

Board Agenda

Regular Meeting

Thursday, August 18, 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 Regular Meeting of July 28, 2022**
2. ****Approve Vendor Payments**

Objective: Approve the payments as presented by Staff.

Action Required: Approve accounts payable in the amount of \$2,596,105.11.

3. Purchase of Meters

Objective: Purchase meters and related equipment.

Action Required: Authorize the General Manager to spend up to \$225,000.00 from the Fiscal Year 2022-23 budgeted amount for the purchase of meters and related equipment.

4. **Biosolids Processing

Objective: Dewater the biosolids drying beds at the Camrosa Water Reclamation Facility (CWRF).

Action Required: Authorize the General Manager to enter into an annual agreement with WBI, Inc., and issue a purchase order, in an amount not to exceed \$93,650.00, for dewatering of the biosolids drying beds.

Special Presentation

5. **Commending Al E. Fox for His Service to the Camrosa Water District

Objective: Commend Al E. Fox for his years of service to the Camrosa Water District.

Action Required: Adopt a resolution of the Board of Directors commending Al E. Fox for his service on the District's Board of Directors.

Primary Agenda

6. **Information Technology (IT) Plan Adoption

Objective: Adopt the District's Information Technology Plan.

Action Required: Adopt a Resolution of the Board of Directors Adopting an Information Technology Plan.

7. ** Purchase Meter Transmission Units for the Zone2 MTU Upgrade CIP

Objective: Purchase a quantity of 1,850, Model 3451, Meter Transmission Units (MTUs) from Aclara as part of the Fiscal Year 2022-23, AMR AclaraOne + MTU Upgrade Zone 2 capital improvement project.

Action Required: Authorize the General Manager to issue a purchase order with Aclara Technologies (a division of Hubbell Inc.), in an amount not to exceed \$216,450.00, for purchase of quantity 1,850, Model 3451 MTUs.

8. Local Production Update

Objective: Receive a briefing on local water production through the fourth quarter of Fiscal Year 2021-22.

Action Required: No action necessary; for information only.

9. **Public Works Contract Inspection Services

Objective: Outsource construction inspection services.

Action Required: It is recommended that the Board of Directors authorize the General Manager to enter into an agreement with Cannon Corporation, in an amount not to exceed \$249,937.00, for on-call inspection services.

10. Drought Update

Objective: Receive an update on the drought.

Action Required: No action necessary; for information only.

CLOSED SESSION: The Board may enter into a closed session to confidentially discuss pending litigation as authorized by Government Code 54956.9(d)(4).

11. Closed Session Conference with Legal Counsel – Pending Litigation

Objective: To confer with and receive advice from counsel regarding pending litigation.

Action Required: No action necessary; for information only.

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/

August 18, 2022

Board of
Directors
Agenda Packet

Board Minutes

Regular Meeting

Thursday, July 28, 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 (via teleconference)
 Jeffrey C. Brown, Director
 Timothy H. Hoag, Director

Staff: Tony Stafford, General Manager
 Ian Prichard, Assistant General Manager
 Tamara Sexton, Finance Manager
 Joe Willingham, IT Manager
 Jozi Zabarsky, Customer Service Manager
 Terry Curson, District Engineer
 Greg Jones, Legal Counsel

Public Comments

None

Consent Agenda

1. Approve Minutes of the Regular Meeting of July 14, 2022

The Board approved the Minutes of the Regular Meeting of July 14, 2022.

Motion: Brown **Second:** Hoag

Yes: Brown-Foreman-Hoag-West

Absent: Fox

2. Approve Vendor Payments

A summary of accounts payable in the amount of \$1,337,796.12 was provided for Board information and approval. The Board approved the payments to vendors as presented by staff in the amount of \$1,337,796.12.

Motion: Brown **Second:** Hoag

Yes: Brown-Foreman-Hoag-West

Absent: Fox

3. Purchase of Analytical Balance

The Board authorized the General Manager to establish a fixed asset in the amount of \$14,000.00 and issue a purchase order to Mettler-Toledo, in an amount not to exceed \$14,000.00, for the purchase of a replacement analytical balance in the water laboratory.

