c. Have all periods of employees' unavailability approved in advance by management in accordance with the District's Employee Handbook and documented.
 - d. Employees must notify their supervisor promptly when unable to perform work assignments because of equipment failure or other unforeseen circumstances.
 - e. For any District-owned equipment the employee takes to and/or uses at the Alternate Worksite, Employees agree to follow policies regarding the use of District-owned equipment as outlined in the Employee Handbook and further on in this policy. Employees will report to their supervisor any loss, damage, or unauthorized access to District-owned equipment immediately upon discovery of such loss, damage, or unauthorized access.

3.22.4.3 General Duties, Obligations and Responsibilities

Employees must adhere to the provisions and terms set forth in the Telecommuting Agreement (TA). Any deviation from the TA requires prior written approval from the Camrosa Water District.

1. All existing duties, obligations, responsibilities, and conditions of employment remain unchanged. Telecommuting employees are expected to abide by all District policies and procedures, rules and regulations, and all other official District documents and directives.
2. Employees authorized to perform work at an Alternate Worksite must meet the same standards of performance and professionalism expected of District employees in terms of job responsibilities, work product, timeliness of assignments, and contact with other District employees and the public.
3. Employees shall ensure that all official District documents are retained and maintained according to the normal operating procedures in the same manner as if working at a District worksite.
4. Employees may receive approval to use personal computer equipment or be provided with District issued equipment at the discretion of the General Manager or designee. If provided computer equipment the employee must protect the equipment from theft, damage, and loss.
5. The employee must designate a work area suitable for performing District business that allows them to perform their duties safely, efficiently, and, as necessary, confidentially. It is the employee's responsibility to assess the suitability of their Alternate Worksite and to ensure their Alternate Worksite is ergonomically sound.
6. The District shall not be responsible for costs associated with the use of computer and/or cellular equipment, including energy, data or maintenance costs, network costs, home maintenance, home workspace furniture, ergonomic equipment, liability for third-party claims, or any other incidental costs (e.g., utilities associated with the employee's telecommuting). Expenditures associated with any of the foregoing may qualify to be covered in whole or in part by the District upon approval by the employee's supervisor prior to purchase.

7. Employees may receive a virtual private network (“VPN”) account, as approved by the General Manager or designee, to securely access the District network.
8. Employees shall continue to abide by practices, policies, and procedures for requests of annual leave and other leaves of absences. Requests to work overtime, declare vacation, or take other time off from work must be pre-approved in writing by each employee’s supervisor. If an employee becomes ill while working under a TA, he/she shall notify his/her supervisor immediately and record on his/her timesheet any hours not worked due to incapacitation.
9. Employees must take reasonable precautions to ensure their devices (e.g., computers, laptops, tablets, smart phones, etc.) are secure before connecting remotely to the District’s network and must close or secure all connections to District desktop or system resources (e.g., remote desktop, VPN connections, etc.) when not conducting work for the District. Employees must maintain adequate firewall and security protection on all such devices used to conduct District work from the Alternate Worksite.
10. Employees shall exercise the same precautions to safeguard electronic and paper information, protect confidentiality, and adhere to the District’s records retention policies, especially as it pertains to the Public Records Act. Employees must safeguard all sensitive and confidential information (both on paper and in electronic form) relating to District work they access from the Alternate Worksite or transport from their District worksite to the Alternate Worksite. Employees must also take reasonable precautions to prevent third parties from accessing or handling sensitive and confidential information they access from the Alternate Worksite or transport from their District worksite to the Alternate Worksite. Employees must return all records, documents, and correspondence to the District at the termination of the TA or upon request by their supervisor or General Manager.
11. Employees’ salary and benefits remain unchanged. Workers’ Compensation benefits will apply only to injuries arising out of and in the course of employment as defined by Workers’ Compensation law. Employees must report any such work-related injuries to their supervisor immediately. The District shall not be responsible for injuries or property damage unrelated to such work activities, including injuries to third persons when said injuries occur at the Alternate Worksite.
12. All of Employees’ existing supervisory relationships, lines of authority, and supervisory practices remain in effect. Prior to the approval of this Agreement, supervisors and employees shall agree upon a reasonable set of goals and objectives to be accomplished. Supervisors shall use reasonable means to ensure that timelines are adhered to, and that goals and objectives are achieved.
13. Any breach of the telecommuting agreement by the employee may result in termination of the Agreement and/or disciplinary action, up to and including termination of employment.

The employee must sign the Telecommuting Agreement and the Telecommuting Equipment document for all District owned property provided to the employee for telecommuting purposes (see Appendices F and G). When the employee ceases to telecommute or is terminated, all District owned equipment shall be returned to the IT Department within five (5) business days.

3.23 Data Backup and Recovery Policy

3.23.1 Definitions

3.23.1.1 Data Backup

The saving of files to an offline storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

3.23.1.2 Data Recovery

The process of bringing or restoring offline storage data from offline media and putting it on an online storage system such as a file server.

3.23.1.3 Archive

The saving of old or unused files to an offline storage media for the purpose of freeing up room on an online storage media.

3.23.1.4 Full Backup

A complete copy of an online storage media in its entirety. This process backs up all files into a single version, regardless of the state of the Archive-Bit of each file.

3.23.1.5 Differential Backup

A partial copy of an online storage media which saves only the difference in the data since the last full back up to an offline storage media.

3.23.1.6 Incremental Backup

An incremental backup is similar to a differential backup, being only a partial copy of an online storage media, however this method provides optimal space savings on an offline storage media.

3.23.1.7 GFS Backup

Short for Grandfather-Father-Son, a GFS is a common and most widely used backup rotation strategy for storage consisting of daily incremental, weekly differential, and monthly full backups.

3.23.1.8 Recovery Point Objective (RPO)

The point in time to which data must be recovered after a data outage (e.g., a cyber-attack, natural disaster, or a communication failure). A typical value for RPO is twenty-four hours, however the value depends on change rate and criticality of the data recovery needs (e.g., an RPO of one-second would probably be necessary for bank ATM transactions)

3.23.1.9 Recover Time Objective (RTO)

Following a data outage, the RTO is the maximum tolerable length of time that a business organization can endure before an IT system, computer or network is restored.

3.23.2 Overview

One of the most critical functions any organization can undertake is ensuring a structured and highly formalized data backup and recovery policy and procedures are in place. An organization without its data – or the inability to retrieve and restore such data in a complete, accurate, and timely manner – faces serious issues as a viable entity. Backups are a must, especially considering today's growing

regulatory compliance mandates and the ever-increasing cyber security threats for which business face on a daily basis.

3.23.3 Purpose

The purpose of this backup and recovery policy is to provide for the continuity, restoration and recovery of critical data and systems in the event of an equipment failure, intentional destruction of data, or disaster.

3.23.3.1 Scope

The District's IT Department is responsible for the backup and recovery of data held in central systems and related databases. The responsibility for backup up data held on the workstations of individual users falls entirely to the user. Individual users should consult the Personal Storage Backup and Recovery procedure of this IT Plan for instructions on backing up and restoring their individual business-related files.

3.23.4 Policy Detail

3.23.4.1 Backup Schedule

All application servers (physical and/or virtual), VM host servers, domain controllers, and shared file repositories of any kind used at Camrosa, will be backed up daily/nightly. The District will utilize a combination of backup types and rotation schedules (full, differential, incremental, GFS) depending on:

- Server criticality
- Offline storage media location (cloud or local)
- Available offline storage space

3.23.4.2 Recover Point Objective (RPO)

The IT Department shall provide a Recover Point Objective not to exceed twenty-four (24) hours.

3.23.4.3 Recovery Time Objective (RTO)

The IT Department shall provide a Recovery Time Objective not to exceed twenty-four (24) hours to recover a single server/system. In the event of a multiple server outage the RTO will be best effort.

3.23.4.4 Retention

Daily/nightly data archives will be held for a period of three (3) months. Annual archives will be performed for each server at the end of the calendar year and will be held for five (5) years.

3.23.4.5 Responsibility

The IT Manager or designee shall be responsible for the oversight of the Data Backup and Recovery program, including performing, managing, monitoring and regular testing of data backups.

3.23.4.6 Backup and Restoration Testing

The ability to restore data from backups shall be tested at least once per month.

3.23.4.7 Storage Locations

At a minimum the District will maintain two (2) independent offline archive media sets, on premise, per server or asset being backed up. Additionally, the District will maintain at least one cloud based offline archive media set per server or asset being backed up.

3.23.4.8 Restoration

User's that need files restored must submit a request to the IT Help Desk. Required information shall include:

- Server name and or drive letter
- Directory path
- File name(s)
- Creation date(s)
- Date and time (if known) the file(s) was/were deleted or destroyed


3.24 Personal Storage Backup and Recovery Policy and Procedure


3.24.1 Overview


In an effort to protect individual user's business-related files, the District has provided each user with one (1) terabyte of cloud storage hosted by Microsoft OneDrive.

3.24.2 Accessing files

To access your OneDrive files, navigate to the location shown below in your file explorer:

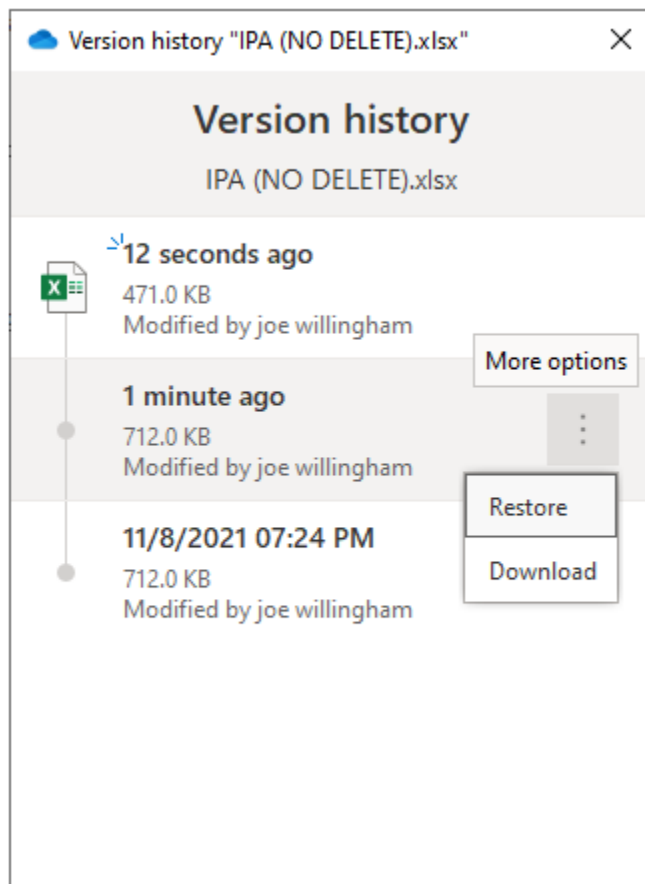
 OneDrive - camrosawater

 Desktop

 Documents

3.24.3 File Revision Retention

Currently Microsoft allows up to thirty revisions of each file. Users can restore previous file versions, by right-clicking on a file in their file explorer, OneDrive repository and then selecting the ellipses as shown below and selecting Restore or Download.



3.24.4 Access to OneDrive

In addition to accessing their Camrosa OneDrive from the District office, users can also access their OneDrive files at home by opening an internet browser and navigating to <https://onedrive.com> and entering their user credentials (email address and O365 password). Optionally, users at home may also freely download and install the OneDrive desktop application to their personal computers to access their OneDrive files. Note, all District policies regarding the safeguard and security of confidential District information still apply. User's must NOT keep any customer PII of any kind or sensitive District information in their District OneDrive cloud repositories.

3.25 Internet Of Things Policy

3.25.1 Definitions

3.25.1.1 Internet of Things (IoT)

Refers to network or Internet connected devices such as appliances, thermostats, monitors, sensors, and portable items that can measure, store, and transmit information. The IoT connects billions of devices to the Internet and involves the use of billions of data points, all of which need to be secured.

3.25.1.2 Data points

A discrete unit of information. Any single fact is a data point.

3.25.2 Overview

IoT devices may be business oriented, consumer based, or a hybrid of both. The devices may be company provided or employee owned, such as through a BYOD policy.

3.25.3 Purpose

The purpose of this policy is to establish a defined IoT structure to ensure that data and operations are properly secured. IoT devices continue making inroads in the business world; therefore, it is necessary for the Camrosa Water District to have this structure in place.

3.25.4 Policy Detail

3.25.4.1 IoT Device Procurement

IoT devices that are to be used for company operations should be purchased and installed by IT personnel.

Employee-owned IoT devices used for business purposes must be used in accordance with the Bring Your Own Device (BYOD) Policy. Unless otherwise permitted, all such devices will only be permitted to connect to a Guest WiFi network.

The use of all IoT devices, whether company provided, or employee owned, should be requested via Appendix H, IoT Device Usage Request Form and submitted to the IT department for approval. Only manager level employees and above may request the usage and/or procurement of IoT devices.

The IT department is responsible for identifying compatible platforms, purchasing equipment, and supporting organization provided and authorized IoT devices.

3.25.4.2 Cybersecurity Risks and Privacy Risk Considerations

It is important for the District to understand the use of IoT because many IoT devices affect cybersecurity and privacy risks differently than IT devices do. Being aware of the existing IoT usage and possible future usage will assist the District in understanding how the characteristics of IoT affect managing cybersecurity and privacy risks, especially in terms of risk response.

It is important for the District to manage cybersecurity and privacy risk for IoT devices versus conventional IT devices, determining how those risk considerations might impact risk management in general, risk response and particularly mitigation, and identifying basic cybersecurity and privacy controls may want to consider, adapt, and potentially include in requirements when acquiring IoT

devices. The IoT Risk Management Guide contains insight as to the differences in risk between conventional IT devices and IoT devices. This document resides in the IT document storage area.

APPENDIX A
Receipt of Acceptable Use of the Camrosa Water District's Information
Systems

I have received a copy of the CAMROSA WATER DISTRICT's Acceptable Use of Information Systems Policy.

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 the material contained in the Comprehensive IT Policy.

I understand the most updated policies and Bylaws will always be located on the intranet for my reference, and it will be my responsibility to review the policies and Bylaws as they are updated.

I further understand the content of the Comprehensive IT Policy supersedes all policies previously issued. I also understand that the CAMROSA WATER DISTRICT may supersede, change, eliminate, or add to any policies or practices described in the Comprehensive IT 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 Comprehensive IT policies as they are updated.

User's Signature: _____

User's Name (printed): _____

Date: _____

APPENDIX B
Camrosa Water District – Notice of Data Breach

(Page intentionally left blank)

Date: MM/DD/YYYY

NOTICE OF DATA BREACH

What Happened?

Give a brief, general description of the breach incident if that information is available at the time the notice is provided. If possible, provide the date of the breach, an estimated date, or a date range within which the breach occurred. State whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

What Information Was Involved?

Provide a list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

What We Are Doing

Briefly, provide a description of what steps the District has taken or plans to take as a result of the data breach.

What You Can Do

If the breach exposed credit-card information, a social security number, or a driver's license or California identification card number, provide a list of toll-free telephone numbers and addresses of the major credit reporting agencies.

Provide a source or sources for customers to check the on-going status of the data breach investigation through public postings, District website, social media, etc.

APPENDIX C

Virtual Private Network (VPN) Use Agreement

This Virtual Private Network Agreement is entered into between the User and the Camrosa Water District, effective the date this agreement is executed by the District's Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a remote desktop or mobile device connecting to the District's network is a privilege granted to the User by management approval per the Network Security and VPN Acceptable Use Policy. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to the District and to ensure the data remains secure.

In the event of a security breach or threat, the District reserves the right, without prior notice to the User, to disable or disconnect the VPN connection of the remote desktop or mobile device.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following District policies, published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, Anti-Virus, E-Mail, Password, Safeguarding Customer Information, and Telecommuting.

User of the remote desktop or mobile device shall not remove sensitive information from the District network, attack District assets, or violate any of the security policies related to the subject matter of this agreement.

The User understands and agrees that his/her use of the VPN software is required as part of his/her employment at the District and is permitted to connect to internal information services in support of District activities only. The User will safeguard the VPN access as well as its components (software/password) from any unauthorized use.

The VPN will be used on a District issued desktop or mobile device that is protected by a personal firewall. The district issued remote desktop or mobile device may be subject to scanning from the IT Department to check compliance with the contents of this Agreement.

SUPPORT

The District will offer support for connectivity to the District network. The District is not responsible for ISP outages that result in a failure of connectivity to the District network.

The User certifies that this Agreement has been read and understands the above conditions under which the User may be provided access to the District computer/information systems.

User's Signature: _____

User's Name (printed): _____

Date: _____

APPENDIX D

Bring Your Own Device (BYOD) Agreement

This Bring Your Own Device Agreement is entered into between the User and the Camrosa Water District (the District), effective the date this agreement is executed by the District's Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a supported BYOD device owned by the User in connection with the District's business is a privilege granted to the User, by management approval, per the *Bring Your Own Device (BYOD) and Camrosa Guest Network Access* policy. A supported BYOD device is defined as cell phone, tablet, or laptop running a manufacturer's supported version of its operating system. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to the District and to ensure the data remains secure.

In the event of a security breach or threat, the District reserves the right, without prior notice to the User, to disable or disconnect some or all BYOD services related to connection of a personal device to the District's Guest Network.

REIMBURSEMENT CONSIDERATIONS

The User is personally responsible for their BYOD devices and monthly cost of any carrier service. Accordingly, the District will NOT reimburse the User, for any loss, cost, or expense associated with the use or connection of a personal device to the District's Guest Network. This includes, but is not limited to, expenses for voice minutes used to perform District business, data charges related to the use of District services, expenses related to text or other messaging, cost of handheld devices, components, parts, or data plans, cost of replacement handheld devices in case of malfunction whether or not the malfunction was caused by using applications or services sponsored or provided by the District, loss related to unavailability of, disconnection from, or disabling the connection of a device to the District's Guest Network, and loss resulting from compliance with this Agreement or any other applicable District policies.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following applicable policies is mandatory: Acceptable Use of Information Systems, BYOD and Camrosa Guest Network Access, and other related policies including, but not limited to, Anti-Virus, E-Mail, Network Security, Password, Safeguarding Member Information, Telecommuting.

The User of the personal device shall not attempt to remove sensitive information from the District network, attack District assets, or violate any of the security policies related to the subject matter of this Agreement.

SUPPORT

The District will offer the following support for the personal devices: connectivity to the District Guest Network, including email and calendar, and security services, including policy management, password management, and decommissioning and/or remote wiping in case of loss, theft, device failure, device

degradation, upgrade (trade-in), or change of ownership. The District is not able to provide any additional assistance on any personally owned device and is not responsible for carrier network or system outages that result in a failure of connectivity to the District Guest Network.

The User assumes full liability for software or hardware failures associated with their personal devices including, but not limited to, an outage or crash of any or all of the District's Guest Network, programming and other errors, bugs, viruses, and other software or hardware failures resulting in the partial or complete loss of data, or which render the user's device inoperable.

DISCLAIMER

The District expressly disclaims, and the User releases the District from, all liability for any loss, cost, or expense of any nature whatsoever sustained by the User in connection with the privilege afforded the User under the terms of the Agreement.

User' Signature

User's Name (printed)

Date

Appendix E

Cloud Computing Adoption

Approved Public Cloud Services

This listing is not represented to be exhaustive and is meant to serve as a point-in-time list of approved or disapproved public cloud services as of the revision date in this appendix. Any cloud service not explicitly listed as approved should be assumed to be not approved until documented otherwise.

Services Approved for Camrosa Use	Services Not Approved for Camrosa Use

APPENDIX F

Telecommuting Agreement

Employee Acknowledgement:

I, the undersigned employee (“Employee”), have read the Telecommuting Policy and Agreement (“TA” or “Agreement”) in its entirety and I agree to abide by the terms and conditions they contain. I understand and agree that the TA is temporary and contingent upon approval, implementation, and withdrawal by the General Manager or designee. Approval does not imply entitlement to a permanently modified position or a continued telecommute arrangement.

I understand and agree that the TA is voluntary and may be terminated at any time. I further understand that Camrosa Water District may, at any time, change any or all of the conditions under which approval to participate in the TA is granted, with or without notice.

I agree to and understand my duties, obligations, and responsibilities. I also understand it is my responsibility to provide adequate advance notification to my supervisor if I am unable to keep any of the agreed upon commitments and/or deliverables. If I fail to do so, I understand this Agreement may be immediately terminated.

I certify that my Alternate Worksite is safe, secure, and ergonomically sound.

Any District-owned items or equipment I have taken to and/or will be using at my Alternate Works are listed on the attached Equipment Checkout Sheet.

The Agreement is valid from _____ to _____. I understand this Agreement expires on _____ and may not continue unless Camrosa Water District approves a new TA in writing. Camrosa Water District may rescind this Agreement at any time.

Regularly Assigned Place of Employment: The days and hours Camrosa Water District expects the Employee to be physically present at Camrosa Water District worksite are the following:

[Supervisor can add more space as necessary]

Alternate Worksite: The location and address of the Alternate Worksite is:

Street

City, State, Zip Code

Phone Number

The days and hours ("Work Schedule") the Camrosa Water District permits the Employee to be physically present at the Alternate Worksite are the following:

[Supervisor can add more space as necessary]

I hereby agree to report any work-related injury to my supervisor at the earliest reasonable opportunity. I hereby agree to hold Camrosa Water District harmless for injury to third parties at the Alternate Worksite.

I hereby affirm by my signature that I have read this Emergency Telecommuting Agreement and understand and agree to all of its provisions.

Employee's Signature

Date

Employee's Name and Title (printed)

Supervisor's Signature

Date

Supervisor's Name and Title (printed)

General Manager Signature

Date

APPENDIX G

Telecommuting Equipment Checkout Sheet

EMPLOYEE NAME:

ITEM

DATE CHECKED OUT

DATE RETURNED

SIGNATURE

DATE _____

APPENDIX H
IoT Device Usage Request Form

Date

Manager Name

Requester Name

Type of Device

Date Needed

Describe the need for this device

Board Memorandum

July 14, 2022

To: General Manager

From: Ian Prichard, Assistant General Manager

Subject: Drought Update

Objective: Receive an update on the drought.

Action Required: No action necessary; for information only.

Discussion: Due to the ongoing drought and infrastructure deficiencies, the California Department of Water Resources (DWR) and the Metropolitan Water District of Southern California (MWD) do not have sufficient supply to fulfill demands in parts of the MWD service area this summer. Those agencies have passed emergency regulations requiring retail agencies, including Camrosa, to implement strict conservation mandates. In response, at its June 23, 2022 meeting, the Camrosa Board of Directors adopted Resolution 22-08 Declaring a Stage Three Water Supply Shortage. The declaration limits potable outdoor irrigation to ten minutes per station one day a week, in addition to other specified regulations. Stage Three also authorizes the District to impose penalties, both financial and physical (flow restriction or disconnection), for violations of water-use prohibitions.

MWD accepted the Stage Three declaration as compliant with the “watering restrictions” pathway described by their Emergency Water Conservation Program (EWCP), established April 26, 2022. Agencies deemed noncompliant are required to abide by the second, “volumetric” pathway. Under that pathway, agencies exceeding their monthly “Volumetric Target Allocation” (VTA) are subject to penalties of \$2,000 per acre foot.

The EWCP provides MWD’s general manager the ability to move all affected agencies to a “zero outdoor watering” scenario after September 1, 2022, without returning to the MWD board, should the need for greater conservation arise. Noncompliance with the “zero outdoor watering” requirements at that time would result in moving the noncompliant agency to the volumetric pathway.

MWD has stated that moving all affected agencies to the volumetric pathway is an option after December 1, 2022. Under any volumetric scenario, the \$2,000/AF penalty structure would adhere.

Staff will present options for developing a mechanism to equitably pass on any penalties the District may incur during this drought under MWD’s Emergency Water Conservation Program.

Board Memorandum

July 14, 2022

To: General Manager

From: Ian Prichard, Assistant General Manager

Subject: Master Plan

Objective: Begin the master planning process.

Action Required: Authorize the General Manager to enter into an agreement with and issue a purchase order to Woodard & Curran in an amount not to exceed \$557,046.00 for support in developing a near-term Capital Improvement Plan for repair, rehabilitation, and replacement needs of the District's infrastructure.

Discussion: Between climatic, legislative, litigatory, and political pressures, the State Water Project, which today constitutes more than half the District's potable demand, no longer represents a dependable supply. At the same time, the cost to produce local water has also increased, driven by an ever-expanding regulatory environment. Groundwater, water loss, conservation, environmental justice, rate setting—the list of current and impending regulatory constraints is long and expanding.

To maximize the District's capacity to adapt to a changing political and water supply landscape, the Board has begun a long-term planning process. Earlier this spring, staff prepared a Request for Qualifications and distributed it to six firms to evaluate their ability to develop a strategic plan and a two-part master plan: a near-term plan focused on rehabilitation, replacement, and maintenance to inform the next five-year rate study in 2024; and a long-term water resources plan to envision water supplies to a fifty-year horizon. Two of the six firms, Woodard & Curran and MKN, responded as a partnership. The Board approved Woodard & Curran's proposal for a 2022 Strategic Plan at the May 12, 2022 Board meeting, and held the first three of five strategic planning workshops the last week May and the first of June. The initial workshops were productive, and the Board anticipates a final 2022 Strategic Plan in August.

The strategic planning workshops also provided Woodard & Curran additional context for proposing on the first part of the master plan. As detailed in the attached proposal, this phase is intended to develop a five- and ten-year Capital Improvement Plan (CIP) for maintenance of existing facilities. Woodard & Curran proposes a review of existing documents, studies, and reports; the physical inspection of aboveground facilities; condition and risk assessments on the potable, nonpotable/recycled, and wastewater pipeline systems; and an analysis of potable water storage alternatives. Woodard & Curran recognizes that this process is an extension of the 2022 Strategic Plan and has built into their proposal interaction with a "technical advisory group" composed of District management and members of the Board, as well as substantial interaction with District staff at various levels through the different analyses and tasks.

In addition to the eight core tasks that comprise the near-term CIP, the proposal also includes two optional tasks: development of a wastewater system hydraulic model and an outreach and advocacy plan.

Significant discussion during the initial strategic plan workshops focused on the criticality of outreach and advocacy to the District's near-term tactics and long-term strategy. Communication with and education of customers, regional and statewide partners, and regulatory groups formed a part of the 2008 Strategic Plan and informs how staff perform their roles. As we look towards the future, outreach and advocacy represent an indispensable part of the projects and programs the organization plans to take on. Staff recommends including the outreach and advocacy plan as part of the master planning effort.

The wastewater model would provide a comprehensive, field-calibrated technical tool for wastewater planning, including capacity evaluation, design criteria, and system performance. The advantages to the District having a wastewater model would be multiplied if we anticipated significant wastewater service expansion in the service area. Given how close we are to build-out, however, and the current unlikelihood of expanding the sewer system into the Santa Rosa Valley, staff recommends forgoing Task 9 at this time.

As such, the \$557,046.00 in the action requested above is for Tasks 1-8 and Task 10 of the Woodard & Curran proposal. This plan is included in the FY2022-23 budget.

**Camrosa Water District
7385 Santa Rosa Rd.
Camarillo, CA 93012
Telephone (805) 482-4677 - FAX (805) 987-4797**

Some of the important terms of this agreement are printed on pages 2 through 3. For your protection, make sure that you read and understand all provisions before signing. The terms on Page 2 through 3 are incorporated in this document and will constitute a part of the agreement between the parties when signed.

TO: Woodard & Curran
888 South Figueroa #1700
Los Angeles, CA 90017

DATE: July 14, 2022
Agreement No.: 2023-77

The undersigned Consultant offers to furnish the following: for professional services for developing a near-term CIP for repair, rehabilitation and replacement needs of existing infrastructure per proposal dated June 29, 2022 (attached)

Contract price \$: Not to exceed \$557,046.00 for Task 1-8 and Task 10.

Contract Term: July 14, 2022 – June 30, 2024

Instructions: Sign and return original. Upon acceptance by Camrosa Water District, a copy will be signed by its authorized representative and promptly returned to you. Insert below the names of your authorized representative(s).

Accepted: Camrosa Water District

Consultant: Woodard & Curran Inc.

By: _____
Tony L. Stafford

By: _____
Persephene St. Charles

Title: General Manager

Title: Senior Vice President

Date: _____

Date: July 7, 2022

Other authorized representative(s):

Other authorized representative(s):

Consultant agrees with Camrosa Water District (District) that:

- a. Indemnification: To the extent permitted by law, Consultant shall hold harmless, defend at its own expense, and indemnify the District, its directors, officers, employees, and authorized volunteers, against any and all liability, claims, losses, damages, or expenses, including **reasonable attorney's fees and costs, arising from** negligent acts, errors or omissions of Consultant or its officers, agents, or employees in rendering services under this contract; excluding, however, such liability, claims, losses, damages or expenses arising from the District's sole negligence or willful acts.
- b. Minimum Insurance Requirements: Consultant shall procure and maintain for the duration of the contract insurance against claims for injuries or death to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of that work by the Consultant, his agents, representatives, employees or subcontractors.
- c. Coverage: Coverage shall be at least as broad as the following:
 1. Commercial General Liability (CGL) - Insurance Services Office (ISO) Commercial General Liability Coverage (Occurrence Form CG 00 01) including products and completed operations, property damage, bodily injury, personal and advertising injury with limit of at least two million dollars (\$2,000,000) per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location (coverage as broad as the ISO CG 25 03, or ISO CG 25 04 endorsement provided to the District) or the general aggregate limit shall be twice the required occurrence limit.
 2. Automobile Liability - (If applicable) Insurance Services Office (ISO) Business Auto Coverage (Form CA 00 01), covering Symbol 1 (any auto) or if Consultant has no owned autos, Symbol 8 (hired) and 9 (non-owned) with limit of one million dollars (\$1,000,000) for bodily injury and property damage each accident.
 3. Workers' Compensation Insurance - as required by the State of California, with Statutory Limits, and **Employer's Liability Insurance with limit of no less than \$1,000,000 per** accident for bodily injury or disease.
 4. Waiver of Subrogation: The insurer(s) named above agree to waive all rights of subrogation against the District, its directors, officers, employees, and authorized volunteers for losses paid under the terms of this policy which arise from work performed by the Named Insured for the District; but this provision applies regardless of whether or not the District has received a waiver of subrogation from the insurer.
 5. Professional Liability - (also known as Errors & Omission) Insurance appropriate to the Consultant profession, with limits no less than \$1,000,000 per occurrence or claim, and \$2,000,000 policy aggregate.
- d. If Claims Made Policies:
 1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.
 2. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of the contract of work.
 3. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, the Consultant **must purchase "extended reporting"** coverage for a minimum of five (5) years after completion of contract work.

If the Consultant maintains broader coverage and/or higher limits than the minimums shown above, the District requires and shall be entitled to the broader coverage and/or higher limits maintained by the Consultant. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the District. The parties agree that neither party shall be responsible or liable to the other party for special, indirect or consequential damages and the total aggregate liability of each respective party under this Agreement for any and all claims against such party whatsoever arising out of this Agreement shall not exceed the total insurance proceeds **paid under such respective party's applicable insurance policies subject to the minimum limits specified in this Agreement.**

Other Required Provisions: The general liability policy must contain, or be endorsed to contain, the following provisions:

- a. Additional Insured Status: District, its directors, officers, employees, and authorized volunteers are to be given additional insured status (at least as broad as ISO Form CG 20 10 10 01), with respect to liability arising out of work or operations performed by or on behalf of the Consultant including materials, parts, or equipment furnished in connection with such work or operations.
- b. Primary Coverage: For any claims related to this project, the Consultant's **insurance coverage shall be primary** at least as broad as ISO CG 20 01 04 13 as respects to the District, its directors, officers, employees, and authorized volunteers. Any insurance or self-insurance maintained by the District, its directors, officers, employees, and authorized volunteers shall be excess of the Consultant's insurance and shall not contribute with it.

Notice of Cancellation: Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to the District.

Self-Insured Retentions: Self-insured retentions must be declared to and approved by the District. The District may require the Consultant to provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. The policy language shall provide, or be endorsed to provide, that the self-insured retention may be satisfied by either the named insured or the District.

Acceptability of Insurers: Insurance is to be placed with insurers having a current A.M. Best rating of no less than A:VII or as otherwise approved by the District.

Verification of Coverage: Consultant shall furnish the District with certificates and amendatory endorsements or copies of the applicable policy language effecting coverage required by this clause. All certificates and endorsements are to be received and approved by the District before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive the **Consultant's** obligation to provide them. The District reserves the right to require certified redacted copies of all required insurance policies, including policy Declaration and Endorsements pages listing all policy endorsements. If any of the required coverages expire during the term of this agreement, the Consultant shall deliver the renewal certificate(s) including the general liability additional insured endorsement to Camrosa Water District prior to the expiration date.

Subcontractors: Consultant shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Consultant shall ensure that the District, its directors, officers, employees, and authorized volunteers are an additional insured on Commercial General Liability Coverage.

Other Requirements:

- a. Consultant shall not accept direction or orders from any person other than the General Manager or the person(s) **whose name(s) is (are) inserted on Page 1 as "other authorized representative(s)."**
- b. Payment, unless otherwise specified on Page 1, is to be 30 days after acceptance by the District.
- c. Permits required by governmental authorities will be **obtained at Consultant's expense, and Consultant will comply** with applicable local, state, and federal regulations and statutes including Cal/OSHA requirements.
- d. Any change in the scope of the professional services to be done, method of performance, nature of materials or price thereof, or to any other matter materially affecting the performance or nature of the professional services will not be paid for or accepted unless such change, addition or deletion is approved in advance, in writing by the District. **Consultant's "other authorized representative(s)" has/have the authority to execute such written change for Consultant.**

The District may terminate this Agreement at any time, with or without cause, giving written notice to Consultant, specifying the effective date of termination.

Via Electronic Mail

June 29, 2022



Ian Prichard
Assistant General Manager
Camrosa Water District
7385 Santa Rosa Road
Camarillo, CA 93012

Re: Proposal for Developing a Near-Term CIP for Repair, Rehabilitation and Replacement Needs of Existing Infrastructure for the Camrosa Water District

Dear Mr. Prichard,

Woodard & Curran is pleased to present our proposal to develop a five- and 10-year Capital Improvement Plan (CIP) for repair, rehabilitation and replacement needs of existing infrastructure for the Camrosa Water District's (CWD or District). It is understood that this near-term CIP development is the second phase of three-phase planning process. Our proposal includes the scope of work, schedule and fee for development of the near-term CIP, with the assumption that a third phase to complete the Master Plan will be contracted separately.

Woodard & Curran will be conducting this update in partnership with MKN Associates. Our proposed workplan is designed to result in development of a five- and ten-year CIP by June 2023 that will determine necessary repair, rehabilitation and rehabilitation needs of CWD's existing infrastructure for the next five to ten years. Continuous feedback and dialogue with District staff throughout the CIP development process will be critical to completing the following:

- Condition assessments of above ground facilities and horizontal infrastructure within the potable water, non-potable water and wastewater systems, with identification of high priority projects within each system
- An evaluation of storage alternatives for the potable water system
- Five- and ten-year CIP and accompanying technical memorandum

In addition, our proposal includes optional tasks for development of a wastewater system model to improve the District's understanding of its wastewater system, and development of an outreach and advocacy plan that will set a path forward for the District's engagement with customers and stakeholders.

We thank you for the opportunity to submit our proposal and look forward to working with you on this exciting project.

Sincerely,

A handwritten signature in blue ink, appearing to read "Persephene St Charles".

Persephene St Charles
Principal-in-Charge

A handwritten signature in blue ink, appearing to read "Brian Van Lienden".

Brian Van Lienden
Project Manager



SCOPE OF WORK

Task 1. Project Management and Meetings

Subtask 1.1 Project Management and Controls

Woodard & Curran will set up and maintain project management and controls systems to ensure that the project scope, schedule and budget are maintained. This subtask will cover a period of 12 months through June 2023. Woodard & Curran will conduct up to twenty (20), 30-minute project progress calls with District staff to indicate progress and receive necessary input.

Woodard & Curran will develop and submit to the District monthly progress reports documenting at the task level, the following:

- summary of work completed over the most recent month
- list of proposed activities for the upcoming month
- list of pending data needs to support the planned activities for the upcoming month
- major decisions
- project schedule status

Subtask 1.2 Meetings with Staff and Technical Advisory Committee

Woodard & Curran will participate in up to six (6) meetings with District staff to discuss and receive input on technical information related to project tasks. It is assumed that each meeting will be no more than two hours long, that up to three of these meetings will be in person, and that up to two Woodard & Curran team members will be in attendance.

Woodard & Curran will participate in up to three (3) meetings with the Technical Advisory Committee (TAC) to receive input and feedback on project tasks. In addition, Woodard & Curran will participate in one Board meeting to present the final CIP. It is assumed that each meeting will be no more than two hours long, that up to two TAC meetings and the Board meeting will be in person, and that up to two Woodard & Curran team members will be in attendance at each meeting.

Task 1 Deliverables:

- Twelve (12) monthly progress reports
- Meeting materials for TAC meetings



Task 2: Data Collection and Review

Woodard & Curran will collect existing information related to the potable water, non-potable water¹ and wastewater systems provided by the District. The information collected may include relevant reports, planning documents, drawings, maps, facility information, and other required data including, but not limited to:

- Planning documents
- Flushing and/or hydrant test reports;
- Record drawings of any facilities for which up-to-date data is not included in the current GIS data;
- CCTV inspection records of wastewater facilities
- Asset inventories for vertical and horizontal assets including maintenance histories
- Booster station as-built drawings and operating information (pump models, type, and capacities; pump curves, on and off operating levels);
- Water tank geometry, base and overflow elevations, and typical operating levels (from SCADA);
- Available water system SCADA data (treatment plants, booster stations, storage facilities, wells);
- Maintenance records and inspection reports, including data relating to maintenance hotspots and known problem areas (including horizontal infrastructure break and failure history);
- Operational data related to surface water supplies
- Capacity and quality concerns with existing wells; operational data for existing wells; studies documenting proposed wells.

As part of this task, Woodard & Curran will also complete an initial desktop review to identify facilities in which additional field investigation and/or data collection is needed to supplement existing information based on the lack of sufficient data and/or reports of aging or deteriorating infrastructure.

Task 2 Deliverables:

- Data and information request

¹ The non-potable water system includes unregulated surface water and treated recycled water.



Task 3: Condition Assessment of Above Ground Facilities

Subtask 3.1 – Develop Plan for Above Ground Facility Condition Assessments

The Woodard & Curran team will review available reports, drawings, and data, and will interview staff to develop an overall plan for the condition assessment of storage tanks, pump stations, wells, PRV stations, metering stations, lift stations and treatment facilities. The above ground facility assessments will be conducted using industry recommended standards and guidelines, which will be selected in coordination with District staff. The final plan for performing the condition assessment will be reviewed and approved by District staff.

Subtask 3.2 – Perform Site Assessments of Above Ground Facilities

The Woodard & Curran team will perform a walk-through of facilities, accompanied by District staff, where notes and photos will be taken, as described below.

Storage and Conveyance Facilities and Well Sites

The Woodard & Curran team will visit the District's storage tanks, booster pump stations, PRV stations, metering stations, and well sites to complete a visual inspection (including digital photos) to confirm and supplement as-built information and document existing conditions and deficiencies. The field assessments will include discussions with District staff with respect to operational issues, age of facilities, and Staff requested improvements. The team will evaluate the pumping capacity of the production wells; storage capacity to serve fire, emergency, and operational requirements; and the ability of the booster pump station (BPS) to provide the required pressures and flows for existing and projected future system demands. Assessment of the facilities will include the following:

- Condition of process piping, mechanical, structural, architectural, electrical and building systems;
- Safety compliance
- Pumping station capacity and redundancy
- Tank capacity and configuration
- Well capacity
- Failure of facility coatings
- Existing and recommended monitoring and alarm systems
- Emergency backup power and controls
- Visual inspection of buildings and fencing

It is estimated for storage tanks, booster pump stations, PRV stations, metering stations, and well facilities, approximately 45-60 minutes will be spent at each site, taking photos, notes and interviewing staff. Approximately 8 facilities will be reviewed per day (29 sites in 3.5 days).

Lift Stations

The Woodard & Curran team will visit the District's lift stations to complete a visual inspection (including digital photos) to confirm and supplement as-built information and document existing condition and deficiencies. The evaluation will include visual inspection of the dry well



(if applicable), wet well, piping, valves, and panels to document existing and potential deficiencies and provide recommendations for improvements. The field assessments will include discussions with District staff with respect to operational issues, age of facilities, and Staff requested improvements. Assessment of the lift stations will include the following:

- Safety compliance
- Flood resilience
- Backup power provisions (including on-site generators and/or connections for a portable generator)
- Any signs of wet well corrosion including exposed rebar or delamination, which typically occur near the top of the wet well
- Failure of pipe or mechanical system coatings
- Operation/maintenance access
- Bypassing provisions
- Safety issues for operator access
- Visual inspection of buildings and fencing

It is estimated approximately 45-60 minutes will be spent at each lift station, taking photos and notes, and interviewing staff. The four lift stations will be reviewed within one day by a principal or senior engineer and assistant engineer.

Diversion Structure, Reclamation Facility and Desalter

The Woodard & Curran team will perform a visual condition assessment of the Diversion Structure, Camrosa Water Reclamation Facility and Round Mountain Desalter to review information collected from plans and reports and to gather current information. As part of this effort, the team will visit the sites to document the condition of existing systems and interview the plant operators. The team will review the existing buildings, pavement, and equipment and review maintenance records to identify maintenance, repair, or possible enhancements. The diversion structure evaluation will include the interior of the structure; it is assumed that District staff will temporarily shut down operation of the structure to allow for the inspection. A single day is planned for the sites, with a senior engineer, a treatment process engineer, and electrical engineer participating.

Subtask 3.3 – Develop Above Ground Condition Assessment Technical Memorandums

Findings of the above ground facility assessments will be documented in 3 separate technical memorandums (potable, non-potable, wastewater). Draft technical memorandums will be submitted to the District for review and comments. District comments will be incorporated into the final technical memorandums.

Task 3 Deliverables

- Draft and Final Above Ground Potable Water Condition Assessment Technical Memorandum
- Draft and Final Above Ground Non-Potable Water Condition Assessment Technical Memorandum
- Draft and Final Above Ground Wastewater Condition Assessment Technical Memorandum



Task 4: Horizontal Potable Water System Performance and Risk Assessment

Woodard & Curran will perform a performance and risk assessment of the horizontal potable water system, which includes below-grade infrastructure (pipelines, valves, etc.) that is included in the District's existing potable water system hydraulic model.

Subtask 4.1 – Review Existing Potable Water System Hydraulic Model

Woodard & Curran will perform a review of the existing potable water system model and associated documentation, including the November 13, 2020 Technical Memorandum by Water Systems Consulting, Inc. The purpose of the review will be to ensure that the modeling approach and data is appropriate for the performance assessments to be performed in subtasks 4.2 and 4.3 and for the storage analysis to be performed in Task 7. It is assumed that the version of the hydraulic model previously developed by the District will be sufficient for this task and that no additional model development, calibration or scenario development will be required. However, Woodard & Curran will provide suggestions for future model development, including additional calibration based on the review.

Subtask 4.2 – Horizontal Potable Water System Performance Assessment

Woodard & Curran will use the calibrated potable water system model to evaluate the performance of the water distribution system under a previously developed baseline scenario depicting current water system operations. The assessment will be used to identify system deficiencies with existing operations used as the basis for evaluation. Types of deficiencies to be identified could include, but are not limited to, excessive pipe velocities/head loss, high water age, excessive pressures, and low delivery pressures or available fire flow. Based on this assessment, improvement projects will be identified to address the deficiencies.

Subtask 4.3 – Horizontal Potable Water System Risk Assessment

Under this task, Woodard & Curran will work with District staff to establish the criteria to be used in the condition and risk assessment such as asset useful life, likelihood of failure (LOF) criteria and consequence of failure (COF) criteria. Woodard & Curran will utilize the information developed in Subtask 4.2 to conduct a condition and risk assessment for the District's potable horizontal infrastructure assets. The analysis will be used to produce risk scores for the District's distribution system pipelines, which are based on the pipelines' COF and LOF scores (e.g., risk score = COF x LOF). Based on the risk scores and condition assessment data, a list of potential construction projects and estimated costs will be developed to address compromised pipelines. The projects will be prioritized based on a cost-benefit ratio, with high priority projects identified to include in the near-term CIP (Task 8).

Subtask 4.4 – Develop Technical Memorandum

Woodard & Curran will prepare a draft and final Technical Memorandum to summarize the results of the potable water system performance and risk assessment. A draft technical memorandum will be submitted to District staff for review. District comments will be incorporated into the final technical memorandum.



Task 4 Deliverables

- Draft and Final Horizontal Potable Water System Performance and Risk Assessment Technical Memorandum

Task 5: Horizontal Non-Potable Water System Performance and Risk Assessment

Woodard & Curran will perform a performance and risk assessment of the horizontal non-potable water system, which includes below-grade infrastructure (pipelines, valves, etc.) that is included in the District's existing non-potable water system hydraulic model.

Subtask 5.1 – Review Existing Non-Potable Water System Hydraulic Model

Woodard & Curran will perform a review of the existing non-potable water system model and associated documentation. The purpose of the review will be to ensure that the modeling approach and data is appropriate for the performance assessments to be performed in subtasks 5.2 and 5.3. It is assumed that the version of the hydraulic model previously developed by the District will be sufficient for this task and that no additional model development, calibration or scenario development will be required. However, Woodard & Curran will provide suggestions for future model development, including additional calibration based on the review.

Subtask 5.2 – Update Non-Potable Water System Hydraulic Model

Woodard & Curran will review the District's existing hydraulic model and perform updates as needed to assess system performance. Updates are anticipated to include:

- Evaluate customer usage records to estimate monthly usage by customer type and add any new customers.
- Evaluate SCADA data related to water supply and tank levels to estimate diurnal usage patterns (separate usage patterns may be developed for up to 4 pressure zones, and for specific customers where data is available). Based on this data, and the evaluation of customer usage, a maximum day extended period simulation (EPS) scenario and a peak hour scenario will be developed. Up to three supply alternatives will also be developed.
- Model Validation and EPS Calibration to confirm the modeled facility controls are consistent with system operations. A two week summer calibration period will be used. Where modeled flow and pressure differs substantially from observed SCADA data, Woodard & Curran will work with the district to identify potential reasons. The fee estimate assumes that the operating controls in the model are generally consistent with current field operations.

Subtask 5.3 – Horizontal Non-Potable Water System Performance Assessment

Woodard & Curran will use the calibrated non-potable water distribution system model to evaluate the performance of the non-potable water distribution system under previously



developed baseline scenarios depicting current operations. The assessment will be used to identify system deficiencies with existing operations used as the basis for evaluation. Types of deficiencies to be identified could include, but are not limited to, excessive pipe velocities/head loss, high water age, and low delivery pressures. Based on this assessment, improvement projects will be identified to address the deficiencies.

Subtask 5.4 – Horizontal Non-Potable Water System Risk Assessment

Under this task, Woodard & Curran will work with District staff to establish the criteria to be used in the condition and risk assessment such as asset useful life, and LOF and COF criteria. Woodard & Curran will utilize the information collected in Subtask 5.2 to conduct a condition and risk assessment for the District's horizontal non-potable water infrastructure assets. The analysis will be used to produce risk scores for the District's distribution system pipelines, which are based on the pipelines' COF and LOF scores (e.g., risk score = COF x LOF). Based on the risk scores and condition assessment data, a list of potential construction projects and estimated costs will be developed to address compromised pipelines. The projects will be prioritized based on a cost-benefit ratio, with high priority projects identified to include in the near-term CIP (Task 8).

Subtask 5.5 – Develop Technical Memorandum

Woodard & Curran will prepare a draft and final Technical Memorandum to summarize the results of the non-potable water system performance and risk assessment. A draft technical memorandum will be submitted to District staff for review. District comments will be incorporated into the final technical memorandum.

Task 5 Deliverables

- Draft and Final Non-Potable Water System Performance and Risk Assessment Technical Memorandum

Task 6: Wastewater Collection System Condition Assessment

Due to limitations in available data on the horizontal wastewater system, Woodard & Curran proposes a less rigorous condition assessment as compared to the performance and risk assessments proposed for the potable and non-potable water systems. If Optional Task 9 is activated, a performance assessment (subtask 9.4) will be performed in addition to the condition assessment described below.

Subtask 6.1 – Horizontal Wastewater System Condition Assessment

Woodard & Curran perform an evaluation of the condition of the wastewater system. Woodard & Curran will work with District staff to identify repair, rehabilitation and replacement needs for the wastewater collection system and to develop a method of prioritization for these potential projects. The project identification will be based on GIS data, maintenance history (e.g. cleaning frequency, maintenance notes) data and recommendations of District staff. A list of potential construction projects and estimated costs will be developed to address compromised pipelines, with high priority projects identified to include in the near-term CIP (Task 8).



Subtask 6.2 – Develop Technical Memorandum

Woodard & Curran will prepare a draft and final Technical Memorandum to summarize the results of the horizontal wastewater system condition assessment. A draft technical memorandum will be submitted to District staff for review. District comments will be incorporated into the final technical memorandum.

Task 6 Deliverables:

- Draft and Final Horizontal Wastewater System Condition Assessment Technical Memorandum

Task 7: Potable Water System Storage Alternatives Analysis

Woodard & Curran will perform an analysis of potential potable water system storage alternatives using the potable water system hydraulic model utilized in Task 4. Unlike the assessment performed in Task 4, which is focused on the existing potable water system, this analysis will evaluate potential changes to storage facilities within the potable water system.

Subtask 7.1 – Alternatives Development

It is assumed that the Baseline scenario for this analysis will be the existing model scenario that was utilized for the potable system performance assessment in Task 4 above, and that no additional work will need to be performed on the Baseline scenario. Woodard & Curran will work with District staff to identify two alternatives reflecting changes to system storage within the potable water system. For each of these alternatives, brief descriptions and high-level cost estimates will be developed along with modeling assumptions. Assumptions for these alternatives will be developed and provided to District staff for review and approval prior to performing model simulations.

Subtask 7.2 – Hydraulic Model Simulation of Alternatives

Model simulations will be performed for the two system storage alternatives developed in Subtask 7.1. This will include updating the existing hydraulic baseline model to represent the potential changes to the storage and distribution system included in each alternative. Results developed for each alternative will be compared to the already existing Baseline scenario. Tables and figures will be developed depicting the results of the model simulations.