Motion: Brown **Second:** Hoag

Yes: Brown-Foreman-Hoag-West

Absent: Fox

4. Annual Disclosure of Director/Employee Reimbursements

The Board accepted the Annual Disclosure Report of Director/Employee Reimbursements for FY2021-22.

Motion: Brown **Second:** Hoag

Yes: Brown-Foreman-Hoag-West

Absent: Fox

Primary Agenda

5. Upgrade/Migrate Automatic Meter Reading (AMR) to AclaraOne

The Board authorized the General Manager to enter into an agreement with Aclara Technologies (a division of Hubbell Inc.), in an amount not to exceed \$42,185.60, for implementation and year-one support of AclaraOne.

Motion: Hoag **Second:** Foreman

Yes: Brown-Foreman-Hoag-West

Absent: Fox

6. Renew ESRI GIS Three-Year Enterprise License Agreement and Support Services

The Board authorized the General Manager to enter into a new three-year agreement with ESRI Inc, in the amount of \$33,000.00, billed annually at \$11,000.00 per year, for licensing and support of ESRI's Enterprise GIS application software.

Motion: Foreman **Second:** Brown

Yes: Brown-Foreman-Hoag-West

Absent: Fox

7. Greenlaw Partners (Skurka Aerospace) Water Will Service Letter

The Board authorized the General Manager to issue a Water Will-Serve letter to Greenlaw Partners for the Skurka Aerospace property.

Motion: Hoag **Second:** Brown

Yes: Brown-Foreman-Hoag-West

Absent: Fox

8. Drought Update

Received a presentation regarding developing a mechanism to equitably pass on any penalties the District may incur during this drought under MWD's Emergency Water Conservation Program.

No action taken; for information only.

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

9. Closed Session Conference with Legal Counsel – Pending Litigation

CANCELED

Comments by General Manager

- Notices were mailed out regarding the August 4, 2022 GSA stakeholders engagement session.
- The hours for non-potable filling station have been extended from 8am-12pm to 8am-4pm. Additional days may be added if needed.

Comments by Directors

- Director Foreman shared information received at the ACWA quarterly meeting regarding SB222 and water quality.
- President West shared positive feedback he received regarding the interaction of the directors at the recent virtual townhall meeting.

Adjournment

There being no further business, the meeting was adjourned at 6:34 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

August 18, 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 \$2,596,105.11.

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

Payroll PR 7-2 & ME	\$ 97,980.08
Accounts Payable 07/21/2022-08/10/2022	<u>\$ 2,498,125.03</u>
Total Disbursements	<u>\$ 2,596,105.11</u>