Subtask 7.3 –Develop Technical Memorandum

Woodard & Curran will prepare a draft and final Technical Memorandum to summarize the results of the potable water system storage alternatives analysis. A draft technical memorandum will be submitted to District staff for review. District comments will be incorporated into the final technical memorandum.

Task 7 Deliverables

- Draft and Final System Storage Alternatives Analysis Technical Memorandum



Task 8: Near-Term CIP Development

Under this task, Woodard & Curran will utilize the information developed from the assessments in the tasks above to develop a five- and ten- year capital improvement plan (CIP) to prioritize repair, rehabilitation and replacement needs of the District's existing infrastructure and proactively manage available capital funds.

Subtask 8.1 – Estimate Project Costs and Cost Factors

Estimated costs for each recommended repair, rehabilitation and replacement project identified in the previous tasks will be developed. Cost estimates will be prepared to AACE Class 5 standards (-50% to +100%). This task also includes developing cost factors to be used in the risk and rehabilitation/repair models, which will be based on simple replacement, using assumed per linear foot unit factors based on pipeline diameter, rather than project-specific estimates.

Subtask 8.2 – Establish CIP Goals, Priorities and Constraints

Woodard & Curran will work with District staff to establish goals, priorities and constraints for the development of the CIP. This will include identifying rating criteria to be used for project prioritization as well as funding levels and operational constraints (e.g., limits on the number of concurrent major projects).

Subtask 8.3 – Develop Project Ranking Matrix

Woodard & Curran will develop short project descriptions for the recommended repair, rehabilitation and replacement projects identified in the above tasks and develop project cost estimates for those projects. Costs and other relevant information for each project will be used to prioritize system improvements using the criteria developed in Subtask 8.1.

Subtask 8.4 – Develop Five- and Ten-Year CIP and Technical Memorandum

Woodard & Curran will develop a complete list of capacity and condition-related projects, prioritized and scheduled based on results of the work conducted under in the above tasks. Woodard & Curran will provide the Draft five- and ten-Year CIP to the District for review and will incorporate comments into a Final CIP. Woodard & Curran will prepare a Draft technical memorandum that outlines the goals of the CIP and presents the recommended improvements and costs to meet short and long-range requirements. Comments received on the Draft TM will be incorporated into a Final technical memorandum.

Task 8 Deliverables

- Draft and Final CIP, including individual project cost estimates and project prioritization and budgets by fiscal year. The final CIP will be formatted and editable in Excel and include a ranking for all recommended system improvements
- Draft and Final CIP Technical Memorandum



Optional Task 9: Wastewater System Model Development

Under this task, Woodard & Curran will develop a wastewater system model that will provide a performance assessment of the existing wastewater system and that can be used for future analyses by the District.

Subtask 9.1 – Data Collection and Review

Woodard & Curran will collect additional information, beyond what has already been collected in Task 2, needed to develop the wastewater system model. The information may include, but is not limited to:

- Available water consumption data by customer account;
- Latest County tax assessor's database and/or the District's customer billing database, which include parcel use information, number of dwelling units, lot sizes, etc., and sewer connections.
- Record drawings for all sewers 10-inches and larger;
- Pump station station as-built drawings and operating information (pump models, type, and capacities; pump curves, on and off operating levels);

Subtask 9.2 – Flow Monitoring

Flow monitoring will be conducted to quantify dry and wet weather flows in the system and to calibrate the sewer system hydraulic model. This task involves the following activities.

Flow Monitoring Planning

Woodard & Curran will develop a plan for temporary flow monitoring in the sewer system, including proposed flow monitoring and rain gauge locations. The monitoring plan will be designed to isolate critical sewer drainage basins. This subtask includes developing a preliminary plan, a workshop with the District to discuss feedback on the sites selected and coordination with the flow monitoring subcontractor, and identifying final sites.

Conduct Flow Monitoring

Woodard & Curran will subcontract with an experienced flow monitoring firm to perform the flow monitoring field work. After the District's review and approval of the flow-monitoring plan, Woodard & Curran's flow monitoring subcontractor will conduct a reconnaissance of the flow monitoring sites to confirm the locations are appropriate for monitoring from the standpoint of hydraulic conditions, safety, and access. The subcontractor will also determine the appropriate meter type and sensors for the specific hydraulic conditions at each site (all gravity flow meters will be area-velocity type, capable of recording both flow depth and velocity). The flow monitoring subcontractor will then install, calibrate and maintain the flow meters and rain gauge for up to 2 months during the rainy season and remove the equipment at the end of this monitoring period. Woodard & Curran will review flow monitoring site reports to confirm final flow meter locations and will periodically review the flow monitoring data during the flow monitoring periods to check data quality and consistency. The flow monitoring subcontractor will provide final electronic data files (15-minute data) at the conclusion of the monitoring.

The flow monitoring data will be provided to the District along with summary information for each flow monitoring site and plots of depth, velocity, flow rate, and rainfall. Analysis of the



flow monitoring data to quantify infiltration/inflow (I/I) and develop design flows is an integral part of model calibration and will be conducted as part of Subtask 9.3.

Subtask 9.2 Assumptions:

- District to indicate any known information concerning bypasses, overflows, critical surcharge areas, and maintenance habits that may impact the flow monitoring sites.
- District will clean sewers if needed to remove debris or sediment for meter installation.
- District will assist in providing access to any meter sites located out of public right-of-way and provide a secure site for rain gauge installation at a District facility or facilitate obtaining a site at another public facility.
- Flow monitoring will include approximately 5-6 flow monitors and 1 rain gauge for 2 months.

Subtask 9.3 – Hydraulic Model Development and Calibration

Woodard & Curran will develop and calibrate a hydraulic model of the collection system. Woodard & Curran will use InfoWorks™ ICM software and its own software licenses for the modeling work; however, all model files developed and generated as part of the project will be provided to the District at project conclusion. This will include the following activities.

Develop Model Network

Using data from the District's GIS and asset inventory database, Woodard & Curran will develop a hydraulic model of the sewer system. As the District's GIS data does not include elevation information, invert and rim elevation data will be extracted from sewer record drawings (supplemented with USGS DEM data, if appropriate). The modeled sewer network will include, at a minimum, all larger sewers and critical small diameter pipes, including those that serve areas of significant size, are known or suspected by District staff to have capacity problems, and is anticipated to include approximately 20 percent of District sewers. Where data from record drawings is unclear, Woodard & Curran would consult with District staff for clarification and/or field verification. Less critical smaller-diameter pipelines will not be included in the initial model but could be added in the future as needed. The model will also include any pump stations located within the modeled trunk network.

Following the construction of the model database, a QA/QC process called "model validation," will be used to verify the data before beginning any model runs. This process includes checking network connectivity and data completeness and reasonableness for apparent discrepancies (e.g., negative pipe slopes, outlet pipe invert elevations higher than inlet invert elevations etc.). Missing or suspect data will be resolved to the extent possible through review of available record drawings or requested field verification. The source of all new or updated data in the model will be documented directly in the model database using InfoWorks "flags" and notes.

Woodard & Curran will also delineate model subcatchment (subbasin) boundaries and assign the model loads and preliminary flow factors developed as part of Subtask 9.2 to the subcatchments.

Develop Existing Model Loads and Preliminary Flow Factors

Woodard & Curran will review existing parcel, customer billing and water use data, land use type, number and type of dwelling units, etc. that are collected under Task 2 to determine the



best approach for using this data to estimate existing base wastewater flows. The exact methodology to be used to develop model loadings will depend on the format and completeness of available parcel-based data; however, it is anticipated that a combination of the District's sewer customer database, water use records, and flow monitoring data will be the primary sources of data for developing model loads. It is anticipated that water use records will be used to develop model loads for the few non-residential parcels served by the Town.

Woodard & Curran will develop preliminary criteria to be used to estimate wastewater flows, including unit base wastewater flow factors for residential connections; diurnal base wastewater flow patterns; and infiltration/inflow parameters. These criteria will be developed based on the flow monitoring data plus our team's experience with similar systems. These criteria will be verified/refined through the model calibration process below.

Calibrate Model

Woodard & Curran will run the model under existing conditions and compare the computed dry weather and wet weather flow hydrographs to observed flow monitoring data. Modeling parameters such as unit flow rates, diurnal curves, and I/I factors will be adjusted as needed to achieve a reasonable match for modeled to metered flows.

Subtask 9.3 Assumptions:

- Data will be extracted from approximately 110 record drawings.
- Woodard & Curran will use its own model licenses for the work under this project
- District will provide record drawings, additional survey data if needed, and assistance with field verification if needed to obtain or confirm data for critical sewers included within the model.

Subtask 9.4 – System Evaluation

This task involves evaluation of collection system capacity and identification of specific improvement needs to address any deficiencies and includes the following activities.

Establish Capacity Evaluation and Design Criteria

Woodard & Curran will propose design and hydraulic criteria to be used for assessing the capacity of existing sewer facilities and sizing new facilities, including Manning's "n" factor for gravity sewers, maximum d/D values, minimum and maximum velocities, slopes, and depth of cover, and pump station design and reliability considerations (e.g., firm capacity). Woodard & Curran will also identify alternative approaches for defining an appropriate design storm or storms, including use of an actual historical storm or a synthetic event based on rainfall intensity-duration-frequency statistics. Woodard & Curran will propose criteria for evaluating the performance of the system under the design event (e.g., acceptable level of surcharge) that reflects the District's desired level of service and risk acceptance. The proposed criteria will be reviewed and discussed with District staff.

Evaluate Existing System Performance

Using the hydraulic model, Woodard & Curran will evaluate the performance of the existing gravity trunk sewers, pump stations included in the model, and force mains under existing and



future dry and design wet weather flows. Thematic maps and hydraulic gradeline plots will be prepared to present the identified capacity problem areas.

Subtask 9.5 – Develop Technical Memorandum

Woodard & Curran will prepare a draft and final Technical Memorandum to summarize development of the wastewater system model. A draft technical memorandum will be submitted to District staff for review. District comments will be incorporated into the final technical memorandum.

Task 9 Deliverables:

- Calibrated hydraulic model for the wastewater system (model files plus data exported to GIS and/or Excel tables), to be provided at project completion.
- Draft and Final Wastewater System Model Development Technical Memorandum

Optional Task 10: Outreach and Advocacy Plan Development

Woodard & Curran will work closely with District staff and Board of Directors to strategize the most effective ways to implement Public Outreach and Legislative/Regulatory Advocacy and will develop a plan outlining the efforts to do so.

Subtask 10.1 - Research

Woodard & Curran will review existing literature and host conversations to get a fundamental understanding of the District's needs and priorities. This may include involvement in or observation of one or more Strategic Planning Workshops (currently ongoing) by a communications specialist.

Subtask 10.2 - Workshop

Following completion of the Strategic Plan, our team will host a follow-up workshop specifically focused on outreach and advocacy activities. The intent of this workshop will be to strategize and discuss with District staff and Board members the intent and desired outcomes of outreach and advocacy efforts. The workshop will result in a prioritized list of issues that should be addressed in the Outreach and Advocacy Plan.

Subtask 10.3 - Plan Development

Using data gathered during the research phase, information and the issues list from the workshop, and best management practices, our team will develop a draft Outreach and Advocacy Plan that will be provided to the District for review. The plan will include:

- Key messages for the public
- Key messages for elected representatives
- Contact information for representatives
- Recommendations for website content management
- Recommendations for social media content and engagement



- Recommendations for “earned” media opportunities
- Analysis of the workload associated with recommendations

A final plan will then be developed that incorporates comments from District staff and Board members.

Task 10 Deliverables

- Draft and Final Outreach and Advocacy Plan



Schedule

The following schedule allows for completion of the Near-Term CIP by June 2023.

	Jul 2022	Aug 2022	Sep 2022	Oct 2022	Nov 2022	Dec 2022	Jan 2023	Feb 2023	Mar 2023	Apr 2023	May 2023	Jun 2023	Jul 2023	Aug 2023	Sep 2023
1. Project Management & Meetings															
2. Data Collection & Review															
3. Condition Assessment of Above Ground Facilities															
4. Assessment of Horizontal Potable Infrastructure															
5. Assessment of Horizontal RW Infrastructure															
6. Assessment of Horizontal WW Infrastructure															
7. System Storage Analysis															
8. Near-Term CIP Development															
9. Wastewater System Model Development															
10. Outreach & Advocacy Plan Development															

Tasks	Labor											Outside Services				ODCs		Total		
	Persephene St. Charles	Brian Van Lienden	Matt Elsner	Nate Hansen	Chris Van Lienden	Zoey Wang	Cathy Greenman	Gisa Ju	Planner/ Engineer	Katie Evans	Admin.	Total Hours	Total Labor Costs (1)	MKN	Wastewater Flow Monitoring	Subtotal	Sub Consultant Total Cost (2)	ODCs	Total ODCs (3)	Total Fee
	PIC	PM	Lead Engineer	Condition Assess.	Modeling Lead	Modeling	WW Model	WW Model	Support	Comm.	Admin			SUB	SUB					
	\$330	\$295	\$315	\$245	\$295	\$245	\$315	\$330	\$205	\$315	\$120									
Task 1: Project Management and Meetings																				
1.1 Project Management and Controls	4	64							32		16	116	\$28,680			\$0	\$0		\$0	\$28,680
1.2 Meetings with Staff (6), TAC (3) and Board (1)	24	56	24		8					8		120	\$36,880	\$16,412		\$16,412	\$18,053	\$780	\$858	\$55,791
Subtotal Task 1:	28	120	24	0	8	0	0	0	32	8	16	236	\$65,560	\$16,412	\$0	\$16,412	\$18,053	\$780	\$858	\$84,471
Task 2: Data Collection and Review																				
2.1 Compile and Review Documents and Data		4	8		4	16			32			64	\$15,360			\$0	\$0		\$0	\$15,360
Subtotal Task 2:	0	4	8	0	4	16	0	0	32	0	0	64	\$15,360	\$0	\$0	\$0	\$0	\$0	\$0	\$15,360
Task 3: Condition Assessment of Above Ground Facilities																				
3.1 Develop Plan for Above Ground Facility Condition Assessments		2	4						6			12	\$3,080	\$5,538		\$5,538	\$6,092		\$0	\$9,172
3.2 Perform Site Assessments of Above Ground Facilities			24									24	\$7,560	\$42,000		\$42,000	\$46,200	\$260	\$286	\$54,046
3.3 Develop Above Ground Condition Assessment TMs (3 TMs)		4	16						8			28	\$7,860	\$16,628		\$16,628	\$18,291		\$0	\$26,151
Subtotal Task 3:	0	6	44	0	0	0	0	0	14	0	0	64	\$18,500	\$64,166	\$0	\$64,166	\$70,583	\$260	\$286	\$89,369
Task 4: Horizontal Potable Water System Performance and Risk Assessment																				
4.1 Review Existing Potable Water System Hydraulic Model					12	40						52	\$13,340			\$0	\$0		\$0	\$13,340
4.2 Horizontal Potable Water System Performance Assessment			6		8	48						62	\$16,010			\$0	\$0		\$0	\$16,010
4.3 Horizontal Potable Water System Risk Assessment		2	16	32	4	8			48			110	\$26,450			\$0	\$0		\$0	\$26,450
4.4 Develop Technical Memorandum		2	10	24	12	24			20			92	\$23,140			\$0	\$0		\$0	\$23,140
Subtotal Task 4:	0	4	32	56	36	120	0	0	68	0	0	316	\$78,940	\$0	\$0	\$0	\$0	\$0	\$0	\$78,940
Task 5: Horizontal Non-Potable Water System Performance and Risk Assessment																				
5.1 Review Existing Non-Potable Water System Hydraulic Model					8	24						32	\$8,240			\$0	\$0		\$0	\$8,240
5.2 Update Non-Potable Water System Hydraulic Model					16	64			48			128	\$30,240			\$0	\$0		\$0	\$30,240
5.3 Horizontal Non-Potable Water System Performance Assessment			6		8	48						62	\$16,010			\$0	\$0		\$0	\$16,010
5.4 Horizontal Non-Potable Water System Risk Assessment		2	8	16	4	8			32			70	\$16,730			\$0	\$0		\$0	\$16,730
5.5 Develop Technical Memorandum		2	6	16	8	16			16			64	\$15,960			\$0	\$0		\$0	\$15,960
Subtotal Task 5:	0	4	20	32	44	160	0	0	96	0	0	356	\$87,180	\$0	\$0	\$0	\$0	\$0	\$0	\$87,180
Task 6: Horizontal Wastewater System Condition Assessment																				
6.1 Horizontal Wastewater System Condition Assessment		2	20	24					24			70	\$17,690			\$0	\$0		\$0	\$17,690
6.2 Develop Technical Memorandum		2	4	16					16			38	\$9,050			\$0	\$0		\$0	\$9,050
Subtotal Task 6:	0	4	24	40	0	0	0	0	40	0	0	108	\$26,740	\$0	\$0	\$0	\$0	\$0	\$0	\$26,740
Task 7: Potable Water System Storage Alternatives Analysis																				
7.1 Alternatives Development		8	4		8	8						28	\$7,940			\$0	\$0		\$0	\$7,940
7.2 Hydraulic Model Simulation of Alternatives (2)		8			24	32						64	\$17,280			\$0	\$0		\$0	\$17,280
7.3 Develop Technical Memorandum		8	4		16	32						60	\$16,180			\$0	\$0		\$0	\$16,180
Subtotal Task 7:	0	24	8	0	48	72	0	0	0	0	0	152	\$57,580	\$0	\$0	\$0	\$0	\$0	\$0	\$57,580
Task 8: Near-Term CIP Development																				
8.1 Estimate Project Costs and Cost Factors			16			24			80			120	\$27,320			\$0	\$0		\$0	\$27,320
8.2 Establish CIP Goals, Priorities and Constraints		2	4		4				8			18	\$4,670	\$9,006		\$9,006	\$9,907		\$0	\$14,577
8.3 Develop Project Ranking Matrix		2	8		4	4			8			26	\$6,910	\$14,641		\$14,641	\$16,105		\$0	\$23,015
8.4 Develop Five- and Ten-Year CIP and Technical Memorandum	4	4	12		6	12			50			88	\$21,240	\$8,063		\$8,063	\$8,869		\$0	\$30,109
Subtotal Task 8:	4	8	40	0	14	40	0	0	146	0	0	252	\$60,140	\$31,710	\$0	\$31,710	\$34,881	\$0	\$0	\$95,021
Optional Task 9: Wastewater Model Development																				
9.1 Review Data and Documents							6		12			18	\$4,350			\$0	\$0		\$0	\$4,350
9.2 Conduct Flow Monitoring							8	2	16			26	\$6,460		\$50,000	\$50,000	\$55,000		\$0	\$61,460
9.3 Hydraulic Model Development and Calibration							80	10	236			326	\$76,880			\$0	\$0		\$0	\$76,880
9.4 System Evaluation		2					22	3	40			67	\$16,710			\$0	\$0		\$0	\$16,710
9.5 Develop Technical Memorandum		2					30	6	48			86	\$21,860			\$0	\$0		\$0	\$21,860
Subtotal Task 9:	0	4	0	0	0	0	146	21	352	0	0	523	\$126,260	\$0	\$50,000	\$50,000	\$55,000	\$0	\$0	\$181,260
Optional Task 10: Outreach & Advocacy Plan Development																				
10.1 Research										8		8	\$2,520			\$0	\$0		\$0	\$2,520
10.2 Workshop	6	6							8	16		36	\$10,430			\$0	\$0	\$195	\$215	\$10,645
10.3 Plan Development	2	2							2	24		30	\$9,220			\$0	\$0		\$0	\$9,220
Subtotal Task 10:	8	8	0	0	0	0	0	0	10	48	0	74	\$22,170	\$0	\$0	\$0	\$0	\$195	\$215	\$22,385
TOTAL WITHOUT OPTIONAL TASKS	32	174	200	128	154	408	0	0	428	8	16	1548	\$410,000	\$112,288	\$0	\$112,288	\$123,517	\$1,040	\$1,144	\$534,661
TOTAL	40	186	200	128	154	408	146	21	790	56	16	2145	\$558,430	\$112,288	\$50,000	\$162,288	\$178,517	\$1,235	\$1,359	\$738,306

1. The individual hourly rates include salary, overhead and profit.

2. Subconsultants will be billed at actual cost plus 10%.

3. Other direct costs (ODCs) such as reproduction, delivery, mileage (rates will be those allowed by current IRS guidelines), and travel expenses, will be billed at actual cost plus 10%.

4. W&C reserves the right to adjust its hourly rate structure and ODC markup at the beginning of the calendar year for all ongoing contracts.

5. Additional Woodard & Curran staff may perform work on the project, based on our standard billing rate schedule currently in effect.

Board Memorandum

July 14, 2022

To: General Manager

From: Tamara Sexton, Finance Manager

Subject: Rate Adjustments

Objective: Adopt the proposed July 2022 rate adjustments.

Action Required: Adopt Resolution 22-11 of the Board adopting a Schedule of Rates, Fees and Charges for Water and Sanitary Service.

Discussion: The attached Resolution adopts the “Schedule of Rates, Fees and Charges for Water and Sanitary Service” for the commodity and fixed meter service fees.

On June 13, 2019, the Board of Directors convened a public hearing and adopted a five-year schedule of water and wastewater rates based upon the Rate Study prepared by Black & Veatch in 2019. The adopted rates were to be implemented beginning July 2019 through July 2023. During the development of the Fiscal Year (FY) 2021-2022 budget, staff and the Board agreed to defer the “July 2021” rate adjustment for the non-potable enterprise. The deferral of the non-potable rates was a result of higher contractual water sales to Pleasant Valley County Water District. It is unclear how consistent such volumes will be on an annual basis in the future. The last non-potable rate adjustment was on July 1, 2020. Potable rates were increased according to the five-year rate schedule proposed in the 2019 Rate Study.

Staff proposes implementing the “July 2022” potable and wastewater rates and the “July 2021” non-potable rates effective July 1, 2022. The proposed rate adjustment includes the projected operation and maintenance expenses, capital outlay, and reserves for the potable, non-potable and wastewater enterprise consistent with the cost-of-service analysis performed as part of the 2019 Rate Study. The adopted FY2022-23 operating budget assumed implementation of the “July 2021” non-potable rates and the “July 2022” potable and wastewater rates.

Attached is the modified Schedule of Rates, Fees and Charges for Water and Sanitary Service for FY2022-2023. The final rate increase of the five-year schedule proposed by the 2019 Rate Study will be in July 2023; a Schedule of Rates, Fees and Charges for Water and Sanitary Service for FY2023-2024 will be presented for Board approval during the budget process next year.

Resolution No: 22-11

A Resolution of the Board of Directors
of Camrosa Water District

Adopting a Schedule of Rates, Fees and Charges for Water and Sanitary Services

Whereas, the District's Ordinance 40-16, Rules and Regulations Governing the Provision of Water and Sanitary Services, requires that a "Schedule of Rates, Fees and Charges for Water and Sanitary Service" be adopted by Resolution of the Board; and

Whereas, sufficient net income must be generated from operations to ensure the long-term financial health of the District; and

Whereas, the District undertook a comprehensive Water and Wastewater Rate Study in 2019 to evaluate the existing water and wastewater rates to determine the best way to adequately fund water and wastewater utility operations and capital projects while keeping rates as affordable as possible; and

Whereas, on June 13, 2019 Board of Directors adopted the current 5-year Schedule of Rates, Fees and Charges for Water and Sanitary Service to accommodate the District's evolving demands, the steadily increasing cost of water imported through Calleguas Municipal Water District, the continually escalating costs of ongoing and new water and wastewater regulations, and increases in the cost of electrical power, fuel and chemicals, which includes rate increases scheduled for July 2019 through July 2023; and

Whereas, the Board of Directors elected to defer the adopted non-potable rates scheduled for July 2021, as a result of higher contractual water sales to Pleasant Valley County Water District; and

Whereas, as part of the development of the Fiscal Year 2022-23 operating budget, it was determined that implementation of the non-potable rates previously deferred is required to fund the projected operation and maintenance expenses, capital outlay, and reserves for non-potable water; and

Whereas, the proposed "Schedule of Rates, Fees and Charges for Water and Sanitary Service" will produce a balanced budget to accommodate projected capital expenditures, provide for reserves mandated by debt issuance covenants, and provide for necessary protection against unanticipated emergencies;

Now, Therefore, Be It Resolved by the Camrosa Water District Board of Directors that the existing rates for Water and Sanitary Service be increased sufficiently to ensure long-term financial stability of the District; and

Be It Further Resolved that the attached "Schedule of Rates, Fees and Charges for Water and Sanitary Service" is hereby adopted effective July 1, 2022;

Be It Further Resolved that the attached "Schedule of Rates, Fees and Charges for Water and Sanitary Service" may be automatically adjusted to pass through to the customer the adopted increases or decreases in the wholesale charges for water established by another public agency; and

Be It Further Resolved that the provision for automatic adjustments may only cover a period not to exceed five years, ending July 2023, without conducting another scheduled public hearing.

Adopted, Signed, and Approved this 14th day of July, 2022.

Eugene F. West, President
Board of Directors
Camrosa Water District

(ATTEST)
Tony L. Stafford, Secretary
Board of Directors
Camrosa Water District

Potable Water Service Classification (Unit rates per hundred cubic feet)		July 2019	July 2020	July 2021	July 2022	July 2023
Residential/Master Meter/Domestic Agricultural	First					
12 Units		3.28	3.47	3.61	3.81	4.01
Residential/Master Meter/Domestic Agricultural	13					
Units and Higher		3.65	3.82	4.01	4.22	4.45
Commercial/Industrial/Public		3.65	3.82	4.01	4.22	4.45
Municipal Irrigation/Residential Irrigation		3.65	3.82	4.01	4.22	4.45
Fire Service/Other		3.65	3.82	4.01	4.22	4.45
Agricultural Irrigation		3.65	3.82	4.01	4.22	4.45
Temporary Construction/Temporary Agricultural		4.91	5.29	5.6	5.88	6.17
Temporary Municipal		4.91	5.29	5.6	5.88	6.17
Emergency Water Service		4.91	5.29	5.6	5.88	6.17
Commercial/Industrial/Public Out of Bounds		4.91	5.29	5.6	5.88	6.17
Residential Out of Bounds		4.91	5.29	5.6	5.88	6.17
Non-Potable / Recycled Water Service Classification (Unit rates per hundred cubic feet)		July 2019	July 2020	No Adjustment	July 2022	July 2023
Non-Potable Commercial Agricultural		1.92	2.08		2.19	2.59
Non-Potable Landscape Irrigation Water		1.92	2.08		2.19	2.59
Non-Potable Residential Landscape		1.92	2.08		2.19	2.59
Non-Potable Temporary Construction		1.92	2.08		2.19	2.59
Blended Non-Potable Agricultural		2.46	2.7		3.15	3.67
Recycled Commercial Agricultural		1.92	2.08		2.19	2.59
Recycled Landscape Irrigation		1.92	2.08		2.19	2.59
Recycled Surplus Water (Served Outside District)		1.92	2.08		2.19	2.59
Contractual Non-Potable/Recycled Water Service (Unit rates per hundred cubic feet)		July 2017	January 2021	January 2022	January 2023	January 2024
Non-Potable Commercial Agricultural (contractual) - Note 1		0.61	0.62	0.67	tbd	tbd
Recycled Commercial Agricultural (contractual) - Note 1		0.40	0.40	0.43	tbd	tbd
Monthly Meter Service Charge		July 2019	July 2020	July 2021	July 2022	July 2023
Fire Service						
1		51.03	51.65	61.96	63.93	67.46
1.5		51.03	51.65	61.96	63.93	67.46
2		51.03	51.65	61.96	63.93	67.46
3		51.03	51.65	61.96	63.93	67.46
4		51.03	51.65	61.96	63.93	67.46
6		77.09	78.03	93.6	96.58	101.9
8		129.17	130.74	156.84	161.82	170.74
10		343.45	347.63	417.02	430.27	453.98
Potable/Blended Agricultural/Domestic Agricultural		July 2019	July 2020	July 2021	July 2022	July 2023
3/4 Master Metered		6.21	6.19	6.21	6.35	6.57
3/4		12.79	12.77	13.26	13.58	14.08
1		21.41	21.4	22.63	23.19	24.06
1.5		42.94	42.93	46.02	47.17	48.96
2		68.89	68.89	74.22	76.09	78.99
3		151.09	151.12	163.54	167.68	174.1
4		259.02	259.09	280.82	287.92	298.98
6		388.69	388.81	421.73	432.41	449.02
8		647.9	648.11	703.38	721.21	748.93
Non-Potable Irrigation		July 2019	July 2020	No Adjustment	July 2022	July 2023
3/4 Master Metered		4.89	4.88		4.91	5.20
3/4		7.51	7.52		8.09	8.60
1		10.28	10.32		11.72	12.51
1.5		17.19	17.30		20.78	22.25
2		25.52	25.72		31.70	33.99
3		51.90	52.40		66.30	71.19
4		86.54	87.43		111.72	120.02
6		128.16	129.51		166.30	178.70
8		211.35	213.63		275.39	295.99
Sewer Rates		July 2019	July 2020	July 2021	July 2022	July 2023
Monthly Sewer Charge		33.49	35.83	38.37	40.62	43.05
Residential Monthly Sewer Service through City of T.O.		July 2019	July 2020	July 2021	July 2022	July 2023
Monthly Sewer Charge		46.76	47.22	47.69	48.15	48.61

Notes:

1. Contractual customer agreements increase January based on index of prior fiscal year.
2. Pump Zone Surcharge: Applies to certain areas in the District that are situated at higher elevations; therefore require additional pumping for water delivery. Potable water pump zone charge is \$0.12 per HCF. Non-potable water pump zone charge is \$0.07 per HCF.
3. Wildwood Estates Facilities Construction Fee is \$0.152 per HCF.
4. Billing units in hundred cubic feet (HCF). One HCF equals 748 gallons. One acre-foot=435.6 HCF.

Board Memorandum

July 14, 2022

To: Board of Directors

From: General Manager

Subject: Closed Session Conference with Legal Counsel – Personnel

Objective: Conduct a performance review of the General Manager.

Action Required: No action necessary; for information only.

Discussion: The Board may enter closed session for discussion of the General Manager's performance (as authorized by Government Code 54957). The Board may not, however, based on advice of the Board's legal counsel, discuss the General Manager's compensation, or make any determinations to adjust it in closed session; the Board can only discuss and adjust compensation in open session.

Board Memorandum

July 14, 2022

To: Board of Directors

From: General Manager

Subject: General Manager's Performance and Salary Review

Objective: Review the General Manager's performance and compensation.

Action Required: Consider the General Manager's performance review and salary adjustment.

Discussion: The General Manager's performance and salary evaluation is the responsibility of the Board of Directors. The last performance evaluation and salary adjustment occurred at the Board meeting of June 24, 2021.

Board Memorandum

July 14, 2022

To: Board of Directors

From: General Manager

Subject: Salary and Classification Schedule

Objective: Adopt the Salary and Classification Schedule.

Action Required: Adopt Resolution 22-12 Adjusting the District's Salary and Classification Schedule for Employees.

Discussion: The Salary and Classification Schedule is to be approved by the Board of Directors if there is a change.

The Salary and Classification Schedule is being updated to reflect five new positions included in the Fiscal Year 2022-23 budget, two of which are for succession of future retirees. The five positions are: IT Coordinator, Water Loss Control Coordinator, Laboratory Analyst I, and two System Operators (I).

In addition, the maximum salary range is being adjusted for the following positions: District Engineer, Finance Manager, I.T. and Special Projects Manager, System Operator II, and Instrumentation Technician.

The Laboratory Technician classification is being reclassified as Laboratory Analyst I/II, and Water Quality Supervisor to Laboratory Supervisor.

The attached salary schedule is recommended for approval.

Resolution No: 22-12

A Resolution of the Board of Directors
of Camrosa Water District

**Adjusting the District's Salary and
Classification Schedule for Employees**

Whereas, the Board of Directors shall establish by resolution a Salary and Classification Schedule consisting of salary rates allocated to salary ranges; and

Whereas, except as otherwise provided herein, employees shall receive compensation provided in the Salary and Classification Schedule for the classification of the position in which they are employed; and

Whereas, the Salary and Classification Schedule shall include a descriptive title, salary ranges, and the number of allocated positions; and

Whereas, the General Manager shall recommend to the Board of Directors changes in the Salary and Classification Schedule to meet the needs of the District; and

Whereas, such changes may include but not be limited to a new position, salary range adjustment for the position, reclassification of the position only, or reclassification of the incumbent within the position, and must be submitted to the Board of Directors for approval; and

Whereas, the General Manager may appoint new employees within the salary range of the classifications, in accordance with the Salary and Classification Schedule; and

Whereas, the District's Salary and Classification Schedule attached hereto shall reclassify position titles, add new positions approved by the Board as part of the Fiscal Year 2022-23 budget and adjust the maximum salary ranges of positions which have attained near maximum range; and

Now, Therefore, Be It Resolved that the Camrosa Water District Board of Directors hereby adopts the Salary and Classification Schedule.

Adopted, Signed, and Approved this 14th day of July, 2022.

Eugene F. West, President
Board of Directors
Camrosa Water District

(ATTEST)
Tony L. Stafford, Secretary
Board of Directors
Camrosa Water District

CAMROSA WATER DISTRICT SALARY SCHEDULE

SALARY AND CLASSIFICATION SCHEDULE

Effective: July 9, 2022

Position	Minimum	Original Max	Adjusted Maximum	FTE	FLSA	Time Base
Assistant General Manager/Water Resources & Regulatory Compliance	\$ 130,000	\$ 185,000		1	N	Annually
Chief Plant Operator	\$ 75,000	\$ 100,000		1	Y	Annually
Customer Service Manager	\$ 100,000	\$ 135,000		1	N	Annually
Customer Service Representative/ Accounts Payable Technician	\$ 45,000	\$ 67,500		1	Y	Annually
Customer Service Representative/Administrative Assistant	\$ 45,000	\$ 67,500		1	Y	Annually
District Engineer	\$ 110,000	\$ 155,000	\$ 160,000	1	N	Annually
Manager of Engineering & Capital Projects	\$ 120,000	\$ 175,000		0	N	Annually
Field Service Technician I	\$ 40,000	\$ 55,000		0	Y	Annually
Field Service Technician II	\$ 45,000	\$ 60,000		2	Y	Annually
Finance Manager	\$ 110,000	\$ 165,000	\$ 170,000	1	N	Annually
General Manager	\$ 241,020	\$ 241,020		1	N	Annually
GIS Specialist	\$ 55,000	\$ 80,000		0	Y	Annually
I.T. and Special Projects Manager	\$ 120,000	\$ 175,000	\$ 180,000	1	N	Annually
IT Coordinator	\$ 75,000	\$ 105,000		1	Y	Annually
Instrumentation Technician	\$ 65,000	\$ 90,000	\$ 95,000	2	Y	Annually
Laboratory Technician	\$ 55,000	\$ 80,000				
Laboratory Analyst I	\$ 45,000	\$ 60,000		1	Y	Annually
Laboratory Analyst II	\$ 60,000	\$ 90,000		1	Y	Annually
Laboratory Supervisor	\$ 90,000	\$ 120,000		0	N	Annually
Senior Accountant	\$ 75,000	\$ 105,000		1	N	Annually
Senior Customer Service Representative	\$ 65,000	\$ 85,000		0	Y	Annually
Senior Customer Service Representative/Specialist	\$ 70,000	\$ 97,365		1	Y	Annually
Senior Field Service Technician	\$ 55,000	\$ 70,000		0	Y	Annually
Senior System Operator	\$ 75,000	\$ 105,000		2	Y	Annually
Superintendent of Operations	\$ 115,000	\$ 155,000		1	N	Annually
System Field Supervisor	\$ 80,000	\$ 110,000		0	Y	Annually
System Operator I	\$ 55,000	\$ 75,000		4	Y	Annually
System Operator II	\$ 60,000	\$ 85,000	\$ 90,000	2	Y	Annually
Water Loss Control Coordinator	\$ 80,000	\$ 100,000		1	Y	Annually
Water Quality & Environmental Compliance Supervisor	\$ 100,000	\$ 142,371		1	N	Annually
Water Quality Supervisor	\$ 90,000	\$ 120,000				
				29		
Board Member (per Meeting)	\$ 200.00				N	Per Meeting
Part-Time Student/Paid Internship	\$ 16.00				Y	Hourly
Part-Time/Temporary Employee	\$ 16.00				Y	Hourly



Read File

The following material is provided to members of the Board for information only and is not formally a part of the published agenda.

- A. Vendor Listing
- B. 2022 Board Calendar

Purchase From Vendor Pay To Vendor	Payable Number	Post Date	Item	Payment
FRB - First Republic Bank				
Paid To Same Vendor				
FRB - First Republic Bank	Pymt#3 Retention	04/08/2022	Retention Made to Repibic Bank (James Chusman)	10228.95
FRB - First Republic Bank	RetentionCUS5-PPE#4	05/17/2022	Retention Cuschamn Inc.(CUS05) PPO#4	10766.7
FRB - First Republic Bank	Retention Pymt5	06/14/2022	Retention Pymt #5	30120.6
				51116.25
ACL01 - ACLARA TECHNOLOGIES				
Paid To Same Vendor				
ACL01 - ACLARA TECHNOLOGIES	22102233	06/10/2022	MTUs	43543.5
ACW02 - ACWA JOINT POWERS INS				
Paid To Same Vendor				
ACW02 - ACWA JOINT POWERS INS	1stQTR-2022	04/01/2022	Workers Comp Premium 1st QTR 2022	8215.45
AGR00 - AG RX INC.				
Paid To Same Vendor				
AGR00 - AG RX INC.	99568	04/13/2022	Weed abatement	4812.63
AGR00 - AG RX INC.	99619	04/13/2022	Weed abatement	3132.2
AGR00 - AG RX INC.	99761	06/01/2022	Weed abatement	6464.32
AGR00 - AG RX INC.	99765	06/15/2022	Weed abatement	4502.81
				18911.96
ALE01 - ALEXANDER'S CONTRACT SERVICES, INC				
Paid To Same Vendor				
ALE01 - ALEXANDER'S CONTRACT SERVICES, INC	104014	04/08/2022	Meter Reading	1488.69
ALE01 - ALEXANDER'S CONTRACT SERVICES, INC	104051	05/04/2022	Meter Reading	1487.42
ALE01 - ALEXANDER'S CONTRACT SERVICES, INC	104116	06/01/2022	Meter Reading Service	1473.9
				4450.01
ALL06 - ALLCABLE				
Paid To Same Vendor				
ALL06 - ALLCABLE	4031864	05/17/2022	1B Comm Building Enclosure	830.3
ALL06 - ALLCABLE	4032524	06/27/2022	4B Radio Tower	160.6
ALL06 - ALLCABLE	4032586	06/27/2022	4B Radio Tower	740.17
ALL06 - ALLCABLE	4032603	06/30/2022	Cat6 Cable	2731.25
ALL06 - ALLCABLE	4032605	06/30/2022	Radio Tower 4B	191.19
				4653.51
ALL07 - ALLIED ELECTRONICS, INC				
Paid To Same Vendor				
ALL07 - ALLIED ELECTRONICS, INC	9016400576	06/27/2022	4B Radio Tower - Parts	2845.23
ALL07 - ALLIED ELECTRONICS, INC	9016400577	06/27/2022	4B Radio Tower - Power Converters	817.76
				3662.99
ALL11 - ALL PEST AND REPAIR, INC.				
Paid To Same Vendor				

ALL11 - ALL PEST AND REPAIR, INC.	0025442	04/29/2022	Pest Control - VTA1-1900	600
ALL11 - ALL PEST AND REPAIR, INC.	0025475	04/29/2022	Pest Control - VTA1-7385	420
ALL11 - ALL PEST AND REPAIR, INC.	0025541	05/17/2022	Pest Control-VTA1-1900	600
ALL11 - ALL PEST AND REPAIR, INC.	0025578	05/17/2022	Pest Control-VTA1-7385	420
ALL11 - ALL PEST AND REPAIR, INC.	0025644	06/14/2022	Outside Contracts - Pest Control	600
ALL11 - ALL PEST AND REPAIR, INC.	0025681	06/14/2022	Outside Contracts - Pest Control	420
				<hr/>
				3060

ALL14 - ALLCONNECTED INC

Paid To Same Vendor

ALL14 - ALLCONNECTED INC	105182	04/07/2022	AllConnected - Managed IT/OT Services	7489.04
ALL14 - ALLCONNECTED INC	43069	05/03/2022	AllConnected - Managed IT/OT Services	1936.8
ALL14 - ALLCONNECTED INC	105207	05/17/2022	AllConnected - Managed IT/OT Services	7489.04
ALL14 - ALLCONNECTED INC	43081	05/17/2022	AllConnected - Managed IT/OT Services	11880.26
ALL14 - ALLCONNECTED INC	43082	05/17/2022	AllConnected - Managed IT/OT Services	8382.5
ALL14 - ALLCONNECTED INC	105229	05/26/2022	AllConnected - Managed IT/OT Services	7489.04
ALL14 - ALLCONNECTED INC	43095	05/26/2022	AllConnected - Managed IT/OT Services	1500.75
ALL14 - ALLCONNECTED INC	43096	05/26/2022	AllConnected - Managed IT/OT Services	2219.74
ALL14 - ALLCONNECTED INC	43097	05/26/2022	AllConnected - Managed IT/OT Services	12331.63
ALL14 - ALLCONNECTED INC	105473	06/10/2022	AllConnected - Managed IT/OT Services	7489.54
				<hr/>
				68208.34

AME13 - AMERICAN PUBLIC WORKS CONSULTING ENGINEERS, LLC

Paid To Same Vendor

AME13 - AMERICAN PUBLIC WORKS CONSULTING ENGINEERS, LLC	2022-8	04/11/2022	PV Well No. 2 Project Management Services	3875
AME13 - AMERICAN PUBLIC WORKS CONSULTING ENGINEERS, LLC	2022-9	05/03/2022	PV Well No. 2 Project Management Services	4960
				<hr/>
				8835

AQU02 - AQUA-METRIC SALES CO

Paid To Same Vendor

AQU02 - AQUA-METRIC SALES CO	INV0087808	05/04/2022	NP Meters	41033.06
AQU02 - AQUA-METRIC SALES CO	INV0087808-R	05/04/2022	NP Meters	-41033.06
AQU02 - AQUA-METRIC SALES CO	IN0087808-	05/10/2022	NP Meters	38259.26
				<hr/>
				38259.26

ASC01 - ACWA/JPIA

Paid To Same Vendor

ASC01 - ACWA/JPIA	3-22 PR ME	04/01/2022	COBRA, Dir West & Swann premiums	3829.93
ASC01 - ACWA/JPIA	INV0011295	04/01/2022	Dental Insurance	312.16
ASC01 - ACWA/JPIA	INV0011296	04/01/2022	Medical-PPO	3934.65
ASC01 - ACWA/JPIA	INV0011297	04/01/2022	Vision	86.05
ASC01 - ACWA/JPIA	INV0011309	04/01/2022	Dental Insurance	2097.34
ASC01 - ACWA/JPIA	INV0011316	04/01/2022	Medical-HMO	20759.4
ASC01 - ACWA/JPIA	INV0011317	04/01/2022	Medical-PPO	2461.44
ASC01 - ACWA/JPIA	INV0011318	04/01/2022	Medical-PPO	15076.38
ASC01 - ACWA/JPIA	INV0011328	04/01/2022	Vision	413.04
ASC01 - ACWA/JPIA	4-22 PR ME	05/02/2022	COBRA premium, Dir West Premium & Swann Credit	3406.11
ASC01 - ACWA/JPIA	INV0011462	05/02/2022	Dental Insurance	2063.62
ASC01 - ACWA/JPIA	INV0011469	05/02/2022	Medical-HMO	19901.57
ASC01 - ACWA/JPIA	INV0011470	05/02/2022	Medical-PPO	2461.44

ASC01 - ACWA/JPIA	INV0011471	05/02/2022	Medical-PPO	15076.38
ASC01 - ACWA/JPIA	INV0011481	05/02/2022	Vision	395.83
ASC01 - ACWA/JPIA	INV0011486	05/02/2022	Dental Insurance	312.16
ASC01 - ACWA/JPIA	INV0011487	05/02/2022	Medical-PPO	3934.65
ASC01 - ACWA/JPIA	INV0011488	05/02/2022	Vision	86.05
ASC01 - ACWA/JPIA	5-22 PR ME	06/01/2022	COBRA premium, Credit Lajoie, Dir West Premium	2254.88
ASC01 - ACWA/JPIA	INV0011555	06/01/2022	Dental Insurance	2063.62
ASC01 - ACWA/JPIA	INV0011562	06/01/2022	Medical-HMO	19901.57
ASC01 - ACWA/JPIA	INV0011563	06/01/2022	Medical-PPO	2461.44
ASC01 - ACWA/JPIA	INV0011564	06/01/2022	Medical-PPO	15076.38
ASC01 - ACWA/JPIA	INV0011574	06/01/2022	Vision	395.83
ASC01 - ACWA/JPIA	INV0011578	06/01/2022	Dental Insurance	312.16
ASC01 - ACWA/JPIA	INV0011579	06/01/2022	Medical-PPO	3934.65
ASC01 - ACWA/JPIA	INV0011580	06/01/2022	Vision	86.05
				143094.78
AWA01 - AWA				
Paid To Same Vendor				
AWA01 - AWA	06-14217	06/08/2022	Lunch Symposium-4 Attendees	400
AWA01 - AWA	06-14245	06/30/2022	AWA Training Course (TC)	30
				430
BAD02 - BADGER METER INC				
Paid To Same Vendor				
BAD02 - BADGER METER INC	1504630	06/30/2022	Potable Meters	4613.9
BAD02 - BADGER METER INC	1508379	06/30/2022	Potable Meters	5234.87
BAD02 - BADGER METER INC	1509625	06/30/2022	Potable Meters	4729.73
BAD02 - BADGER METER INC	1513008	06/30/2022	Potable Meters	3320.46
BAD02 - BADGER METER INC	1513626	06/30/2022	Potable Meters	72509.58
				90408.54
BAS02 - BASELINE ENTERPRISES				
Paid To Same Vendor				
BAS02 - BASELINE ENTERPRISES	19541	04/11/2022	Fuel Tank Inspection	981.75
BAS02 - BASELINE ENTERPRISES	19559	04/29/2022	Outside Contracts - Fuel Tank Inspection	981.75
BAS02 - BASELINE ENTERPRISES	19628	05/17/2022	Fuel Tank Inspection	981.75
BAS02 - BASELINE ENTERPRISES	19714	06/14/2022	Outside Contracts - Fuel Tank Inspection	981.75
				3927
BLA06 - BLACK MAGIC METAL ART INC.				
Paid To Same Vendor				
BLA06 - BLACK MAGIC METAL ART INC.	900	06/30/2022	Repair Parts - Antenna Mounts	960
BON01 - BONDY GROUNDWATER CONSULTING, INC.				
Paid To Same Vendor				
BON01 - BONDY GROUNDWATER CONSULTING, INC.	077-06	04/08/2022	PM: Santa Rosa GSP	3542.5
BON01 - BONDY GROUNDWATER CONSULTING, INC.	083-01	04/11/2022	University Well Investigation	163.5
BON01 - BONDY GROUNDWATER CONSULTING, INC.	GSA077-07	05/18/2022	PM: Santa Rosa GSP	1547.06
BON01 - BONDY GROUNDWATER CONSULTING, INC.	077-08 GSA	05/31/2022	PM: Santa Rosa GSP	5014
				10267.06

BOS02 - BOSCO CONSTRUCTORS, INC.**Paid To Same Vendor**

BOS02 - BOSCO CONSTRUCTORS, INC.	Pymt #3	04/12/2022	Effluent Pond Construction Services	183464.26
BOS02 - BOSCO CONSTRUCTORS, INC.	Retention-Pymt#3	04/12/2022	Retention Pymt#3- Project- RW21-01	-9173.21
				174291.05

BOU02 - BOUTWELL*FAY LLP**Paid To Same Vendor**

BOU02 - BOUTWELL*FAY LLP	35180	04/08/2022	Legal Services Profit Share	2014.5
--------------------------	-------	------------	-----------------------------	--------

BRE02 - BRENNTAG PACIFIC, INC.**Paid To Same Vendor**

BRE02 - BRENNTAG PACIFIC, INC.	BPI236982	04/29/2022	Materials & Supplies - Chemicals RMWTP	4098.53
BRE02 - BRENNTAG PACIFIC, INC.	BPI247926	06/10/2022	Materials & Supplies - Checimals RMWTP	6134.65
				10233.18

CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT**Paid To Same Vendor**

CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT	033422	04/12/2022	Water Purchase	672618.51
CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT	SMP031022	04/12/2022	SMP CMWD - SMP Pipeline Fee	14963.07
CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT	040822	05/17/2022	Water Purchase	633116.89
CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT	smp041822	05/17/2022	SMP CMWD-SMP Pipeline Fee	16528.18
CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT	055922	06/10/2022	Water Purchase	761114.59
CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT	2022-00000025	06/10/2022	SMP CMWD - SMP Sampling Fee	1772
CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT	SMP051022	06/10/2022	SMP CMWD - SMP Pipeline Fee	16901.65
				2117014.89

CAN03 - Cannon Corporation**Paid To Same Vendor**

CAN03 - Cannon Corporation	79561	04/11/2022	Contract Inspection Services	2175
CAN03 - Cannon Corporation	79566	04/11/2022	Contract Inspection Services	5365
CAN03 - Cannon Corporation	79652	05/03/2022	Construction Services	1183.5
CAN03 - Cannon Corporation	80059	05/03/2022	Engineering Support Services during construction	112.25
CAN03 - Cannon Corporation	80140	05/03/2022	Contract Inspection Services	725
CAN03 - Cannon Corporation	80141	05/03/2022	Construction Services	870
CAN03 - Cannon Corporation	80142	05/03/2022	Out of Scope	841.5
CAN03 - Cannon Corporation	80143	05/03/2022	Contract Inspection Services	408
CAN03 - Cannon Corporation	80144	05/03/2022	Contract Inspection Services	5485.5
CAN03 - Cannon Corporation	80145	05/03/2022	Engineering Support Services during construction	2755
CAN03 - Cannon Corporation	80287	05/17/2022	Construction Services	682
CAN03 - Cannon Corporation	80342	05/17/2022	Engineering Support Services during construction	3025
CAN03 - Cannon Corporation	80343	05/17/2022	Contract Inspection Services	4364
CAN03 - Cannon Corporation	80344	05/17/2022	Contract Inspection Services	1496
CAN03 - Cannon Corporation	80345	05/17/2022	Out of Scope	217.5
CAN03 - Cannon Corporation	80346	05/17/2022	Construction Services	1871.5
CAN03 - Cannon Corporation	80347	05/17/2022	Contract Inspection Services	1353
CAN03 - Cannon Corporation	80331	05/31/2022	Design Camsprings new waterline under Conejo Creek	12510.75
CAN03 - Cannon Corporation	80456	05/31/2022	Engineering Support Services during construction	72.5
CAN03 - Cannon Corporation	78993	06/10/2022	Additional Analysis	354.5