DISBURSEMENT APPROVAL	
BOARD MEMBER	DATE
BOARD MEMBER	DATE
BOARD MEMBER	DATE

Tony L. Stafford, General Manager

Month of : July-22

CAL-Card Monthly Summary					
Date Purchased	Statement Date	Vendor Name	Purchase Total	Item Description	Staff
07/17/22	07/22/22	Rolling Pin	\$51.43	Food for Main line Leak - Santa Rosa Rd	KW
07/20/22	07/22/22	Amazon	\$235.89	Kitchen supplies for CWRP	JS
07/19/22	07/22/22	Amazon	\$32.34	Kitchen supplies for CWRP	JS
06/29/22	07/22/22	Home Depot	\$120.87	Silicone and Paint for pipe rack at RMWTP	JS
06/23/22	07/22/22	Amazon	\$90.00	Parts for Pennywell air test	JS
06/23/22	07/22/22	Amazon	\$61.11	Parts for Pennywell air test	JS
07/15/22	07/22/22	Home Depot	\$106.12	Wet/Dry VAC	GM
07/14/22	07/22/22	Home Depot	\$172.46	Nitrile Gloves, pliers and screwdriver	GM
07/11/22	07/22/22	Red Wing Boots	\$268.11	Kylee's work boots	GM
07/07/22	07/22/22	Troemner	\$212.76	Calibrate Standard weights	GM
07/06/22	07/22/22	B and B Do It center	\$25.75	Parts for testing penny well	GM
07/06/22	07/22/22	UPS Store	\$248.09	Ship samples for University well	GM
07/07/22	07/22/22	Harbor Freight Tools	\$235.91	Vacuum pump and compressor and Screwdrivers	MP
07/05/22	07/22/22	CWEA	\$192.00	CWEA Annual Membership Dues	MP
07/05/22	07/22/22	ERA	\$219.83	Quick Turnaround O&G PT sample	MP
07/18/22	07/22/22	zoom	\$33.13	webinar for ASRGS stakeholder engagement	IP
07/02/22	07/22/22	Thinking2	\$80.00	web site hosting	IP
06/30/22	07/22/22	zoom	\$199.90	teleconferencing for Board & staff meetings	IP
07/20/22	07/22/22	Smart & Final	\$140.27	Kitchen Supplies	CP
07/12/22	07/22/22	Red Wing	\$284.20	Boots for Regal Morales	CP
07/06/22	07/22/22	Smart & Final	\$191.92	Kitchen Supplies	CP
07/19/22	07/22/22	Coastal Pipco	\$132.57	Materials/ repair parts for CWRP	JK
07/12/22	07/22/22	Home Depot	\$322.26	Tools and materials for work truck #38	JK
06/29/22	07/22/22	Coastal Pipco	\$184.12	repair parts for sewer lift 2	JK
06/28/22	07/22/22	FG Wilcox Tools, Inc	\$35.83	Bolts/hardware for sewer lift #2	JK
06/27/22	07/22/22	Target	\$36.08	Sunscreen (PPE)	JK
07/12/22	07/22/22	Famcon	\$44.83	Bushings for Meter Stations 5&7	JN
06/23/22	07/22/22	Central Communications	\$471.00	After-Hours Call Center	JZ
07/01/22	07/22/22	Staples - RETURN CREDIT	-\$117.95	Mailing labels	JZ
07/11/22	07/22/22	The Home Depot	\$41.52	Mortar & supplies for sluice gate repair at Ponds	BB
07/08/22	07/22/22	Industrial Bolt & Supply	\$91.26	Anchors for sluice gate repair at Ponds	BB
07/08/22	07/22/22	VC Metals	\$189.94	Metal for sluice gate repair at Ponds	BB
06/28/22	07/22/22	Batteries Plus	\$75.27	Batteries for UPS at City Tower	BB
06/28/22	07/22/22	Batteries Plus	\$225.80	Batteries for UPS at City Tower	BB
06/24/22	07/22/22	U-Rent	\$68.84	Propane for forklift	BB
06/23/22	07/22/22	VC Metals	\$26.94	Aluminum plate for radio mounting at Res 4B	BB
06/30/22	07/22/22	The Home Depot	\$112.78	Red rusty metal primer- Connex pipe rack	CC
07/12/22	07/22/22	McMaster-Carr	\$449.07	Ball valves for meter stations 5/7	BR
06/25/22	07/22/22	Home Depot	\$48.07	Spray bottles for O&M	BR
07/12/22	07/22/22	Red Wing	\$306.71	Safety Boots for Mike Smith	MS
07/05/22	07/22/22	Oil Changers	\$69.11	Oil Change for Vehicle #40	MS
07/06/22	07/22/22	Oil Stop	\$69.18	vehicle service	TS
07/02/22	07/22/22	CarWashClub	\$56.99	monthly vehicle wash	TS
07/19/22	07/22/22	Spectrum	\$1,249.00	Spectrum Internet	JW
07/16/22	07/22/22	Mailchimp	\$59.00	Drought awareness outreach	JW
07/11/22	07/22/22	Callfire	\$99.00	online IVR - Delinquent Call Out (Monthly Service Fee)	JW
07/02/22	07/22/22	DNS Made Easy	\$1,740.00	Domain Naming System - CAMROSA.COM Annual Renewal	JW
07/01/22	07/22/22	Google.com	\$132.00	google corporate email domain - camrosawaterdistrict.org monthly charges - currently 11 seats	JW
07/01/22	07/22/22	DLT Solutions	\$678.15	Autocad annual support renewal	JW
06/26/22	07/22/22	Spectrum	\$86.56	Spectrum Cable	JW
07/19/22	07/22/22	Ashwell Trophy	\$42.55	Desk Bar for Arne Anselm	DA
07/01/22	07/22/22	Backgrounds Online	\$40.50	Background Check (KF)	DA
07/07/22	07/22/22	Industrial Bolt	\$81.89	Stainless washers for Penny Well	CS
07/06/22	07/22/22	Red Wing	\$308.83	Safety Boots Chad	CS
07/01/22	07/22/22	Buffums Safe Lock	\$215.00	Valet Keys for Brian's Truck #39	CS
06/30/22	07/22/22	The Home Depot	\$207.94	Conejos Gac Sign Hardware	CS
06/28/22	07/22/22	Establos Meat Market	\$85.44	Food for Leak Moorpark Rd	CS
06/22/22	07/22/22	Home Depot	\$90.50	Hardware for 4B Radio Hut	CS
			\$11,258.67		