CAN03 - Cannon Corporation	78993	06/10/2022	Design Services Res 4C Tank	5232.35
CAN03 - Cannon Corporation	80570	06/28/2022	Engineering Support Services during construction	223
CAN03 - Cannon Corporation	80627	06/28/2022	Design Camsprings new waterline under Conejo Creek	11022.04
CAN03 - Cannon Corporation	80653	06/28/2022	Construction Services	1947.05
CAN03 - Cannon Corporation	80805	06/28/2022	Contract Inspection Services	1223.5
CAN03 - Cannon Corporation	80806	06/28/2022	Engineering Support Services during construction	3228
CAN03 - Cannon Corporation	80807	06/28/2022	Contract Inspection Services	4527
CAN03 - Cannon Corporation	80808	06/28/2022	Contract Inspection Services	1156
CAN03 - Cannon Corporation	80809	06/28/2022	Out of Scope	652.5
CAN03 - Cannon Corporation	80810	06/28/2022	Construction Services	1205.5
				76284.44
CAT02 - CATALYST DIVING INC				
Paid To Same Vendor				
CAT02 - CATALYST DIVING INC	05272022-2	06/01/2022	Reservoir Cleaning	12125
CAT02 - CATALYST DIVING INC	05272022-3	06/01/2022	Reservoir Cleaning	4381.5
				16506.5
CDT01 - CALIFORNIA DEPARTMENT OF TAX ADMINISTRATION				
Paid To Same Vendor				
CDT01 - CALIFORNIA DEPARTMENT OF TAX ADMINISTRATION	1st Qtr-2022	04/29/2022	Use Tax 1st Qtr 2022	26
CEI01 - COMMUNICATION ENTERPRISES, INC.				
Paid To Same Vendor				
CEI01 - COMMUNICATION ENTERPRISES, INC.	163202	05/03/2022	1B Radio Hut Transfer Radio Equipment	11187.93
CEN03 - Central Courier LLC				
Paid To Same Vendor				
CEN03 - Central Courier LLC	50918	04/08/2022	Courier Service	433.25
CEN03 - Central Courier LLC	51039	05/17/2022	Courier Service	433.25
CEN03 - Central Courier LLC	51223	06/15/2022	Courier Services	750.84
				1617.34
CHR04 - CHROMALOX INC				
Paid To Same Vendor				
CHR04 - CHROMALOX INC	1849735	05/03/2022	CIP Tank Heater - RMWTP	10351.09
CIT01 - CITY OF CAMARILLO				
Paid To Same Vendor				
CIT01 - CITY OF CAMARILLO	29538	06/30/2022	Recycled Water from CamSan per June 2017 agrrement	61612.58
CLI01 - CLIFTON LARSON ALLEN LLP				
Paid To Same Vendor				
CLI01 - CLIFTON LARSON ALLEN LLP	3332619	06/30/2022	Profesional Auditing Services FY2021-22	600
CLI01 - CLIFTON LARSON ALLEN LLP	3332619-2	06/30/2022	GASB 87 Lease Accounting Implementation Assistance	1600
				2200
CMU01 - CALIFORNIA MUNICIPAL UTILITIES ASSOCIATION				
Paid To Same Vendor				
CMU01 - CALIFORNIA MUNICIPAL UTILITIES ASSOCIATION	20-0424	06/15/2022	Annual Membership 7-01-22 th 6-30-23	4179

COL04 - COLONIAL SUPPLEMENTAL INS**Paid To Same Vendor**

COL04 - COLONIAL SUPPLEMENTAL INS	INV0011456	04/21/2022	Colonial Benefits	101.42
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011457	04/21/2022	Colonial Benefits	29.3
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011458	04/21/2022	Colonial Benefits	41.4
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011459	04/21/2022	Colonial Benefits	107.1
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011549	05/19/2022	Colonial Benefits	101.42
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011550	05/19/2022	Colonial Benefits	29.3
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011551	05/19/2022	Colonial Benefits	41.4
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011552	05/19/2022	Colonial Benefits	107.1
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011738	06/16/2022	Colonial Benefits	101.42
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011739	06/16/2022	Colonial Benefits	29.3
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011740	06/16/2022	Colonial Benefits	41.4
COL04 - COLONIAL SUPPLEMENTAL INS	INV0011741	06/16/2022	Colonial Benefits	107.1
				837.66

COR03 - CORELOGIC INFORMATION SOLUTIONS, INC**Paid To Same Vendor**

COR03 - CORELOGIC INFORMATION SOLUTIONS, INC	30600088	04/29/2022	Ventura Cty Assessors Parcel Info	154.5
COR03 - CORELOGIC INFORMATION SOLUTIONS, INC	30604323	05/18/2022	Ventura County Assessors Parcel Info	154.5
COR03 - CORELOGIC INFORMATION SOLUTIONS, INC	30610338	06/15/2022	Ventura Cty Assesors Parcel Info-Online Services	154.5
				463.5

COR04 - Core & Main LP**Paid To Same Vendor**

COR04 - Core & Main LP	Q768217	05/17/2022	6" Meters for CSUCI	8830.3
------------------------	---------	------------	---------------------	--------

COU01 - COUNTY OF VENTURA RMA OPERATIONS**Paid To Same Vendor**

COU01 - COUNTY OF VENTURA RMA OPERATIONS	IN0225797	05/17/2022	Permit - Environmental Health Inspection RMWTP	3133.69
COU01 - COUNTY OF VENTURA RMA OPERATIONS	IN0225531	05/27/2022	County Cross Connection Program	3961.57
				7095.26

COU03 - COUNTY OF VENTURA PUBLIC WORKS**Paid To Same Vendor**

COU03 - COUNTY OF VENTURA PUBLIC WORKS	332737	04/13/2022	Leak Repair- Encroachment permit	1570
--	--------	------------	----------------------------------	------

CTO00 - CITY OF THOUSAND OAKS**Paid To Same Vendor**

CTO00 - CITY OF THOUSAND OAKS	301-50122	05/18/2022	Sewer Treatment Read Road Tract Sewer	1078.2
-------------------------------	-----------	------------	---------------------------------------	--------

CUL02 - CULLIGAN OF VENTURA COUNTY**Paid To Same Vendor**

CUL02 - CULLIGAN OF VENTURA COUNTY	2010478-April22	04/11/2022	Water Softener - Penny Well	77.5
CUL02 - CULLIGAN OF VENTURA COUNTY	May2022	05/03/2022	Water Softener - Penny Well	72.5
CUL02 - CULLIGAN OF VENTURA COUNTY	Jun20-2010478	06/10/2022	Water Softener - Penny Well - Cust#2010478	72.5
				222.5

CUS01 - CUSTOM PRINTING**Paid To Same Vendor**

CUS01 - CUSTOM PRINTING	163387	06/08/2022	Window Envelopes	553.18
CUS01 - CUSTOM PRINTING	163387-R	06/08/2022	Window Envelopes	-553.18
CUS01 - CUSTOM PRINTING	163387-1	06/20/2022	Window Envelopes	535.18
				535.18
CUS05 - JAMES C. CUSHMAN, INC.				
Paid To Same Vendor				
CUS05 - JAMES C. CUSHMAN, INC.	Pymt#3	04/08/2022	GAC Construction	204579
CUS05 - JAMES C. CUSHMAN, INC.	Retention Pymt#3	04/08/2022	Retention Payment #3	-10228.95
CUS05 - JAMES C. CUSHMAN, INC.	PPE#4	05/17/2022	GAC Construction	215334
CUS05 - JAMES C. CUSHMAN, INC.	Reternrtion-PPE#4	05/17/2022	Retention on Invoice Ref# PPE#4	-10766.7
CUS05 - JAMES C. CUSHMAN, INC.	Pymt#5	06/14/2022	GAC Construction	602412
CUS05 - JAMES C. CUSHMAN, INC.	Retention-Pymt 5	06/14/2022	Retention Payment #5	-30120.6
				971208.75
DAM01 - DAMAR CONSTRUCTION INC				
Paid To Same Vendor				
DAM01 - DAMAR CONSTRUCTION INC	22027-001	05/17/2022	Sand Removal	9920.5
DAN05 - DANIELS TIRE SERVICE, INC				
Paid To Same Vendor				
DAN05 - DANIELS TIRE SERVICE, INC	250118916	05/03/2022	F550 Tires	1662.79
DIE01 - DIENER'S ELECTRIC, INC				
Paid To Same Vendor				
DIE01 - DIENER'S ELECTRIC, INC	33155	05/31/2022	Power Study CWRF RMWTP	6000
EDD01 - EMPLOYMENT DEVELOP. DEPT.				
Paid To Same Vendor				
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011395	04/07/2022	Payroll-SIT	4423.1
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011422	04/12/2022	Payroll-SIT	1185.72
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011485	04/21/2022	Payroll-SIT	3839.48
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011491	04/21/2022	Payroll-SIT	13.2
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011495	04/28/2022	Payroll-SIT	13.65
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011516	05/05/2022	Payroll-SIT	3883.95
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011577	05/19/2022	Payroll-SIT	3759.57
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011584	05/19/2022	Payroll-SIT	12.37
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011645	06/02/2022	Payroll-SIT	4157.49
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011766	06/16/2022	Payroll-SIT	3791.87
EDD01 - EMPLOYMENT DEVELOP. DEPT.	CM0000374	06/27/2022	Payroll-SIT	-0.84
EDD01 - EMPLOYMENT DEVELOP. DEPT.	INV0011822	06/30/2022	Payroll-SIT	3954.99
				29034.55
EJH01 - E.J. HARRISON & SONS INC				
Paid To Same Vendor				
EJH01 - E.J. HARRISON & SONS INC	855	04/11/2022	Trash Removal Role off Bins	763.29
EJH01 - E.J. HARRISON & SONS INC	33436	04/29/2022	Trash Removal - CWRF	494.59
EJH01 - E.J. HARRISON & SONS INC	4606	05/17/2022	Trash Removal - CWRF	494.59
EJH01 - E.J. HARRISON & SONS INC	850	05/17/2022	Trash Removal - CWRF	387.34
EJH01 - E.J. HARRISON & SONS INC	864	06/10/2022	Trash Removal - Acct#5-0080466-9	516.94
EJH01 - E.J. HARRISON & SONS INC	9975	06/27/2022	Trash Removal - CWRF	494.59

3151.34**ENH01 - Enhanced Landscape Development, Inc****Paid To Same Vendor**

ENH01 - Enhanced Landscape Development, Inc	80970	04/11/2022	Landscaping	1627
ENH01 - Enhanced Landscape Development, Inc	81130	04/11/2022	Landscaping - Irrigation Repair	70
ENH01 - Enhanced Landscape Development, Inc	83332	05/03/2022	Landscaping	1627
ENH01 - Enhanced Landscape Development, Inc	83636	05/03/2022	Landscaping - Irrigation Repair	145
ENH01 - Enhanced Landscape Development, Inc	85288	06/10/2022	Landscaping	1627
ENH01 - Enhanced Landscape Development, Inc	85400	06/10/2022	Landscaping - Irrigation Repair	154.25
				<hr/> 5250.25

ENT01 - ENTERPRISE FLEET SERV INC**Paid To Same Vendor**

ENT01 - ENTERPRISE FLEET SERV INC	FBN4442476	05/03/2022	Vehicle Lease for April	6917.01
ENT01 - ENTERPRISE FLEET SERV INC	FBN446892	05/18/2022	Vehicle Lease May 2022	7317.01
ENT01 - ENTERPRISE FLEET SERV INC	FBN4492997	06/27/2022	Vehicle Lease June 2022	6917.01
				<hr/> 21151.03

ENV01 - ENVIRONMENTAL RESOURCE ASSOCIATES**Paid To Same Vendor**

ENV01 - ENVIRONMENTAL RESOURCE ASSOCIATES	005733	04/25/2022	Performance Evaluation Sample	<hr/> 220.26
---	--------	------------	-------------------------------	--------------

FAM01 - FAMCON PIPE & SUPPLY, INC**Paid To Same Vendor**

FAM01 - FAMCON PIPE & SUPPLY, INC	S100076628-001	04/12/2022	Repair Parts - Leaking Air Vac	611.33
FAM01 - FAMCON PIPE & SUPPLY, INC	S100075579-001	04/13/2022	24" Main Line Break Santa Rosa -Parts	6258.04
FAM01 - FAMCON PIPE & SUPPLY, INC	S100075610-001	04/13/2022	24" Main Line Break Santa Rosa -Parts	276.71
FAM01 - FAMCON PIPE & SUPPLY, INC	S100076881-001	05/03/2022	Valve for Penny Well	3037.32
FAM01 - FAMCON PIPE & SUPPLY, INC	S100077123-001	05/03/2022	1.5 Leak Repair WO#15937415 Village 7	579.15
FAM01 - FAMCON PIPE & SUPPLY, INC	S100077127-001	05/03/2022	Leak Repair - Parts	1544.4
FAM01 - FAMCON PIPE & SUPPLY, INC	S100077305-001	05/03/2022	Valve Boxes - Valve Replacement CIP	1480.05
FAM01 - FAMCON PIPE & SUPPLY, INC	S100077458-001	05/03/2022	Piping Penny Well	1091.81
FAM01 - FAMCON PIPE & SUPPLY, INC	S100078386-002	05/17/2022	SL1 MCC Electrical Box	804.38
FAM01 - FAMCON PIPE & SUPPLY, INC	S100079680-001	05/27/2022	Leak Repair - 2" Blow off Morpark Rd-WO#16063982	827.01
FAM01 - FAMCON PIPE & SUPPLY, INC	S100079802-001	05/27/2022	Leak Repair - 2" Blow off Morpark Rd-WO#16063982	622.05
FAM01 - FAMCON PIPE & SUPPLY, INC	S100079744-001	06/01/2022	Leak Repair - Parts 2" Blow Off	1668.38
FAM01 - FAMCON PIPE & SUPPLY, INC	S100079424-001	06/15/2022	Repair Parts - CSUCI Meter	1164.74
FAM01 - FAMCON PIPE & SUPPLY, INC	S100079987-001	06/15/2022	Leak Repair - Parts	1437.15
FAM01 - FAMCON PIPE & SUPPLY, INC	S100081478-001	06/27/2022	Repair Parts - Break Away Bolt Kits	418.28
FAM01 - FAMCON PIPE & SUPPLY, INC	S100081727-001	06/27/2022	Leak Repair Villa 26-118 WO#16205469	127.63
FAM01 - FAMCON PIPE & SUPPLY, INC	S100079092-001	06/28/2022	Angle Meter Stops - Repair Parts	2104.25
FAM01 - FAMCON PIPE & SUPPLY, INC	S100081374-001	06/28/2022	Meter Station 5 & 7 - Parts	1901.01
FAM01 - FAMCON PIPE & SUPPLY, INC	S100081612-001	06/28/2022	Hit fire Hydrant	2342.34
				<hr/> 28296.03

FED01 - FEDERAL EXPRESS CORP**Paid To Same Vendor**

FED01 - FEDERAL EXPRESS CORP	7-72-51128	05/26/2022	Send Semi-Annual Groundwtr Reports FCGMA	<hr/> 62.02
------------------------------	------------	------------	--	-------------

FER03 - FERGUSON WATERWORKS #1083**Paid To Same Vendor**

FER03 - FERGUSON WATERWORKS #1083	0792892	04/13/2022	Valve At RMWTP - Concentrate Piping	2310.22
FER03 - FERGUSON WATERWORKS #1083	0794897	04/13/2022	24" Main Line Break Santa Rosa -Pipe	7586.44
FER03 - FERGUSON WATERWORKS #1083	0791147	05/31/2022	6" Airvac - Replacement	10295.84
FER03 - FERGUSON WATERWORKS #1083	0801277	06/27/2022	Leak Repair Parts - 24" Dresser Couplings	9491.63
				29684.13

FIR05 - FIRST AMERICAN TITLE COMPANY**Paid To Same Vendor**

FIR05 - FIRST AMERICAN TITLE COMPANY	APN-5200-090-075	04/04/2022	Preliminary Title Report - Rocky High Rd	400
--------------------------------------	------------------	------------	--	-----

FRO01 - Frontier Communications**Paid To Same Vendor**

FRO01 - Frontier Communications	April 2022	05/03/2022	VOIP - Land Lines	419.59
FRO01 - Frontier Communications	May 2022	05/31/2022	VOIP - Land Lines	428
FRO01 - Frontier Communications	June 2022	06/28/2022	VOIP - Land Lines June 2022	429.22
				1276.81

FRU01 - FRUIT GROWERS LAB. INC.**Paid To Same Vendor**

FRU01 - FRUIT GROWERS LAB. INC.	203787A	04/07/2022	Outside Lab Analysis	84
FRU01 - FRUIT GROWERS LAB. INC.	203785A	04/12/2022	Outside Lab Work for CWRP	265
FRU01 - FRUIT GROWERS LAB. INC.	204190A	04/12/2022	RMWTP Outside Lab Work	40
FRU01 - FRUIT GROWERS LAB. INC.	204191A	04/12/2022	Outside Lab Work	40
FRU01 - FRUIT GROWERS LAB. INC.	204542A	04/26/2022	Outside Lab Work for RMWTP	40
FRU01 - FRUIT GROWERS LAB. INC.	204544A	04/26/2022	Outside Lab Work	40
FRU01 - FRUIT GROWERS LAB. INC.	205133A	04/26/2022	Outside Lab Work for RMWTP	40
FRU01 - FRUIT GROWERS LAB. INC.	205134A	04/26/2022	Outside Lab Work	40
FRU01 - FRUIT GROWERS LAB. INC.	203786A	04/29/2022	Outside Lab Work for CWRP	150
FRU01 - FRUIT GROWERS LAB. INC.	205392A	04/29/2022	Outside Lab Work for RMWTP	80
FRU01 - FRUIT GROWERS LAB. INC.	205394A	04/29/2022	Outside Lab Work	60
FRU01 - FRUIT GROWERS LAB. INC.	205132A	05/03/2022	Lab Water QC	171
FRU01 - FRUIT GROWERS LAB. INC.	206101A	05/03/2022	Outside Labwork for RMWTP	40
FRU01 - FRUIT GROWERS LAB. INC.	206590A	05/12/2022	Outside Lab Work for RMWTP	40
FRU01 - FRUIT GROWERS LAB. INC.	206786A	05/12/2022	RMWTP Outside Lab Work	80
FRU01 - FRUIT GROWERS LAB. INC.	204604A	05/18/2022	Outside Lab Work for Tierra Rejada Well	291
FRU01 - FRUIT GROWERS LAB. INC.	208008A	06/14/2022	Outside Lab Work for RMWTP	40
FRU01 - FRUIT GROWERS LAB. INC.	208967A	06/15/2022	Outside Lab Work	30
FRU01 - FRUIT GROWERS LAB. INC.	207514A	06/21/2022	Outside Lab Analysis	245
FRU01 - FRUIT GROWERS LAB. INC.	207515A	06/21/2022	Outside Lab Analysis	265
FRU01 - FRUIT GROWERS LAB. INC.	207517A	06/21/2022	Outside Lab Analysis	40
FRU01 - FRUIT GROWERS LAB. INC.	207518A	06/21/2022	Outside Lab Analysis	40
FRU01 - FRUIT GROWERS LAB. INC.	206102A	06/27/2022	Outside Lab Work CWRP	150
FRU01 - FRUIT GROWERS LAB. INC.	206103A	06/27/2022	Outside Labwork	385
FRU01 - FRUIT GROWERS LAB. INC.	208009A	06/27/2022	Outside Lab Analysis	920
FRU01 - FRUIT GROWERS LAB. INC.	208968A	06/27/2022	Outside Lab for RMWTP	75
FRU01 - FRUIT GROWERS LAB. INC.	208505A	06/29/2022	RMWTP Outside Lab Work	40
FRU01 - FRUIT GROWERS LAB. INC.	209752A	06/30/2022	Outside Lab Analysis	107
				3838

GEN06 - GENERAL PUMP COMPANY, INC**Paid To Same Vendor**

GEN06 - GENERAL PUMP COMPANY, INC	29333	05/03/2022	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	43040
GEN06 - GENERAL PUMP COMPANY, INC	29335	05/03/2022	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	63250
GEN06 - GENERAL PUMP COMPANY, INC	29336	05/03/2022	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	43040
GEN06 - GENERAL PUMP COMPANY, INC	29391	05/26/2022	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	39200
GEN06 - GENERAL PUMP COMPANY, INC	29377	05/27/2022	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	5170.15
GEN06 - GENERAL PUMP COMPANY, INC	29378	05/27/2022	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	4957.9
GEN06 - GENERAL PUMP COMPANY, INC	29379	05/27/2022	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	5611.78
GEN06 - GENERAL PUMP COMPANY, INC	29380	05/27/2022	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	5757.14
				210026.97

GMS01 - GMS Landscaping Inc**Paid To Same Vendor**

GMS01 - GMS Landscaping Inc	203161	04/13/2022	Tree and Site Maintenance	6000
GMS01 - GMS Landscaping Inc	203210	05/17/2022	Tree and Site Maintenance	6000
				12000

GOL07 - Golden State Labor Compliance**Paid To Same Vendor**

GOL07 - Golden State Labor Compliance	04-2022-06	04/11/2022	PV Well No. 2 Labor Compliance Services	2314
GOL07 - Golden State Labor Compliance	05-2022-06	05/03/2022	PV Well No. 2 Labor Compliance Services	2313
GOL07 - Golden State Labor Compliance	06-2022-34	05/31/2022	PV Well No. 2 Labor Compliance Services	1504
				6131

HAC01 - HACH COMPANY**Paid To Same Vendor**

HAC01 - HACH COMPANY	12908168	04/11/2022	Materials & Supplies - Reagents 6000	334.27
HAC01 - HACH COMPANY	12909318	04/11/2022	Materials & Supplies - Reagents 5500	38.85
HAC01 - HACH COMPANY	12914115	04/11/2022	Materials & Supplies- Reagents 5500	194.28
HAC01 - HACH COMPANY	12965126	04/11/2022	Materials & Supplies- Reagents 5500	857.66
HAC01 - HACH COMPANY	12849300	04/12/2022	Laboratory Supplies	39.4
HAC01 - HACH COMPANY	12988979	04/29/2022	Materials & Supplies - Reagents CL17	921.56
HAC01 - HACH COMPANY	12996624	04/29/2022	Materials & Supplies - Reagents 6000	659.46
HAC01 - HACH COMPANY	13050383	05/27/2022	Materials & Supplies - APA 6000	603.61
HAC01 - HACH COMPANY	13039131	06/01/2022	Reagents CL17	1515.26
HAC01 - HACH COMPANY	13047533	06/01/2022	Reagents - CL17	1427.99
HAC01 - HACH COMPANY	13050643	06/01/2022	Materials & Supplies - Reagents	1662.84
HAC01 - HACH COMPANY	13061956	06/01/2022	Materials & Supplies - Reagents	967.24
HAC01 - HACH COMPANY	13061966	06/01/2022	Materials & Supplies - Reagents	2319.06
HAC01 - HACH COMPANY	13061967	06/01/2022	Reagents APA 6000	2637.84
HAC01 - HACH COMPANY	13087071	06/27/2022	HACH Sequential Chlorination CIP	9737.48
HAC01 - HACH COMPANY	13101255	06/27/2022	Chemical Reagents- Woodcreek	2972.15
HAC01 - HACH COMPANY	13104688	06/27/2022	HACH Sequential Chlorination CIP	3403
HAC01 - HACH COMPANY	13121243	06/30/2022	Chemicals Reagents	915.31
HAC01 - HACH COMPANY	13121309	06/30/2022	HACH Sequential Chlorination CIP	511.71
				31718.97