Camrosa Water District

Accounts Payable Period:

07/21/2022-08/10/2022

Expense	Account Description	Amount
11100	Accounts Rec-Other	
15773	Deferred Outflows-UAL Prep.	
11700	Meter Inventory	
11900	Prepaid Insurance	4071.15
11905	Prepaid Maintenance Ag	
13000	Land	
13400	Construction in Progress	1357043.34
20053	Current LTD Bond 2016	
20052	Current LTD Bond 2012	
20400	Contractor's Retention	5420.23
20250	Non-Potable Water Purchases	
23001	Refunds Payable	1272.73
50110	Payroll FLSA Overtime-Retro	
50010	Water Purchases & SMP	693590.08
50020	Pumping Power	
50100	Federal Tax 941 1 st QTR	
50012	CamSan Reclaimed Water	10205.94
50135	PERS Retirement	
50200	Utilities	22.58
50210	Communications	4660.14
50220	Outside Contracts	84811.90
50230	Professional Services	61137.76
50240	Pipeline Repairs	134621.06
50250	Small Tool & Equipment	1911.79
50260	Materials & Supplies	46945.79
50270	Repair Parts & Equip Maint	70718.30
50280	Legal Services	13315.36
50290	Dues & Subscriptions	192.00
50300	Conference & Travel	233.03
50310	Safety & Training	935.83
50330	Board Expenses	
50340	Bad Debt	
50350	Fees & Charges	4972.00
50360	Insurance Expense	
50500	Misc Expense	
50600	Fixed Assets	2044.02
50700	Interest Expense	
TOTAL		\$2,498,125.03

By Vendor Name

Payable Dates 7/21/2022 - 8/10/2022 Post Dates 7/21/2022 - 8/10/2022

TOTAL VENDOR PAYMENTS-GSA	\$	310,471.94
----------------------------------	-----------	-------------------

3343	07/28/2022	DEPOSIT ONLY-CAMROSA WTR	7-28-22-AP	Transfer to Disbursements Account -AP	Transfer to disbursements-holding	920000
3344	07/28/2022	DEPOSIT ONLY-CAMROSA WTR	7-28-22-PR	Transfer to disbursements account-PR	Transfer to disbursements-holding	139500
					Vendor *CAM* - DEPOSIT ONLY-CAMROSA WTR Total:	1059500
1040	08/08/2022	ACWA JOINT POWERS INS	2022-23	Cyber Insurance	Prepaid liability insurance	4071.15
58277	08/03/2022	AG RX INC.	100128	Weed Abatement - Conejo Well Field	Outsd contracts	628.64
58278	08/03/2022	ALEXANDER'S CONTRACT SERVICES, INC	104207	Meter Reading	Outsd contracts	1450.07
Vendor: ALL11 - ALL PEST AND REPAIR, INC.						
58279	08/03/2022	ALL PEST AND REPAIR, INC.	0025743	Outside Contracts - Pest Control -VTA1-1900	Outsd contracts	650
58279	08/03/2022	ALL PEST AND REPAIR, INC.	0025780	Outside Contracts-Pest Control -VTA1-7385	Outsd contracts	470
					Vendor ALL11 - ALL PEST AND REPAIR, INC. Total:	1120