HAT01 - THE HATHAWAY LAW FIRM, LLP**Paid To Same Vendor**

HAT01 - THE HATHAWAY LAW FIRM, LLP	200568	04/07/2022	Legal Services PFAS	275.19
HAT01 - THE HATHAWAY LAW FIRM, LLP	200569	04/07/2022	Legal Services	1406.51
HAT01 - THE HATHAWAY LAW FIRM, LLP	200936	05/12/2022	Legal Services	611.56
HAT01 - THE HATHAWAY LAW FIRM, LLP	200937	05/12/2022	Legal Services	3155.92
HAT01 - THE HATHAWAY LAW FIRM, LLP	GSA-200932	05/18/2022	GSA Legal Services	733.83
HAT01 - THE HATHAWAY LAW FIRM, LLP	201165	06/08/2022	Legal Services PFAS	61.15
HAT01 - THE HATHAWAY LAW FIRM, LLP	201166	06/08/2022	Legal Services	2537.84
				8782
HEA02 - HealthEquity				
Paid To Same Vendor				
HEA02 - HealthEquity	INV0011382	04/07/2022	HSA-Employee Contribution	438.46
HEA02 - HealthEquity	INV0011383	04/07/2022	HSA Contributions	200
HEA02 - HealthEquity	INV0011465	04/21/2022	HSA-Employee Contribution	438.46
HEA02 - HealthEquity	INV0011466	04/21/2022	HSA Contributions	200
HEA02 - HealthEquity	fwdvyq5	05/03/2022	Consumer Driven Plan Admon Fees	14.75
HEA02 - HealthEquity	INV0011504	05/05/2022	HSA-Employee Contribution	438.46
HEA02 - HealthEquity	INV0011505	05/05/2022	HSA Contributions	200
HEA02 - HealthEquity	INV0011558	05/19/2022	HSA-Employee Contribution	438.46
HEA02 - HealthEquity	INV0011559	05/19/2022	HSA Contributions	200
HEA02 - HealthEquity	INV0011633	06/02/2022	HSA-Employee Contribution	438.46
HEA02 - HealthEquity	INV0011634	06/02/2022	HSA Contributions	200
HEA02 - HealthEquity	u9wdyur	06/08/2022	Consumer Driven Plan Admn Fees June 2022	8.85
HEA02 - HealthEquity	INV0011747	06/16/2022	HSA-Employee Contribution	438.46
HEA02 - HealthEquity	INV0011748	06/16/2022	HSA Contributions	200
HEA02 - HealthEquity	INV0011810	06/30/2022	HSA-Employee Contribution	438.46
HEA02 - HealthEquity	INV0011811	06/30/2022	HSA Contributions	200
				4492.82
HOP02 - HOPKINS GROUNDWATER CONSULTING				
Paid To Same Vendor				
HOP02 - HOPKINS GROUNDWATER CONSULTING	11892	06/28/2022	Additional Scope task 2 & 3	3170
HOP02 - HOPKINS GROUNDWATER CONSULTING	11892	06/28/2022	Secondary Cleaning - Out of Scope	1310
				4480
HOS01 - HOSE-MAN, INC.				
Paid To Same Vendor				
HOS01 - HOSE-MAN, INC.	5296313-0001-05	06/27/2022	Hose for Non Potable Filling Station	404.83
IDE01 - IDEXX LABORATORIES, INC				
Paid To Same Vendor				
IDE01 - IDEXX LABORATORIES, INC	3105770225	05/04/2022	Laboratory Supplies	2066.22
IDE01 - IDEXX LABORATORIES, INC	3105825065	05/12/2022	Laboratory Supplies	21.82
IDE01 - IDEXX LABORATORIES, INC	3108449588	06/21/2022	Lab Supplies	760.15
				2848.19
INF00 - INFOSEND, INC.				
Paid To Same Vendor				
INF00 - INFOSEND, INC.	211007	04/29/2022	Printing & Mailing March 2022 Statements	4900.68
INF00 - INFOSEND, INC.	212871	05/26/2022	Printing & Mailing May 2022 Statements	4892.47

INF00 - INFOSEND, INC.	214626	06/28/2022	Printing & Mailing June 2022 Statements and Insert	5596.47
				15389.62
INT03 - INTERA INCORPORATED				
Paid To Same Vendor				
INT03 - INTERA INCORPORATED	03-22-54	04/08/2022	Santa Rosa GSP	43198.49
INT03 - INTERA INCORPORATED	04-22-29	06/14/2022	Santa Rosa GSP	38200
				81398.49
JAN01 - Janitek Cleaning Solutions-Allstate Cleaning, Inc.				
Paid To Same Vendor				
JAN01 - Janitek Cleaning Solutions-Allstate Cleaning, Inc.	44209A	04/11/2022	Cleaning Service- Janitorial Services	1772
JAN01 - Janitek Cleaning Solutions-Allstate Cleaning, Inc.	44526A	05/03/2022	Janitorial Cleaning Service	1772
JAN01 - Janitek Cleaning Solutions-Allstate Cleaning, Inc.	44819A	06/10/2022	Cleaning Sevice	1772
				5316
JOH06 - JOHN M. ELLSWORTH CO., INC.				
Paid To Same Vendor				
JOH06 - JOHN M. ELLSWORTH CO., INC.	0873002IN	04/11/2022	Fuel Trailer Qty 2 GT110PA	21923.35
KPP01 - KP PUBLIC AFFAIRS LLC				
Paid To Same Vendor				
KPP01 - KP PUBLIC AFFAIRS LLC	1015	04/14/2022	Solve the Water Crisis PR Campaign	15000
LAS02 - CINDY SALDIVAR				
Paid To Same Vendor				
LAS02 - CINDY SALDIVAR	60821	06/14/2022	Notary Svcs-PS2 CWRF Fuel Tank	30
LIB01 - LIBERTY COMPOSTING, INC				
Paid To Same Vendor				
LIB01 - LIBERTY COMPOSTING, INC	30963	05/17/2022	Sludge Removal	7604.38
LIB01 - LIBERTY COMPOSTING, INC	30997	05/31/2022	Sludge Removal	5972.26
				13576.64
LIF01 - LIFTOFF, LLC				
Paid To Same Vendor				
LIF01 - LIFTOFF, LLC	61322	06/14/2022	O365 G3 and Defender License - Annual Renewals	9102
LIG01 - LightGabler				
Paid To Same Vendor				
LIG01 - LightGabler	65189	06/14/2022	HR Consulting	35
LIN01 - LINDE GAS & EQUIPMENT INC				
Paid To Same Vendor				
LIN01 - LINDE GAS & EQUIPMENT INC	70196470	04/29/2022	Acetylene Gas Cylinders	65.8
LIN01 - LINDE GAS & EQUIPMENT INC	10051931	05/17/2022	Acetylene Gas Cylinders	122.4
LIN01 - LINDE GAS & EQUIPMENT INC	10506698	05/27/2022	Acetylene Gas Cylinders	64.25
LIN01 - LINDE GAS & EQUIPMENT INC	11111617	06/27/2022	Acetylene Gas Cylinders	65.8
				318.25
LNL01 - LINCOLN FINANCIAL GROUP				

Paid To Same Vendor

LNL01 - LINCOLN FINANCIAL GROUP	INV0011379	04/07/2022	Deferred Compensation	2058
LNL01 - LINCOLN FINANCIAL GROUP	INV0011461	04/21/2022	Deferred Compensation	2058
LNL01 - LINCOLN FINANCIAL GROUP	INV0011501	05/05/2022	Deferred Compensation	2058
LNL01 - LINCOLN FINANCIAL GROUP	INV0011554	05/19/2022	Deferred Compensation	2058
LNL01 - LINCOLN FINANCIAL GROUP	INV0011630	06/02/2022	Deferred Compensation	2860.44
LNL01 - LINCOLN FINANCIAL GROUP	INV0011743	06/16/2022	Deferred Compensation	2058
LNL01 - LINCOLN FINANCIAL GROUP	INV0011807	06/30/2022	Deferred Compensation	2058
				15208.44

MCM01 - McMASTER-CARR SUPPLY CO**Paid To Same Vendor**

MCM01 - McMASTER-CARR SUPPLY CO	72593510	04/13/2022	Chemical Day Tank - TR Well	875
MCM01 - McMASTER-CARR SUPPLY CO	76829768	05/03/2022	MS 5&7 Rehab Fittings for Transfers	997.99
MCM01 - McMASTER-CARR SUPPLY CO	76834202	05/03/2022	Materials & Supplies , Uni-Strut Hardware	972.74
MCM01 - McMASTER-CARR SUPPLY CO	76840138	05/03/2022	MS 5 & 7 Rehab Fittings for Transducers	993.63
MCM01 - McMASTER-CARR SUPPLY CO	77958376	05/17/2022	Materials & Supplies - SS Hardware	522.99
MCM01 - McMASTER-CARR SUPPLY CO	79926009	06/27/2022	Materials & Supplies - SS Hardware	625.14
MCM01 - McMASTER-CARR SUPPLY CO	79931276	06/27/2022	Repair Parts - Band Saw	75.46
MCM01 - McMASTER-CARR SUPPLY CO	80224580	06/27/2022	Materials & Supplies - SS Hardware	946.72
MCM01 - McMASTER-CARR SUPPLY CO	80389226	06/27/2022	Materials & Supplies - SS Hardware	523.65
				6533.32

MCR01 - MCR TECHNOLOGIES, INC.**Paid To Same Vendor**

MCR01 - MCR TECHNOLOGIES, INC.	40654	04/29/2022	Production Mag Meter Cals	6431.04
MCR01 - MCR TECHNOLOGIES, INC.	40772	06/15/2022	Santa Rosa 8 Well Production Meter	6391.03
MCR01 - MCR TECHNOLOGIES, INC.	40773	06/15/2022	Conejo Well 2 Production Meter	6391.03
MCR01 - MCR TECHNOLOGIES, INC.	40774	06/15/2022	Conejo Well 4 Production Meter	6391.03
MCR01 - MCR TECHNOLOGIES, INC.	40803	06/28/2022	Conejo Well 3 Production Meter	6766.73
				32370.86

MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.**Paid To Same Vendor**

MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100463	04/08/2022	Preparation of Unidirectional Flushing RFP	697.83
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100464	04/08/2022	Preparation of Tank Diving RFP	1470.58
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100465	04/08/2022	(SPCC) Plan Preparation	7700.44
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100481	04/08/2022	GAC Construction Management	13904.36
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100562	04/08/2022	GAC Project Management	3258.7
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100619	05/17/2022	GAC Construction Management	7968.42
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100620	05/17/2022	Preparation of Unidirectional Flushing RFP	1164.16
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100621	05/17/2022	Preparation of Tank Diving RFP	1627.66
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100622	05/17/2022	(SPCC) Plan Preparation	2327.8
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100756	06/14/2022	GAC Construction Management	22395.26
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100758	06/14/2022	(SPCC) Plan Preparation	822.46
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100757	06/27/2022	CO-01: add City traffic control plans	1230.32
MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.	100757	06/27/2022	Preparation of Unidirectional Flushing RFP	1183.49
				65751.48

MNS01 - MNS ENGINEERS, INC.**Paid To Same Vendor**

MNS01 - MNS ENGINEERS, INC.	80198	04/12/2022	Engineering Support services during construction	175
MNS01 - MNS ENGINEERS, INC.	80486	06/14/2022	Penny Well Entrained Air Engineering Services	3186.25
				3361.25

NOH01 - NOHO CONSTRUCTORS

Paid To Same Vendor

NOH01 - NOHO CONSTRUCTORS	Pymt#3-Project PW21-02	04/12/2022	Reservoir 1B communication facility	120000
NOH01 - NOHO CONSTRUCTORS	Retention-Payment#3	04/12/2022	Retention Payment 3-pROJECT pw21-02	-6000
NOH01 - NOHO CONSTRUCTORS	Pymt#6-Projec 20-06	04/13/2022	Additional Fuel Tank Fittings	2360
NOH01 - NOHO CONSTRUCTORS	Pymt#6-Projec 20-06	04/13/2022	Change Order 4	2643.5
NOH01 - NOHO CONSTRUCTORS	Pymt#6-Projec 20-06	04/13/2022	CWRF - Diesel Fuel Tank Installation	19996.5
NOH01 - NOHO CONSTRUCTORS	Retention Pymt#6	04/13/2022	Retention Pymt#6-Project PS 20-06	-1250
NOH01 - NOHO CONSTRUCTORS	CM0000371	06/14/2022	Pump Station 2 - Generator Installation	0
NOH01 - NOHO CONSTRUCTORS	CM0000371-R	06/14/2022	Pump Station 2 - Generator Installation	0
NOH01 - NOHO CONSTRUCTORS	Pymt 4-PW21-02	06/14/2022	Reservoir 1B communication facility	87103
NOH01 - NOHO CONSTRUCTORS	Retention-Pymt 4-PW21-02	06/14/2022	Retention on Payment 4- Project 21-02	-4355.15
NOH01 - NOHO CONSTRUCTORS	Paymt 7-Project-PS 20-06	06/29/2022	Pump Station 2 - Generator Installation	37333.37
NOH01 - NOHO CONSTRUCTORS	Pymt 7- Project 20-06	06/29/2022	Change Order 4	1140.56
NOH01 - NOHO CONSTRUCTORS	Pymt 7- Project 20-06	06/29/2022	CO #1 - Additional Conduits	2667.13
NOH01 - NOHO CONSTRUCTORS	Pymt 7- Project 20-06	06/29/2022	Fuel Tank Anchor Bolt Pull Test	644
NOH01 - NOHO CONSTRUCTORS	Retention-Pymt7	06/29/2022	Retention Pymt7 Project PS20-06	-2089.25
				260193.66

NOR07 - NORTHSTAR CHEMICAL

Paid To Same Vendor

NOR07 - NORTHSTAR CHEMICAL	219939	04/11/2022	Materials Chemicals - Woodcreek Well	2494.89
NOR07 - NORTHSTAR CHEMICAL	220135	04/11/2022	Materials Chemicals - RMWTP	1969.65
NOR07 - NORTHSTAR CHEMICAL	220136	04/11/2022	Materials Chemicals - CWRF	4595.85
NOR07 - NORTHSTAR CHEMICAL	217466	04/25/2022	Materials Chemicals - CWRF	250
NOR07 - NORTHSTAR CHEMICAL	222003	04/29/2022	Materials Chemicals	1004.58
NOR07 - NORTHSTAR CHEMICAL	222004	04/29/2022	Materials Chemicals RMWTP	2462.07
NOR07 - NORTHSTAR CHEMICAL	222443	05/03/2022	Materials Chemicals CWRF - Tank Rental Pick up	500
NOR07 - NORTHSTAR CHEMICAL	222325	05/17/2022	Materials Chemicals -Woodcreek Well	2516.78
NOR07 - NORTHSTAR CHEMICAL	223612	05/26/2022	Materials Chemicals-RMWTP	5402.72
NOR07 - NORTHSTAR CHEMICAL	223613	05/26/2022	Materials Chemicals - CWRF	1707.03
NOR07 - NORTHSTAR CHEMICAL	225317	06/10/2022	Materials & Supplies - Chemicals RMWTP	2048.44
NOR07 - NORTHSTAR CHEMICAL	225318	06/10/2022	Materials & Supplies - Chemicals Woodcreek	2488.33
NOR07 - NORTHSTAR CHEMICAL	225319	06/10/2022	Materials & Supplies - Chemicals Tierra Rejada	1034.22
NOR07 - NORTHSTAR CHEMICAL	227280	06/30/2022	Materials and Supplies - Chemicals RMWTP	2341.7
				30816.26

OLI01 - OLIN CORP-CHLOR ALKALI

Paid To Same Vendor

OLI01 - OLIN CORP-CHLOR ALKALI	3000115968	06/10/2022	Materials & Supplies - Chemicals CWRF	7193.93
--------------------------------	------------	------------	---------------------------------------	---------

OPE01 - OPEN TEXT INC.

Paid To Same Vendor

OPE01 - OPEN TEXT INC.	9003141124	05/27/2022	Alchemy Annual Support Renewal	3110.2
------------------------	------------	------------	--------------------------------	--------

PAP01 - PAPE MATERIAL HANDLING, INC

Paid To Same Vendor

PAP01 - PAPE MATERIAL HANDLING, INC	6441504	04/29/2022	Vehicle Maintenance- Forklift	182.17
PAT02 - CHRISTOPHER PATACSIL				
Paid To Same Vendor				
PAT02 - CHRISTOPHER PATACSIL	TuitionReimb-Spring2022	06/08/2022	Spring 2022 Tuition Reimbursement	609.99
PER01 - PUBLIC EMPLOYEES				
Paid To Same Vendor				
PER01 - PUBLIC EMPLOYEES	INV0011380	04/07/2022	PERS-Classic Employee Portion	343.65
PER01 - PUBLIC EMPLOYEES	INV0011381	04/07/2022	PERS-Classic Employer Portion	507.6
PER01 - PUBLIC EMPLOYEES	INV0011384	04/07/2022	PERS-Classic Employee Portion	4909.18
PER01 - PUBLIC EMPLOYEES	INV0011385	04/07/2022	PERS Survivors	22.32
PER01 - PUBLIC EMPLOYEES	INV0011386	04/07/2022	Employee-PERS Classic	818.22
PER01 - PUBLIC EMPLOYEES	INV0011387	04/07/2022	PERS-Classic Employer Portion	8730.22
PER01 - PUBLIC EMPLOYEES	INV0011388	04/07/2022	Employee-PERS Classic	182.82
PER01 - PUBLIC EMPLOYEES	INV0011389	04/07/2022	Employer-PERS New	840.6
PER01 - PUBLIC EMPLOYEES	INV0011390	04/07/2022	Employee-PERS New	747.58
PER01 - PUBLIC EMPLOYEES	INV0011414	04/12/2022	PERS-Classic Employee Portion	6.72
PER01 - PUBLIC EMPLOYEES	INV0011415	04/12/2022	PERS-Classic Employer Portion	9.93
PER01 - PUBLIC EMPLOYEES	INV0011416	04/12/2022	PERS-Classic Employee Portion	96.06
PER01 - PUBLIC EMPLOYEES	INV0011417	04/12/2022	PERS Survivors	0.93
PER01 - PUBLIC EMPLOYEES	INV0011418	04/12/2022	Employee-PERS Classic	16.01
PER01 - PUBLIC EMPLOYEES	INV0011419	04/12/2022	PERS-Classic Employer Portion	165.55
PER01 - PUBLIC EMPLOYEES	INV0011463	04/21/2022	PERS-Classic Employee Portion	333.99
PER01 - PUBLIC EMPLOYEES	INV0011464	04/21/2022	PERS-Classic Employer Portion	493.34
PER01 - PUBLIC EMPLOYEES	INV0011472	04/21/2022	PERS-Classic Employee Portion	4771.25
PER01 - PUBLIC EMPLOYEES	INV0011473	04/21/2022	PERS Survivors	21.39
PER01 - PUBLIC EMPLOYEES	INV0011474	04/21/2022	Employee-PERS Classic	795.23
PER01 - PUBLIC EMPLOYEES	INV0011475	04/21/2022	PERS-Classic Employer Portion	8492.51
PER01 - PUBLIC EMPLOYEES	INV0011476	04/21/2022	Employee-PERS Classic	182.82
PER01 - PUBLIC EMPLOYEES	INV0011477	04/21/2022	Employer-PERS New	840.6
PER01 - PUBLIC EMPLOYEES	INV0011478	04/21/2022	Employee-PERS New	747.58
PER01 - PUBLIC EMPLOYEES	INV0011502	05/05/2022	PERS-Classic Employee Portion	333.99
PER01 - PUBLIC EMPLOYEES	INV0011503	05/05/2022	PERS-Classic Employer Portion	493.34
PER01 - PUBLIC EMPLOYEES	INV0011506	05/05/2022	PERS-Classic Employee Portion	4771.25
PER01 - PUBLIC EMPLOYEES	INV0011507	05/05/2022	PERS Survivors	21.39
PER01 - PUBLIC EMPLOYEES	INV0011508	05/05/2022	Employee-PERS Classic	795.23
PER01 - PUBLIC EMPLOYEES	INV0011509	05/05/2022	PERS-Classic Employer Portion	8492.51
PER01 - PUBLIC EMPLOYEES	INV0011510	05/05/2022	Employee-PERS Classic	182.82
PER01 - PUBLIC EMPLOYEES	INV0011511	05/05/2022	Employer-PERS New	840.6
PER01 - PUBLIC EMPLOYEES	INV0011512	05/05/2022	Employee-PERS New	747.58
PER01 - PUBLIC EMPLOYEES	INV0011556	05/19/2022	PERS-Classic Employee Portion	333.99
PER01 - PUBLIC EMPLOYEES	INV0011557	05/19/2022	PERS-Classic Employer Portion	493.34
PER01 - PUBLIC EMPLOYEES	INV0011565	05/19/2022	PERS-Classic Employee Portion	4771.25
PER01 - PUBLIC EMPLOYEES	INV0011566	05/19/2022	PERS Survivors	21.39
PER01 - PUBLIC EMPLOYEES	INV0011567	05/19/2022	Employee-PERS Classic	795.23
PER01 - PUBLIC EMPLOYEES	INV0011568	05/19/2022	PERS-Classic Employer Portion	8492.51
PER01 - PUBLIC EMPLOYEES	INV0011569	05/19/2022	Employee-PERS Classic	182.82
PER01 - PUBLIC EMPLOYEES	INV0011570	05/19/2022	Employer-PERS New	840.6
PER01 - PUBLIC EMPLOYEES	INV0011571	05/19/2022	Employee-PERS New	747.58

PER01 - PUBLIC EMPLOYEES	INV0011631	06/02/2022	PERS-Classic Employee Portion	333.99
PER01 - PUBLIC EMPLOYEES	INV0011632	06/02/2022	PERS-Classic Employer Portion	493.34
PER01 - PUBLIC EMPLOYEES	INV0011635	06/02/2022	PERS-Classic Employee Portion	4771.25
PER01 - PUBLIC EMPLOYEES	INV0011636	06/02/2022	PERS Survivors	21.39
PER01 - PUBLIC EMPLOYEES	INV0011637	06/02/2022	Employee-PERS Classic	795.23
PER01 - PUBLIC EMPLOYEES	INV0011638	06/02/2022	PERS-Classic Employer Portion	8492.51
PER01 - PUBLIC EMPLOYEES	INV0011639	06/02/2022	Employee-PERS Classic	182.82
PER01 - PUBLIC EMPLOYEES	INV0011640	06/02/2022	Employer-PERS New	840.6
PER01 - PUBLIC EMPLOYEES	INV0011641	06/02/2022	Employee-PERS New	747.58
PER01 - PUBLIC EMPLOYEES	INV0011745	06/16/2022	PERS-Classic Employee Portion	333.99
PER01 - PUBLIC EMPLOYEES	INV0011746	06/16/2022	PERS-Classic Employer Portion	493.34
PER01 - PUBLIC EMPLOYEES	INV0011754	06/16/2022	PERS-Classic Employee Portion	4771.25
PER01 - PUBLIC EMPLOYEES	INV0011755	06/16/2022	PERS Survivors	21.39
PER01 - PUBLIC EMPLOYEES	INV0011756	06/16/2022	Employee-PERS Classic	795.23
PER01 - PUBLIC EMPLOYEES	INV0011757	06/16/2022	PERS-Classic Employer Portion	8492.51
PER01 - PUBLIC EMPLOYEES	INV0011758	06/16/2022	Employee-PERS Classic	182.82
PER01 - PUBLIC EMPLOYEES	INV0011759	06/16/2022	Employer-PERS New	840.6
PER01 - PUBLIC EMPLOYEES	INV0011760	06/16/2022	Employee-PERS New	747.58
PER01 - PUBLIC EMPLOYEES	INV0011823	06/27/2022	PERS-Classic Employee Portion	5.38
PER01 - PUBLIC EMPLOYEES	INV0011824	06/27/2022	PERS-Classic Employer Portion	7.95
PER01 - PUBLIC EMPLOYEES	INV0011825	06/27/2022	PERS-Classic Employee Portion	76.8
PER01 - PUBLIC EMPLOYEES	INV0011826	06/27/2022	Employee-PERS Classic	12.8
PER01 - PUBLIC EMPLOYEES	INV0011827	06/27/2022	PERS-Classic Employer Portion	132.35
PER01 - PUBLIC EMPLOYEES	INV0011808	06/30/2022	PERS-Classic Employee Portion	328.61
PER01 - PUBLIC EMPLOYEES	INV0011809	06/30/2022	PERS-Classic Employer Portion	485.39
PER01 - PUBLIC EMPLOYEES	INV0011812	06/30/2022	PERS-Classic Employee Portion	4694.45
PER01 - PUBLIC EMPLOYEES	INV0011813	06/30/2022	PERS Survivors	21.39
PER01 - PUBLIC EMPLOYEES	INV0011814	06/30/2022	Employee-PERS Classic	782.43
PER01 - PUBLIC EMPLOYEES	INV0011815	06/30/2022	PERS-Classic Employer Portion	8360.16
PER01 - PUBLIC EMPLOYEES	INV0011816	06/30/2022	Employee-PERS Classic	182.82
PER01 - PUBLIC EMPLOYEES	INV0011817	06/30/2022	Employer-PERS New	840.6
PER01 - PUBLIC EMPLOYEES	INV0011818	06/30/2022	Employee-PERS New	747.58
				<hr/>
				117469.65

PER02 - PERLITER & INGALSBE

Paid To Same Vendor

PER02 - PERLITER & INGALSBE	18683	04/11/2022	Additional Eng. Support Services	9404.5
PER02 - PERLITER & INGALSBE	18692	05/17/2022	Development Construction Cost Fee - ENR Cost Index	932.75
PER02 - PERLITER & INGALSBE	18693	05/17/2022	Additional Eng. Support Services	14484.5
PER02 - PERLITER & INGALSBE	18701	06/14/2022	Additional Eng. Support Services	4176.75
				<hr/>
				28998.5

PER05 - CAL PERS 457 PLAN

Paid To Same Vendor

PER05 - CAL PERS 457 PLAN	INV0011378	04/07/2022	Deferred Compensation	3704.46
PER05 - CAL PERS 457 PLAN	INV0011413	04/12/2022	Deferred Compensation	100
PER05 - CAL PERS 457 PLAN	INV0011460	04/21/2022	Deferred Compensation	3604.46
PER05 - CAL PERS 457 PLAN	INV0011500	05/05/2022	Deferred Compensation	3604.46
PER05 - CAL PERS 457 PLAN	INV0011553	05/19/2022	Deferred Compensation	3366.46
PER05 - CAL PERS 457 PLAN	INV0011629	06/02/2022	Deferred Compensation	3366.46