58280	07/29/2022	ALLCONNECTED INC	105632	AllConnected Managed IT/OT Services and Support	Outsd contracts	FY23-0003	7489.54
58280	07/29/2022	ALLCONNECTED INC	105706	AllConnected Managed IT/OT Services and Support	Outsd contracts	FY23-0003	7489.54
58280	07/29/2022	ALLCONNECTED INC	43144	AllConnected - Managed IT/OT Services	Outsd contracts	FY22-0219-R1	10444.38
58280	07/29/2022	ALLCONNECTED INC	43145	AllConnected - Managed IT/OT Services	Outsd contracts	FY22-0219-R1	3701.25
58280	07/29/2022	ALLCONNECTED INC	43156	Historian Server	Construction in progress	FY22-0365-R1	14399.53
Vendor ALL14 - ALLCONNECTED INC Total:							43524.24
58281	08/08/2022	ANGELICA HERNANDEZ	00003129-2	Closed Act Overpayment Refund- 5347 Holly Ridge	Refunds payable		84.12
58282	08/09/2022	AQUA-METRIC SALES CO	INV0089550	NP Meters	Repair Parts & Equipment Mainten	FY22-0285-R1	50554.12
58283	07/29/2022	ASHLEY MYERS	00007091	Deposit Refund Act 7091 - 408 Lucero Stq	Refunds payable		90.17
58284	08/09/2022	BASELINE ENTERPRISES	19851	Outside Contracts - Fuel Tank Inspector	Outsd contracts		981.75
58276	08/02/2022	CALIFORNIA HIGHWAY PATROL	9770-2022-000455	Copy Police Report for Hydrant Hit 6-21-22	Fees & charges		10
Vendor: CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT							
1041	08/08/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	072022	Water Purchase Potable	Water purchases Potable		545730.04
1041	08/08/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	072022	Water Purchase	CMWD Fixed Charges		74142
1041	08/08/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	072022	Water Purchase-Non Potable	Water purchases Non-Pot		57118.41
1041	08/08/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	SMP070922	SMP CMWD - SMP Pipeline Fee	SMP CWD-RMWTP		16013.78
1041	08/08/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	SMP070922	SMP CMWD - SMP Pipeline Fee	SMP CMWD		585.85
Vendor CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT Total:							693590.08

Vendor: CAN03 - Cannon Corporation

58265	07/21/2022	Cannon Corporation	80863-A	Construction Services	Construction in progress	FY20-0256-R3	99.5
58285	08/09/2022	Cannon Corporation	81197	Engineering Support Services during construction	Construction in progress	FY21-0035-R2	398

Vendor CAN03 - Cannon Corporation Total: **497.5**

58286	08/08/2022	CHELSIE HANSEN	00007195	Closed Acct Overpayment Refund - 277 Via Cantilena	Refunds payable		91.34
58287	08/10/2022	CITY OF CAMARILLO	29619	Recycled water from CamSan June 2022	CamSan Water		10205.94

Vendor: CLI01 - CLIFTON LARSON ALLEN LLP

58288	08/08/2022	CLIFTON LARSON ALLEN LLP	3370881	Profesional Auditing Services FY2021-22	Prof services	FY22-0369-R1	3240
58288	08/08/2022	CLIFTON LARSON ALLEN LLP	3370881-b	GASB 87 Lease Accounting Implementation Assistance	Prof services	FY22-0368-R1	400

Vendor CLI01 - CLIFTON LARSON ALLEN LLP Total: **3640**

58289	08/05/2022	COASTAL-PIPCO	52190289-001	Penny Well Degasifier - Pilot Test	Construction in progress		233.71
58290	08/08/2022	COLANTUONO, HIGHSMITH & WHATLEY, PC	52691	Prop 218-26 Legal Services	Legal services		877.5

Vendor: COU01 - COUNTY OF VENTURA RMA OPERATIONS

58291	07/29/2022	COUNTY OF VENTURA RMA OPERATIONS	IN0228648	County Cross Connection Program	Outsd contracts	FY23-0004	17034.76
58291	07/29/2022	COUNTY OF VENTURA RMA OPERATIONS	IN0229810	County Cross Connection Program	Outsd contracts	FY22-0373	3961.57

Vendor COU01 - COUNTY OF VENTURA RMA OPERATIONS Total: **20996.33**

58292	08/03/2022	CULLIGAN OF VENTURA COUNTY	Aug2022-201478	Water Softener - Penny Well	Outsd contracts		82.5
58293	08/08/2022	DAVID FOWLER	00003475	Deposit Refund Act 3475- 5176 Creekside Rd	Refunds payable		61.61