PER05 - CAL PERS 457 PLAN	INV0011742	06/16/2022	Deferred Compensation	3366.46
PER05 - CAL PERS 457 PLAN	INV0011806	06/30/2022	Deferred Compensation	3366.46
				24479.22
PRO05 - PROVOST & PRITCHARD CONSULTING GROUP				
Paid To Same Vendor				
PRO05 - PROVOST & PRITCHARD CONSULTING GROUP	91538	05/17/2022	GAC CEQA	3760
PRO05 - PROVOST & PRITCHARD CONSULTING GROUP	91538-2	05/17/2022	GAC Engineering	2700
PRO05 - PROVOST & PRITCHARD CONSULTING GROUP	92491	06/14/2022	GAC Engineering	2700
PRO05 - PROVOST & PRITCHARD CONSULTING GROUP	92992	06/29/2022	GAC Engineering	2700
				11860
PUR01 - PURETEC INDUSTRIAL WATER				
Paid To Same Vendor				
PUR01 - PURETEC INDUSTRIAL WATER	1969261	04/11/2022	Deionized Water Service	75.12
PUR01 - PURETEC INDUSTRIAL WATER	1970911	04/29/2022	Chemicals RMWTP	21431.61
PUR01 - PURETEC INDUSTRIAL WATER	1977962	05/17/2022	Deionized Water Service	72.44
PUR01 - PURETEC INDUSTRIAL WATER	1977963	05/17/2022	Deionized Water Service	72.44
PUR01 - PURETEC INDUSTRIAL WATER	1980883	06/27/2022	Chemicals RMWTP	13095.69
PUR01 - PURETEC INDUSTRIAL WATER	1982870	06/27/2022	Chemicals RMWTP	12307.58
PUR01 - PURETEC INDUSTRIAL WATER	1988854	06/27/2022	Chemicals RMWTP	13029.15
				60084.03
QUA02 - QUADIENT LEASING USA, INC.				
Paid To Same Vendor				
QUA02 - QUADIENT LEASING USA, INC.	N9445486	06/15/2022	Postal Meter Equipment Rental 7-10-22 th 10-0-22	371.45
QUA03 - LANDMARK GRADING & PAVING, INC				
Paid To Same Vendor				
QUA03 - LANDMARK GRADING & PAVING, INC	2022-03378	05/03/2022	24" Main Line Break Santa Rosa - Road Repair	38716.82
QUI02 - QUINN COMPANY				
Paid To Same Vendor				
QUI02 - QUINN COMPANY	WON10017599	05/03/2022	Generator Maintenance 52	1873.62
RAI02 - RAIDER PAINTING COMPANY				
Paid To Same Vendor				
RAI02 - RAIDER PAINTING COMPANY	22-9577	05/27/2022	Pipe Repair and Painting MS11	15950
RFS01 - LINCOLN FINANCIAL GROUP				
Paid To Same Vendor				
RFS01 - LINCOLN FINANCIAL GROUP	INV0011391	04/07/2022	Profit Share Contribution	2618.42
RFS01 - LINCOLN FINANCIAL GROUP	INV0011479	04/21/2022	Profit Share Contribution	2618.42
RFS01 - LINCOLN FINANCIAL GROUP	INV0011513	05/05/2022	Profit Share Contribution	2618.42
RFS01 - LINCOLN FINANCIAL GROUP	INV0011572	05/19/2022	Profit Share Contribution	2618.42
RFS01 - LINCOLN FINANCIAL GROUP	INV0011642	06/02/2022	Profit Share Contribution	2618.42
RFS01 - LINCOLN FINANCIAL GROUP	INV0011761	06/16/2022	Profit Share Contribution	2618.42
RFS01 - LINCOLN FINANCIAL GROUP	INV0011819	06/30/2022	Profit Share Contribution	2618.42
				18328.94
RON01 - RON'S PORTABLE WELDING				

Paid To Same Vendor

RON01 - RON'S PORTABLE WELDING	6859	06/30/2022	Materials & Supplies - Pipe Back	1000
RON01 - RON'S PORTABLE WELDING	6860	06/30/2022	Repair Parts - Bumper Mods for Hitch	375
RON01 - RON'S PORTABLE WELDING	6861	06/30/2022	Materials & Supplies - Pipe Rack	375
RON01 - RON'S PORTABLE WELDING	6869	06/30/2022	Materials & Supplies - Pipe Rack	625
				<hr/>
				2375

ROY03 - ROYAL INDUSTRIAL SOLUTIONS**Paid To Same Vendor**

ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1017764	04/12/2022	CWRF Effluent PS VFD 3	8648.41
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1017765	04/12/2022	CWRF Effluent PS VFD 1	8648.41
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1017766	04/12/2022	CWRF Effluent PS VFD 2	8648.41
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1018105	04/12/2022	Replacement VFD PS4 Booster 3	16510.77
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1018106	04/12/2022	Woodcreek VFD Repair	613.12
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1018209	04/12/2022	Repair Parts - Fans	403.65
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1018390	04/12/2022	Reservoir 1B Comm Facility Conduit	254.61
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019158	04/12/2022	Materials and Supplies	483.86
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1016751	04/13/2022	Reservoir 1B Comm Facility Conduit	1373.57
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1016939	04/13/2022	Reservoir 1B Comm Facility Comm	-831.62
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1018478	04/13/2022	Replacement VFD's RMWTP Skids 1&2	1616.67
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019187	04/13/2022	Replacement VFD PS4 Booster 3	351.96
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019027	05/03/2022	Repair Parts - TR Well	972.5
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019137	05/03/2022	Repair Parts - TR Well	155.51
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019182	05/03/2022	Repair Parts - TR Well	423.15
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019242	05/03/2022	Repair Parts - TR Well	203.76
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019271	05/03/2022	Repair Parts - PS 2TO3	826.21
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019307	05/03/2022	Repair Parts - CRWF Effluent VFDs	250.95
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019308	05/03/2022	Repair Parts - CWRF Effluent VFDs	250.95
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019309	05/03/2022	Repair Parts - CWRF Effluent VFDs	250.95
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019875	05/03/2022	Repair Parts - TR Well	490.09
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019987	05/03/2022	Reservoir 1B Comm Facility Conduit	179.05
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020063	05/03/2022	Reservoir 1B Comm Facility Conduit	258.8
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020133	05/03/2022	Reservoir 1B Comm Facility	526.7
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020175	05/03/2022	Reservoir 1B Comm Facility Wire	401.71
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020309	05/03/2022	Rockwell Techconnect Support	12597
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019186	05/17/2022	Woodcreek VFD Repair	22782.13
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019272	05/17/2022	Pump Station 2 to 3 - HOA Switches	978.61
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020401	05/17/2022	Pump Station 2 to 3 SCADA Parts	874.09
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020478	05/17/2022	Materials & Supplies - TyRaps	863.47
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020503	05/17/2022	SL1 Terminals	610.79
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020579	05/27/2022	SL1 Terminals	371.17
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1020989	05/27/2022	Reservoir 1B Comm Facility	990.49
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1021215	05/27/2022	Material & Supplies - Lighting for Conez Boxes	247.29
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1021438	06/14/2022	Read Rd MCC	999.38
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1021495	06/14/2022	Read Rd MCC	492.48
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1021531	06/14/2022	Read Rd MCC	117.65
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1017223	06/27/2022	Read Road MCC	262.24
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019944	06/27/2022	Repair Parts - VFD#3	369.67
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1019945	06/27/2022	Repair Parts - VFD#2	369.67
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1021833	06/27/2022	Read Rodad MCC	747.63

ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1022185	06/27/2022	4B Radio Tower	999.27
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1022259	06/27/2022	4B Radio Tower	417.68
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1022581	06/27/2022	4B Radio Towe	903.53
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1017697	06/28/2022	Repair Parts - Power Supplies	765.81
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1022200	06/28/2022	Repair Parts - Power Supplies	510.54
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1022201	06/28/2022	Repair Parts - Power Supplies	765.81
ROY03 - ROYAL INDUSTRIAL SOLUTIONS	9009-1022202	06/28/2022	Repair Parts - Power Supplies	510.54
				100459.09
RPB01 - RP Barricade, Inc				
Paid To Same Vendor				
RPB01 - RP Barricade, Inc	60998	04/13/2022	Raise Valve Stackings - Traffic Control	1068.22
RPB01 - RP Barricade, Inc	61415	06/27/2022	Engineered TCP Cal Trans Permit-WO#15513094	700
				1768.22
RTL01 - RT LAWRENCE CORPORATION				
Paid To Same Vendor				
RTL01 - RT LAWRENCE CORPORATION	47119	04/29/2022	Processing March 2022 Payments-Lockbox Services	881.88
RTL01 - RT LAWRENCE CORPORATION	47208	05/18/2022	Processing April 2022 Payments-Lockbox Service	753.05
RTL01 - RT LAWRENCE CORPORATION	47298	06/28/2022	Processing June 2022 Payments-Lockbox Servcs	741.52
				2376.45
SAM01 - SAM HILL & SONS, INC.				
Paid To Same Vendor				
SAM01 - SAM HILL & SONS, INC.	4011	04/13/2022	Leak Repair 1" Service	7741.62
SAM01 - SAM HILL & SONS, INC.	4092	04/13/2022	1A Tank Cleaning	11700
SAM01 - SAM HILL & SONS, INC.	4099	04/13/2022	Leak Repair 1" Service	10698.11
SAM01 - SAM HILL & SONS, INC.	4101	04/13/2022	24" Main Line Break Santa Rosa -Repair	51042.29
SAM01 - SAM HILL & SONS, INC.	4116	04/13/2022	Site Clean UP - Road work 1A Tank	6405
SAM01 - SAM HILL & SONS, INC.	4135	05/17/2022	Leak Repair - 1.5" Service	8415.06
SAM01 - SAM HILL & SONS, INC.	4157	06/01/2022	Leak Repair - 14" Effluent Line	3620.58
SAM01 - SAM HILL & SONS, INC.	4171	06/15/2022	Yard Clean Up - Rubble Pile	6960
SAM01 - SAM HILL & SONS, INC.	4172	06/15/2022	Leak Repair - 1" Service Line	5521.14
SAM01 - SAM HILL & SONS, INC.	4173	06/15/2022	Leak Repair - 2" Blow Off	15892.25
				127996.05
SAN04 - Santa Paula Materials, Inc.				
Paid To Same Vendor				
SAN04 - Santa Paula Materials, Inc.	19356	05/04/2022	Materials & Supplies	997.3
SAN04 - Santa Paula Materials, Inc.	19477	05/31/2022	Materials & Supplies - Base for Yard	481.81
SAN04 - Santa Paula Materials, Inc.	19426	06/01/2022	Material and Supplies	1231.41
				2710.52
SCE01 - SOUTHERN CALIF. EDISON				
Paid To Same Vendor				
SCE01 - SOUTHERN CALIF. EDISON	April2022-Resrv B	04/13/2022	Charges Reservoir B-from 8-17-21 th 2-15-22	218.5
SCE01 - SOUTHERN CALIF. EDISON	April2022-B	05/04/2022	Monthly Usage Charges April 2022	144578.3
SCE01 - SOUTHERN CALIF. EDISON	May 2022	05/18/2022	Monthly Usage Charges May 2022	219348.22
SCE01 - SOUTHERN CALIF. EDISON	June2022	06/14/2022	Current Usage Charges-June 2022	154871.47
				519016.49

SCF01 - SC Fuels**Paid To Same Vendor**

SCF01 - SC Fuels	2096937IN	04/11/2022	Material & Supplies - Fuel	1942.24
SCF01 - SC Fuels	2102137IN	04/11/2022	Material & Supplies - Fuel	1628.78
SCF01 - SC Fuels	2106345IN	04/25/2022	Material & Supplies - Fuel	2114.08
SCF01 - SC Fuels	2116564IN	04/29/2022	Material & Supplies - Fuel	1611.32
SCF01 - SC Fuels	2106294IN	05/17/2022	Material & Supplies - Fuel	1607.69
SCF01 - SC Fuels	2107166IN	05/17/2022	Material & Supplies - Fuel - Pond 1 Pump	1272
SCF01 - SC Fuels	2119876IN	05/17/2022	Material & Supplies - Fuel	1696.44
SCF01 - SC Fuels	2126062IN	05/17/2022	Material & Supplies - Fuel - Pond 1 Pump	782.15
SCF01 - SC Fuels	2126287IN	05/17/2022	Material & Supplies - Fuel	1997.27
SCF01 - SC Fuels	2131431IN	05/26/2022	Material & Supplies - Fuel	1412.99
SCF01 - SC Fuels	2136620IN	05/27/2022	Material & Supplies -Fuel	2424.07
SCF01 - SC Fuels	2141189IN	06/10/2022	Materials & Supplies - Fuel	2183.27
SCF01 - SC Fuels	2147230IN	06/10/2022	Materials & Supplies - Fuel	1762.4
SCF01 - SC Fuels	2152720IN	06/27/2022	Materials & Supplies -Fuel Seminary Lift Station	7081
SCF01 - SC Fuels	2153034IN	06/27/2022	Material & Supplies -Fuel	1983.63
				31499.33

SCG01 - SOUTHERN CALIFORNIA GAS**Paid To Same Vendor**

SCG01 - SOUTHERN CALIFORNIA GAS	March 2022	04/08/2022	Usage Charges Account 123 787 1794 1	14.3
SCG01 - SOUTHERN CALIFORNIA GAS	March 2022-A	04/08/2022	Usage Charges Account 170 013 9900 9	138.74
SCG01 - SOUTHERN CALIFORNIA GAS	April 2022	05/12/2022	Monthly Usage Charges Acct 123 787 1794 1	14.3
SCG01 - SOUTHERN CALIFORNIA GAS	April 2022-A	05/12/2022	Monthly Usage Charges Acct 170 013 9900 9	10.56
SCG01 - SOUTHERN CALIFORNIA GAS	May 2022	06/08/2022	Usage Charges - May 2022 Act# 170-013-9900-9	28.76
SCG01 - SOUTHERN CALIFORNIA GAS	May2022-A	06/08/2022	Usage Charges - May 2022 Act# 123-787-1794-1	14.3
SCG01 - SOUTHERN CALIFORNIA GAS	June2022	06/30/2022	June 2022 Usage Charges - Act 17001399009	6.64
SCG01 - SOUTHERN CALIFORNIA GAS	June2022-A	06/30/2022	June 2022 Usage Charges- Acct #12378717941	15.78
				243.38

SEC03 - SYMETRA LIFE INS CO.**Paid To Same Vendor**

SEC03 - SYMETRA LIFE INS CO.	INV0011467	04/21/2022	Life Insurance	270.25
SEC03 - SYMETRA LIFE INS CO.	INV0011560	05/19/2022	Life Insurance	270.25
SEC03 - SYMETRA LIFE INS CO.	INV0011749	06/16/2022	Life Insurance	270.25
				810.75

SMA05 - HADRONEX INC.**Paid To Same Vendor**

SMA05 - HADRONEX INC.	22294	06/30/2022	Smart Covers - Field Repai	135
-----------------------	-------	------------	----------------------------	-----

SPA01 - SPARKLETTS**Paid To Same Vendor**

SPA01 - SPARKLETTS	4667386-041722	04/29/2022	Distilled Bottled Water	74.4
SPA01 - SPARKLETTS	4667386-051522	05/18/2022	Distilled Bottled Water	87.39
SPA01 - SPARKLETTS	4667386-061222	06/15/2022	Distilled Bottled Water	35.93
				197.72

STA05 - STATE WATER RESOURCES CONTROL BOARD

Paid To Same Vendor				
STA05 - STATE WATER RESOURCES CONTROL BOARD	D2Cert-BrainBoring	04/25/2022	Grade 2 Distribution Certificate-Brian Boring	80
STA05 - STATE WATER RESOURCES CONTROL BOARD	T2 Cert-ChadS	05/04/2022	Grade 2 Treatment Renew-Chad Steinlicht	60
STA05 - STATE WATER RESOURCES CONTROL BOARD	T2 Exam-Brian B	05/04/2022	Grade 2 Treatment Exam App Brian Boring	45
STA05 - STATE WATER RESOURCES CONTROL BOARD	D3 Cert-BrandonRoth	05/18/2022	Grade 3 Distribution Certification-Brandon Roth	90
STA05 - STATE WATER RESOURCES CONTROL BOARD	T2 Renew-ChadS	05/26/2022	Grade 2 Treatment Renewal Chad Steinlicht	60
				335
STA13 - STATE WATER RESOURCES CONTROL BOARD				
Paid To Same Vendor				
STA13 - STATE WATER RESOURCES CONTROL BOARD	40522	04/05/2022	Ground Water Extraction & Diversion-6 Wells	300
SUP04 - SUPERIOR TANK COMPANY, INC.				
Paid To Same Vendor				
SUP04 - SUPERIOR TANK COMPANY, INC.	7199	06/01/2022	Repair Level Indicator RMWTP Tank	4986
SWA02 - SWAGELOK/CCFST				
Paid To Same Vendor				
SWA02 - SWAGELOK/CCFST	53671	05/18/2022	Meter Station 5&7 Rehab Transmitter Parts	896.05
THE02 - THE CAPRICORN GROUP				
Paid To Same Vendor				
THE02 - THE CAPRICORN GROUP	18448	06/01/2022	Kitchen-Restroom Supplies	644.91
THE04 - LIFE TECHNOLOGIES CORPORATION				
Paid To Same Vendor				
THE04 - LIFE TECHNOLOGIES CORPORATION	81096436	04/13/2022	Materials & Supplies for the Lab	334.7
THE04 - LIFE TECHNOLOGIES CORPORATION	81480478	06/30/2022	Laboratory Supplies	208.15
				542.85
TOM03 - S-MT SALES, INC.				
Paid To Same Vendor				
TOM03 - S-MT SALES, INC.	16020	05/04/2022	Meter Station 5&7 Rehab Vault Lids	600
TOM03 - S-MT SALES, INC.	16109	06/28/2022	EQ Pond Screens	5712.69
				6312.69
TOT02 - TRAFFIC TECHNOLOGIES LLC				
Paid To Same Vendor				
TOT02 - TRAFFIC TECHNOLOGIES LLC	41209	06/27/2022	Signs for Non Potable Filling Station	897.38
TOT02 - TRAFFIC TECHNOLOGIES LLC	41317	06/30/2022	Conejo GAC Signage	391.39
				1288.77
TOT03 - TOTAL BARRICADE SERVICE INC				
Paid To Same Vendor				
TOT03 - TOTAL BARRICADE SERVICE INC	55459	05/18/2022	Traffic Control - Encroachment Permit MS11	320.05
TOT03 - TOTAL BARRICADE SERVICE INC	55460	05/18/2022	Traffic Control - Encroachment Permit MS11	320.05
TOT03 - TOTAL BARRICADE SERVICE INC	55660	05/27/2022	Traffic Control-Distribution Valve Replacement	490
TOT03 - TOTAL BARRICADE SERVICE INC	55627	06/01/2022	Traffic Control for Valve Replacement.	1169.6
TOT03 - TOTAL BARRICADE SERVICE INC	55659	06/01/2022	Traffic Control for Valve Replacement.	2199.6
TOT03 - TOTAL BARRICADE SERVICE INC	55480	06/10/2022	Traffic Control - Encroachment Permit MS11	320.05

TOT03 - TOTAL BARRICADE SERVICE INC	55692	06/15/2022	Traffic Control for Valve Replacement.	1369.6
				6188.95
TRA02 - TRAVIS AGRICULTURAL, INC				
Paid To Same Vendor				
TRA02 - TRAVIS AGRICULTURAL, INC	22242P	04/13/2022	Piping at RMWTP	3031.29
TRA02 - TRAVIS AGRICULTURAL, INC	22292-F	04/13/2022	Piping at RMWTP	6012.4
TRA02 - TRAVIS AGRICULTURAL, INC	22387-f	05/04/2022	24" Main Line Break Santa Rosa - Landscape Repair	12973
TRA02 - TRAVIS AGRICULTURAL, INC	22391-F	05/04/2022	Concrete Pads for MS 5&7	6863.79
TRA02 - TRAVIS AGRICULTURAL, INC	22397F	05/18/2022	Raise Valve Stackings	2363.2
TRA02 - TRAVIS AGRICULTURAL, INC	22485F	05/18/2022	Install 6" Valve at Penny Well	1952.18
TRA02 - TRAVIS AGRICULTURAL, INC	211360-P2	06/28/2022	Trench plate Rental - Travis AG	1091.23
TRA02 - TRAVIS AGRICULTURAL, INC	22668F	06/28/2022	Sewer Lift 1A MCC	10392.83
TRA02 - TRAVIS AGRICULTURAL, INC	22580-F	06/30/2022	Raise Pump Pedestals - Conejo Wells	18282.63
TRA02 - TRAVIS AGRICULTURAL, INC	22643-F	06/30/2022	Radio Tower 4B - Concete pad	15910
				78872.55
TUR01 - TURF CONSTRUCTION, INC.				
Paid To Same Vendor				
TUR01 - TURF CONSTRUCTION, INC.	14461	06/10/2022	Valve Replacement CIP - Calle Carillo	17124.64
TUR01 - TURF CONSTRUCTION, INC.	14462	06/10/2022	Valve Replacement CIP - Esperance Dr.	10838.32
				27962.96
TYL01 - TYLER TECHNOLOGIES, INC.				
Paid To Same Vendor				
TYL01 - TYLER TECHNOLOGIES, INC.	025-376681	04/25/2022	Incode Annual Maintenance	17601.57
UND01 - UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA, INC				
Paid To Same Vendor				
UND01 - UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA, 320220202		04/11/2022	Dig Alert MonthlyTickets	340
UND01 - UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA, 42020206		05/04/2022	Dig Alert Tickets Motnhly	275.65
UND01 - UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA, 520220206		06/10/2022	Monthly Dig Alert Tickets	349.9
UND01 - UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA, 620220206		06/30/2022	Dig Alert Montly Tickets	414.25
				1379.8
UNI08 - UNIFIRST CORPORATION				
Paid To Same Vendor				
UNI08 - UNIFIRST CORPORATION	328-1364190	04/25/2022	Uniform Cleaning Service	266.74
UNI08 - UNIFIRST CORPORATION	328-1364197	04/25/2022	Office Cleaning Supplies - Towel-Mat Service	72.85
UNI08 - UNIFIRST CORPORATION	328-1366187	04/25/2022	Uniform Cleaning Service	266.74
UNI08 - UNIFIRST CORPORATION	328-1366196	04/25/2022	Office Cleaning Supplies - Towel-Mat Service	72.85
UNI08 - UNIFIRST CORPORATION	328-1368160	04/25/2022	Uniform Cleaning Service	266.74
UNI08 - UNIFIRST CORPORATION	328-1368167	04/25/2022	Office Cleaning Supplies - Towel-Mat Service	72.85
UNI08 - UNIFIRST CORPORATION	328-1370161	04/29/2022	Uniform Cleaning Service	266.74
UNI08 - UNIFIRST CORPORATION	328-1370169	04/29/2022	Office Cleaning Supplies - Towel-Mat Service	72.85
UNI08 - UNIFIRST CORPORATION	328-1372124	05/26/2022	Uniform Cleaning Service	576.9
UNI08 - UNIFIRST CORPORATION	328-1372131	05/26/2022	Towel-Mat Service - Office Cleaning Supplies	72.85
UNI08 - UNIFIRST CORPORATION	328-1374145	05/26/2022	Uniform Cleaning Service	266.44
UNI08 - UNIFIRST CORPORATION	328-1374154	05/26/2022	Towel-Mat Service - Office Cleaning Supplies	75.96

UNI08 - UNIFIRST CORPORATION	328-1376248	05/26/2022	Uniform Cleaning Service	252.87
UNI08 - UNIFIRST CORPORATION	328-1376255	05/26/2022	Towel-Mat Service - Office Cleaning Supplies	75.85
UNI08 - UNIFIRST CORPORATION	328-1378247	05/26/2022	Uniform Cleaning Service	272.43
UNI08 - UNIFIRST CORPORATION	328-1378255	05/26/2022	Towel-Mat Service - Office Cleaning Supplies	75.85
UNI08 - UNIFIRST CORPORATION	328-1380220	05/27/2022	Office Cleaning Supplies - Towel-Mat Service	75.85
UNI08 - UNIFIRST CORPORATION	328-1380213	05/31/2022	Uniform Cleaning Service	550.42
UNI08 - UNIFIRST CORPORATION	328-1382217	06/27/2022	Uniform Cleaning Service	382.89
UNI08 - UNIFIRST CORPORATION	328-1382225	06/27/2022	Office Cleaning Supplies - Towel-Mat Service	85.4
UNI08 - UNIFIRST CORPORATION	328-1384155	06/30/2022	Uniform Cleaning Service	393.58
UNI08 - UNIFIRST CORPORATION	328-1384162	06/30/2022	Office Cleaning Supplies- Towel-Mat Service	75.85
UNI08 - UNIFIRST CORPORATION	328-1386148	06/30/2022	Uniform Cleaning Service	275.28
UNI08 - UNIFIRST CORPORATION	328-1386156	06/30/2022	Office Cleaning Supplies- Towel-Mat Service	75.85
				<hr/>
				4942.63

UNI10 - UNITED STATES TREASURY

Paid To Same Vendor

UNI10 - UNITED STATES TREASURY	INV0011392	04/07/2022	FIT	11612.44
UNI10 - UNITED STATES TREASURY	INV0011393	04/07/2022	Payroll-Social Security Tax	87.2
UNI10 - UNITED STATES TREASURY	INV0011394	04/07/2022	Payroll- Medicare Tax	3056.32
UNI10 - UNITED STATES TREASURY	INV0011420	04/12/2022	FIT	3459.91
UNI10 - UNITED STATES TREASURY	INV0011421	04/12/2022	Payroll- Medicare Tax	378.54
UNI10 - UNITED STATES TREASURY	INV0011482	04/21/2022	FIT	10218.89
UNI10 - UNITED STATES TREASURY	INV0011483	04/21/2022	Payroll-Social Security Tax	104.64
UNI10 - UNITED STATES TREASURY	INV0011484	04/21/2022	Payroll- Medicare Tax	2776.36
UNI10 - UNITED STATES TREASURY	INV0011489	04/21/2022	Payroll-Social Security Tax	471.2
UNI10 - UNITED STATES TREASURY	INV0011490	04/21/2022	Payroll- Medicare Tax	110.2
UNI10 - UNITED STATES TREASURY	INV0011492	04/28/2022	FIT	50.46
UNI10 - UNITED STATES TREASURY	INV0011493	04/28/2022	Payroll-Social Security Tax	122.08
UNI10 - UNITED STATES TREASURY	INV0011494	04/28/2022	Payroll- Medicare Tax	28.54
UNI10 - UNITED STATES TREASURY	INV0011514	05/05/2022	FIT	10362.54
UNI10 - UNITED STATES TREASURY	INV0011515	05/05/2022	Payroll- Medicare Tax	2819.96
UNI10 - UNITED STATES TREASURY	INV0011575	05/19/2022	FIT	10062.53
UNI10 - UNITED STATES TREASURY	INV0011576	05/19/2022	Payroll- Medicare Tax	2745.18
UNI10 - UNITED STATES TREASURY	INV0011581	05/19/2022	FIT	27.5
UNI10 - UNITED STATES TREASURY	INV0011582	05/19/2022	Payroll-Social Security Tax	719.2
UNI10 - UNITED STATES TREASURY	INV0011583	05/19/2022	Payroll- Medicare Tax	168.2
UNI10 - UNITED STATES TREASURY	INV0011643	06/02/2022	FIT	11130.51
UNI10 - UNITED STATES TREASURY	INV0011644	06/02/2022	Payroll- Medicare Tax	2949.46
UNI10 - UNITED STATES TREASURY	INV0011704	06/16/2022	FIT	11.67
UNI10 - UNITED STATES TREASURY	INV0011705	06/16/2022	Payroll-Social Security Tax	545.6
UNI10 - UNITED STATES TREASURY	INV0011706	06/16/2022	Payroll- Medicare Tax	127.6
UNI10 - UNITED STATES TREASURY	INV0011764	06/16/2022	FIT	10117.99
UNI10 - UNITED STATES TREASURY	INV0011765	06/16/2022	Payroll- Medicare Tax	2720.86
UNI10 - UNITED STATES TREASURY	CM0000373	06/27/2022	FIT	-1.54
UNI10 - UNITED STATES TREASURY	INV0011820	06/30/2022	FIT	10538.23
UNI10 - UNITED STATES TREASURY	INV0011821	06/30/2022	Payroll- Medicare Tax	2834.92
				<hr/>
				100357.19

UNI12 - UNIFIED FIELD SERVICES CORPORATION

Paid To Same Vendor

UNI12 - UNIFIED FIELD SERVICES CORPORATION	Pymt #8	04/13/2022	PV Well No. 2 Construction Services	95400
UNI12 - UNIFIED FIELD SERVICES CORPORATION	Retention-Pymt#8	04/13/2022	Retention Pymt#8- Project # PW21-01	-9540
UNI12 - UNIFIED FIELD SERVICES CORPORATION	Payment 9-PW21-01	06/14/2022	PV Well No. 2 Construction Services	137463.02
UNI12 - UNIFIED FIELD SERVICES CORPORATION	Retention-Pymt9	06/14/2022	Retention Pymt 9- Project PW21-01	-13746.3
UNI12 - UNIFIED FIELD SERVICES CORPORATION	Pymt 10-Project PW21-01	06/28/2022	PV Well No. 2 Construction Services	154661.55
UNI12 - UNIFIED FIELD SERVICES CORPORATION	Retention-Pymt10-Proj-PW21-01	06/28/2022	Retention Pymt10-Project PW21-01	-15466.16
				348772.11
UNI13 - UNION MATERIALS TESTING, INC				
Paid To Same Vendor				
UNI13 - UNION MATERIALS TESTING, INC	Inv#23	05/18/2022	GAC Materials Testing	2354
UNI13 - UNION MATERIALS TESTING, INC	36	06/15/2022	Material Testing	1818
				4172
UNU01 - UNUM LIFE INSURANCE				
Paid To Same Vendor				
UNU01 - UNUM LIFE INSURANCE	3-22 PR ME	04/01/2022	Swann Premium-Credit will be reflected on next st	45.41
UNU01 - UNUM LIFE INSURANCE	INV0011315	04/01/2022	Lont Term Disability	1149.88
UNU01 - UNUM LIFE INSURANCE	INV0011327	04/01/2022	Short Term Disability	266.46
UNU01 - UNUM LIFE INSURANCE	CM0000363	05/02/2022	Swann Credit & Patacsil Adust	-44.03
UNU01 - UNUM LIFE INSURANCE	INV0011468	05/02/2022	Lont Term Disability	1111.72
UNU01 - UNUM LIFE INSURANCE	INV0011480	05/02/2022	Short Term Disability	258.03
UNU01 - UNUM LIFE INSURANCE	INV0011561	06/01/2022	Lont Term Disability	1111.72
UNU01 - UNUM LIFE INSURANCE	INV0011573	06/01/2022	Short Term Disability	258.72
				4157.91
USA01 - USA BLUE BOOK				
Paid To Same Vendor				
USA01 - USA BLUE BOOK	929685	04/07/2022	Lab Supplies	96.47
USA01 - USA BLUE BOOK	951813	05/04/2022	Meter Parts	467.9
USA01 - USA BLUE BOOK	951934	05/04/2022	Meter Parts	160.61
USA01 - USA BLUE BOOK	001935	06/10/2022	Laboratory Supplies	78.08
USA01 - USA BLUE BOOK	998746	06/14/2022	Materials & Supplies - Standards	280.91
USA01 - USA BLUE BOOK	921763	06/15/2022	Laboratory Supplies	150.83
USA01 - USA BLUE BOOK	012124	06/21/2022	Lab Supplies	612.93
USA01 - USA BLUE BOOK	015327	06/27/2022	Laboratory Supplies	50.19
USA01 - USA BLUE BOOK	016354	06/27/2022	Ph and Conductivity probe	3622.11
USA01 - USA BLUE BOOK	016356	06/27/2022	Ph and Conductivity Probe	3622.11
USA01 - USA BLUE BOOK	018240	06/27/2022	Materials & Supplies - RMWTP	916.19
USA01 - USA BLUE BOOK	016355	06/28/2022	Ph and Conductivity Probe	3622.11
USA01 - USA BLUE BOOK	950234	06/30/2022	Lab Supplies	127.5
				13807.94
USB02 - U.S. BANK CORPORATE				
Paid To Same Vendor				
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	3/8 copper tubing, Salt,Parts Trwell	580.46
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Acid for RMWTP	225.14
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	After-Hours Call,Cable,Domain,Internet	1567.1
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	After-Hours Call,Cable,Domain,Internet	1622.73
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	After-Hours Call,Cable,Domain,Internet	1446.55
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Belts for CWRf exhaust fan	37.52

USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Business breakfast, Conf Regist, Meeting, Zoom	322.63
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Business breakfast, Conf Regist, Meeting, Zoom	297.81
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Business breakfast, Conf Regist, Meeting, Zoom	334.08
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Certs,SafetyBoots,ExamFees,Training	1194.95
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Certs,SafetyBoots,ExamFees,Training	1340.46
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Certs,SafetyBoots,ExamFees,Training	1294.53
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Conf Regist (IP) & (TLS), Meeting	564.38
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Conf Regist (IP) & (TLS), Meeting	545.03
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Conf Regist (IP) & (TLS), Meeting	503.1
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Gaskets for RMWTP	24.83
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Humidity Sensor	16.05
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Humidity Sensor	8.34
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Humidity Sensor	7.7
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Kitchen Supplies,Phone headset, N95 masks	333.14
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Kitchen Supplies,Phone headset, N95 masks	321.72
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Kitchen Supplies,Phone headset, N95 masks	296.97
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	MAP Gas	125.29
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	office chair	261
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	office chair	270.27
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	office chair	240.93
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Oil change for work truck,Power Steering Fluid	61.14
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Oil change for work truck,Power Steering Fluid	66.23
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Oil change for work truck,Power Steering Fluid	68.59
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Operator Training	14.04
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Operator Training	15.21
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Operator Training	15.75
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	PH Buffers,Ice,Printer Toner,Cooler	256.69
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	PH Buffers,Ice,Printer Toner,Cooler	228.82
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	PH Buffers,Ice,Printer Toner,Cooler	247.89
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Propane for CWRF,Stationary	23.29
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Propane for CWRF,Stationary	20.76
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Propane for CWRF,Stationary	22.49
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Shipped Conejo Creek PFAS samples	4.16
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Shipped Conejo Creek PFAS samples	3.84
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Shipped Conejo Creek PFAS samples	8
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Shipped SD900 controller, Printer Maint Kit	65.56
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Shipped SD900 controller, Printer Maint Kit	60.52
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Shipped SD900 controller, Printer Maint Kit	126.08
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Spill Containment Pallets,Sheet Plastic	1380.41
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	VC-APCD permit for GAC generator	467.25
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Vehicle Service, Monthly vehicle wash	50.4
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Vehicle Service, Monthly vehicle wash	54.6
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	Vehicle Service, Monthly vehicle wash	56.54
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	web site hosting	27.04
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	web site hosting	28
USB02 - U.S. BANK CORPORATE	22-Mar	04/13/2022	web site hosting	24.96
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	ACWA conf,WW meeting,teleconf	455.4
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	ACWA conf,WW meeting,teleconf	405.98
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	ACWA conf,WW meeting,teleconf	439.82
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	After-Hours Call Center, Internet	576.36

USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	After-Hours Call Center, Internet	556.6
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	After-Hours Call Center, Internet	513.79
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Chlorine with Deposit Bottles	315.25
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Door Hanger sleeves	13.11
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Door Hanger sleeves	12.66
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Door Hanger sleeves	11.69
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Field Services Tech recruitment	196
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Field Services Tech recruitment	174.72
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Field Services Tech recruitment	189.28
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	food for leak crew 24 main line leak	137.83
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Hardware for Sewer Lift #2,Pipe & pump cwr	646.39
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Inflight int service, AWA Training,WW Meeting	40.13
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Inflight int service, AWA Training,WW Meeting	35.78
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Inflight int service, AWA Training,WW Meeting	38.76
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Kitchen &Cleaning Supplies	148.12
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Kitchen &Cleaning Supplies	166.16
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Kitchen &Cleaning Supplies	160.46
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Microplastics Seminar,Water Dist & Treat class	470.5
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Microplastics Seminar,Water Dist & Treat class	434.3
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Microplastics Seminar,Water Dist & Treat class	487.2
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Propane for CWR	11.31
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Propane for CWR	12.69
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Propane for CWR	12.26
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Propane,parts,RO system office,Battereis	714.29
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Propane,parts,RO system office,Battereis	636.74
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Propane,parts,RO system office,Battereis	689.8
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Qty 4 HD Webcams,Ethernet cables	185.6
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Qty 4 HD Webcams,Ethernet cables	179.24
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Qty 4 HD Webcams,Ethernet cables	165.45
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Shipped samples to weck labs	38.28
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Shipped samples to weck labs	35.33
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Shipped samples to weck labs	73.61
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Shipped Standard Weights,Adaptor PH Meter	14.32
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Shipped Standard Weights,Adaptor PH Meter	13.21
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Shipped Standard Weights,Adaptor PH Meter	27.53
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Speakers SCADA,PumpPacking,FloatValve	235.27
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Trash bags,zip ties,trays,USB Adapter	157.46
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Trash bags,zip ties,trays,USB Adapter	140.36
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	Trash bags,zip ties,trays,USB Adapter	152.06
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	web site hosting,email domain,IVR	139.1
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	web site hosting,email domain,IVR	134.33
USB02 - U.S. BANK CORPORATE	22-Apr	05/09/2022	web site hosting,email domain,IVR	124
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	ACWA conference	273.33
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	ACWA conference	263.95
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	ACWA conference	243.65
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	After-Hours Call Cent & Internet	630.58
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	After-Hours Call Cent & Internet	652.97
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	After-Hours Call Cent & Internet	582.08
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Air Freshener for RMWTP	12.77
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	board room videocon equipment	84.24

USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	board room videocon equipment	87.23
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	board room videocon equipment	77.76
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Cold patch & hand tools	237.61
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Hand tools for truck 36	110.96
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Headphones,RepairParts,FlowMeter	553.08
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Kitchen Supplies,maks,coffee	106.22
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Kitchen Supplies,maks,coffee	102.58
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Kitchen Supplies,maks,coffee	94.69
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	lab supplies,Icstandards,distilledwater	185.2
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	lab supplies,Icstandards,distilledwater	170.95
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	lab supplies,Icstandards,distilledwater	356.16
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Memb renewal,ChapterMeeting	134.86
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Memb renewal,ChapterMeeting	124.48
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Memb renewal,ChapterMeeting	139.64
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	monthly vehicle wash	19.95
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	monthly vehicle wash	17.78
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	monthly vehicle wash	19.26
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Oil Change,Battery,CarServ,PartsDrinkFrount	233.81
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Oil Change,Battery,CarServ,PartsDrinkFrount	242.11
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Oil Change,Battery,CarServ,PartsDrinkFrount	215.83
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Shipped Thermometers,Calibration serv	65.34
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Shipped Thermometers,Calibration serv	70.78
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Shipped Thermometers,Calibration serv	136.12
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Storge Containers,tools batteries	1939.89
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	teleconferencing,ACWACnf	398.65
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	teleconferencing,ACWACnf	367.99
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	teleconferencing,ACWACnf	412.81
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	USB Cables, fuel, compressor	47.75
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	USB Cables, fuel, compressor	46.12
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	USB Cables, fuel, compressor	42.57
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	Water plug for cwrif	87.27
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	website hosting,cable,cyberbackup,emaildomain	840.46
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	website hosting,cable,cyberbackup,emaildomain	775.81
USB02 - U.S. BANK CORPORATE	22-May	06/15/2022	website hosting,cable,cyberbackup,emaildomain	870.3
				39775.09

UWA01 - UNITED WAY OF VENTURA CO.

Paid To Same Vendor

UWA01 - UNITED WAY OF VENTURA CO.	INV0011377	04/07/2022	Charity-United Way	20
UWA01 - UNITED WAY OF VENTURA CO.	INV0011455	04/21/2022	Charity-United Way	20
UWA01 - UNITED WAY OF VENTURA CO.	INV0011499	05/05/2022	Charity-United Way	20
UWA01 - UNITED WAY OF VENTURA CO.	INV0011548	05/19/2022	Charity-United Way	20
UWA01 - UNITED WAY OF VENTURA CO.	INV0011628	06/02/2022	Charity-United Way	20
UWA01 - UNITED WAY OF VENTURA CO.	INV0011737	06/16/2022	Charity-United Way	20
UWA01 - UNITED WAY OF VENTURA CO.	INV0011805	06/30/2022	Charity-United Way	20
				140

VEN02 - VENTURA REGIONAL SANITATION DISTRICT, INC

Paid To Same Vendor

VEN02 - VENTURA REGIONAL SANITATION DISTRICT, INC	33122	04/29/2022	VRSD Sewer Cleaning	3722.75
---	-------	------------	---------------------	---------

VEN02 - VENTURA REGIONAL SANITATION DISTRICT, INC	4122	05/18/2022	VRSD Sewer Cleaning	3165
				6887.75
VEN20 - VENTURA STEEL INC.				
Paid To Same Vendor				
VEN20 - VENTURA STEEL INC.	269706	06/15/2022	Steel for Pipe Rack - Conex Box	3777.35
VEN21 - VENTURA COUNTY AIR POLLUTION CONTROL DISTRICT				
Paid To Same Vendor				
VEN21 - VENTURA COUNTY AIR POLLUTION CONTROL DISTRICT	1045960	04/11/2022	Generator Permit - Penny Well	652
VEN21 - VENTURA COUNTY AIR POLLUTION CONTROL DISTRICT	1046237	06/10/2022	Generator Permit - PS 1	678
				1330
VEN35 - VENTURA COUNTY OVERHEAD DOOR				
Paid To Same Vendor				
VEN35 - VENTURA COUNTY OVERHEAD DOOR	436202	06/28/2022	Repair - Front Gate	195
VER02 - VERIZON WIRELESS				
Paid To Same Vendor				
VER02 - VERIZON WIRELESS	9907095314	05/27/2022	Cell Phones	2449.82
VER02 - VERIZON WIRELESS	9909413155	06/30/2022	Cell Phone's	2452.5
				4902.32
VER04 - VERIZON BUSINESS, INC				
Paid To Same Vendor				
VER04 - VERIZON BUSINESS, INC	72157834	04/12/2022	VOIP T1 (Verizon)	1221.08
VER04 - VERIZON BUSINESS, INC	9904751498	05/04/2022	Cell Phones	2450.94
VER04 - VERIZON BUSINESS, INC	72206604	05/18/2022	Cell Phones	1221.08
VER04 - VERIZON BUSINESS, INC	72231784	06/15/2022	VOIP T1 (Verizon)	1221.08
				6114.18
WAH01 - KEVIN WAHL				
Paid To Same Vendor				
WAH01 - KEVIN WAHL	Tuition-Spring2022	05/31/2022	Tuition Reimbursementsent Spring Term 2022	1509.47
WAL04 - WALTON MOTORS & CONTROLS, INC				
Paid To Same Vendor				
WAL04 - WALTON MOTORS & CONTROLS, INC	43367	05/04/2022	Motor Repair SL2A	3513.51
WAT12 - WATER SYSTEMS OPTIMIZATION INC.				
Paid To Same Vendor				
WAT12 - WATER SYSTEMS OPTIMIZATION INC.	2200	04/08/2022	WSO Leak Detection	25590
WBI01 - WBI INC				
Paid To Same Vendor				
WBI01 - WBI INC	C-22-1	04/29/2022	Sludge Pressing	48000
WES01 - GENE WEST				
Paid To Same Vendor				
WES01 - GENE WEST	5-10-22 ACWA CONF-Reimb	05/10/2022	Travel Reimbursement-ACWA Conference 5-03 th 5-05	1708.2

WES17 - WESCO DISTRIBUTION, INC**Paid To Same Vendor**

WES17 - WESCO DISTRIBUTION, INC	892889	06/30/2022	Replacement VFD's CWRF Bar Screen	2887.83
---------------------------------	--------	------------	-----------------------------------	---------

WHI03 - WHITE BRENNER LLP**Paid To Same Vendor**

WHI03 - WHITE BRENNER LLP	45025	05/18/2022	Legal Services	4386
WHI03 - WHITE BRENNER LLP	45025-R	05/18/2022	Legal Services	-4386
WHI03 - WHITE BRENNER LLP	45056	05/18/2022	Legal Services	6339
WHI03 - WHITE BRENNER LLP	45056-R	05/18/2022	Legal Services	-6339
WHI03 - WHITE BRENNER LLP	45025-	05/25/2022	Legal Services	4386
WHI03 - WHITE BRENNER LLP	45056-	05/25/2022	Legal Services	1953
WHI03 - WHITE BRENNER LLP	45567	06/29/2022	Legal Services	4546
				10885

WIL05 - Wilmington Trust**Paid To Same Vendor**

WIL05 - Wilmington Trust	Bond 2016-InterJuly2022	06/08/2022	2016 Bond Interest Payment	193520.14
--------------------------	-------------------------	------------	----------------------------	-----------

WWG01 - W W GRAINGER, INC.**Paid To Same Vendor**

WWG01 - W W GRAINGER, INC.	9273488446	04/12/2022	Material & Supplies	353.9
WWG01 - W W GRAINGER, INC.	9297260078	05/04/2022	Material & Supplies	336.26
WWG01 - W W GRAINGER, INC.	9308013037	05/18/2022	Repair Parts	156.75
WWG01 - W W GRAINGER, INC.	9308977694	05/18/2022	Rapair Parts - Pressure Washer	305.37
WWG01 - W W GRAINGER, INC.	9310807103	05/18/2022	Rapair Parts - Solar Charger	111.44
WWG01 - W W GRAINGER, INC.	9313188345	05/18/2022	Repair Parts - Pressure Washer	22.04
WWG01 - W W GRAINGER, INC.	9315565052	05/27/2022	Material and Supplies RMWTP	457.19
WWG01 - W W GRAINGER, INC.	9322118028	05/27/2022	Tools for Truck #39	303.27
WWG01 - W W GRAINGER, INC.	9323904194	05/27/2022	Repair Parts	272.09
WWG01 - W W GRAINGER, INC.	9328855227	06/14/2022	Ladders for Trucks	914.12
WWG01 - W W GRAINGER, INC.	9329468343	06/14/2022	Ladders for Conex Boxes	509.59
WWG01 - W W GRAINGER, INC.	9337856430	06/14/2022	Repair Parts - Motor for SL3	640.01
WWG01 - W W GRAINGER, INC.	9338156061	06/14/2022	Materials & Supplies - RMWTP	581.86
WWG01 - W W GRAINGER, INC.	9340114751	06/14/2022	Repair Parts - Motor SL3	544.94
WWG01 - W W GRAINGER, INC.	9351311080	06/27/2022	Small Tools	951.91
WWG01 - W W GRAINGER, INC.	9360653936	06/30/2022	Small Tools	979.35
WWG01 - W W GRAINGER, INC.	9360653944	06/30/2022	Small Tools	994.7
WWG01 - W W GRAINGER, INC.	9362558547	06/30/2022	Small Tools	973.28
				9408.07

XYL01 - YSI Incorporated**Paid To Same Vendor**

XYL01 - YSI Incorporated	940545	06/15/2022	YSI Sequential Chlorination CIP	25699.33
XYL01 - YSI Incorporated	940799	06/15/2022	YSI Sequential Chlorination CIP	4629.94
XYL01 - YSI Incorporated	942213	06/27/2022	YSI Sequential Chlorination CIP	231.51
				30560.78

2022 Camrosa Board Calendar

JANUARY							FEBRUARY							MARCH							2022 Holidays						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	January 3 rd - New Year's Holiday (Observed) February 21 st - President's Day May 30 th - Memorial Day July 4 th - Independence Day September 5 th - Labor Day November 11 th - Veteran's Day November 24 th & 25 th - Thanksgiving December 23 rd & 26 th - Christmas December 30 th - New Year's Eve						
						1			1	2	3	4	5			1	2	3	4	5							
2	3	4	5	6	7	8	6	7	8	9	10	11	12	6	7	8	9	10	11	12							
9	10	11	12	13	14	15	13	14	15	16	17	18	19	13	14	15	16	17	18	19							
16	17	18	19	20	21	22	20	21	22	23	24	25	26	20	21	22	23	24	25	26							
23	24	25	26	27	28	29	27	28						27	28	29	30	31									
30	31						27	28																			
APRIL							MAY							JUNE							2022 Conferences						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	CASA Winter Conf. (Palm Springs) - Jan. 19 th - 21 st ACWA Spring Conf. (Sacramento) - May 3 rd - 6 th CASA 67th Annual Conf. (Squaw Creek) - Aug. 10 th - 12 th ACWA Fall Conf. (Indian Wells) - Nov. 29 th - Dec. 2 nd						
						1 2	1	2	3	4	5	6	7				1	2	3	4							
3	4	5	6	7	8	9	8	9	10	11	12	13	14	5	6	7	8	9	10	11							
10	11	12	13	14	15	16	15	16	17	18	19	20	21	12	13	14	15	16	17	18							
17	18	19	20	21	22	23	22	23	24	25	26	27	28	19	20	21	22	23	24	25							
24	25	26	27	28	29	30	29	30	31					26	27	28	29	30									
JULY							AUGUST							SEPTEMBER							2022 AWA Meetings						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	"Water Issues" Third Tuesday (except Apr., Aug., Dec.) Waterwise Breakfast (See yellow on calendar) AWA Board Meetings (See orange on calendar) August - DARK (No Meetings or Events) September 29 th - Reagan Library Reception **DATE ?? - Annual Symposium** December 8 th - Holiday Mixer						
						1 2		1	2	3	4	5	6					1	2	3							
3	4	5	6	7	8	9	7	8	9	10	11	12	13	4	5	6	7	8	9	10							
10	11	12	13	14	15	16	14	15	16	17	18	19	20	11	12	13	14	15	16	17							
17	18	19	20	21	22	23	21	22	23	24	25	26	27	18	19	20	21	22	23	24							
24	25	26	27	28	29	30	28	29	30	31				25	26	27	28	29	30								
31																											
OCTOBER							NOVEMBER							DECEMBER							2022 VCSDA Meetings						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	February 1 st - Annual Dinner April 5 th June 7 th August 2 nd October 4 th December 5 th						
						1			1	2	3	4	5					1	2	3							
2	3	4	5	6	7	8	6	7	8	9	10	11	12	4	5	6	7	8	9	10							
9	10	11	12	13	14	15	13	14	15	16	17	18	19	11	12	13	14	15	16	17							
16	17	18	19	20	21	22	20	21	22	23	24	25	26	18	19	20	21	22	23	24							
23	24	25	26	27	28	29	27	28	29	30				25	26	27	28	29	30	31							
30	31																										

Camrosa Water District
7385 Santa Rosa Road
Camarillo, CA 93012

Note: Board of Directors meetings are highlighted in **RED**. Board Meetings are held on the **2nd & 4th Thursday** of each month at 5pm unless indicated.