Vendor: DAV01 - DAVMAR AIR

58294	07/29/2022	DAVMAR AIR	11422	Air Compressor Maintenance Pond 3	Outsd contracts	FY22-0370	3883.01
58294	07/29/2022	DAVMAR AIR	11428	Air Compressor Maintenance CWRF	Outsd contracts	FY22-0371	1824.26

Vendor DAV01 - DAVMAR AIR Total: **5707.27**

58295	07/29/2022	DLT SOLUTIONS, LLC	SI556201	Annual Autodesk Autocad Support Renewal	Outsd contracts		678.15
58296	08/08/2022	DONGCHEOL HYUN	00003359	Deposit Refund Act 3359 - 888 Creekside Cir	Refunds payable		9.74
58297	07/29/2022	DONNA A CALAMIA	00001660	Deposit Refund Act 1660 - 5053 Galano Dr	Refunds payable		47.35
58298	08/09/2022	E.J. HARRISON & SONS INC	875	Trash Removal- CWRF	Outsd contracts		922.23
58299	07/29/2022	EDY TOLEDO	00002265	Deposit Refund Act 2265 - 388 Mira Flores Ct	Refunds payable		30.22
58300	07/29/2022	ELAP-CDHS	EA-AN-0922-1638	ELAP Fees for Water Lab	Fees & charges	FY23-0013	4250
58301	08/03/2022	Enhanced Landscape Development, Inc	88071	Landscaping	Outsd contracts		2082
58302	08/09/2022	ENVIRONMENTAL RESOURCE ASSOCIATES	007581	Recertification Samples	Materials & supplies		4882.62
58303	08/08/2022	ESQUIRE PROPERTY MANAGEMENT	00006488	Deposit Refund Act 6488 - 7042 Paseo Encantada	Refunds payable		110

Vendor: FAM01 - FAMCON PIPE & SUPPLY, INC

58304	08/10/2022	FAMCON PIPE & SUPPLY, INC	S100081253-001	Repair Parts14" and 18" Couplings - Effluent Line	Repair parts & equipment	FY23-0031	6572.28
58304	08/08/2022	FAMCON PIPE & SUPPLY, INC	S100083009-001	Parts for Meter Station 5&7 -Rehabilitation	Construction in progress		132.08
58304	08/10/2022	FAMCON PIPE & SUPPLY, INC	S100083424-001	Leak Repair 2" Blow Off - Parts	Pipeline repairs	FY23-0029	3584.3
58304	08/10/2022	FAMCON PIPE & SUPPLY, INC	S100083470-001	24" Main Line Break Santa Rosa -Parts	Pipeline repairs	FY23-0025	4387.6
58304	08/10/2022	FAMCON PIPE & SUPPLY, INC	S100083534-001	24" Main Line Break Santa Rosa -Parts	Pipeline repairs	FY23-0025	4387.6
58304	08/08/2022	FAMCON PIPE & SUPPLY, INC	S100083983-001	Small Tools and Equipment - Hand Tools Unit 40-22	Small tools & equipment		442.94
58304	08/10/2022	FAMCON PIPE & SUPPLY, INC	S100084129-001	24" Main Line Break Santa Rosa -Parts	Pipeline repairs	FY23-0025	4310.38
58304	08/10/2022	FAMCON PIPE & SUPPLY, INC	S100084164-001	24" Main Line Break Santa Rosa -Parts	Pipeline repairs	FY23-0025	4310.38
58304	08/10/2022	FAMCON PIPE & SUPPLY, INC	S100084186-001	Leak Fire Hydrant Bury - Parts	Pipeline repairs	FY23-0026	1131.49
58304	08/10/2022	FAMCON PIPE & SUPPLY, INC	S100084334-001	Leak Repair 6" Valve - Parts	Pipeline repairs	FY23-0027	1411.09

Vendor FAM01 - FAMCON PIPE & SUPPLY, INC Total: **30670.14**

Vendor: *FRB* - First Republic Bank

1035	07/26/2022	First Republic Bank	CUS05-Rtn Pymt 6	Retenton Paymt 6 P.O. FY22-0179	Contractor's retention		16473.8
1042	08/03/2022	First Republic Bank	Retention-PPE#7	Retention sent to First Rep Bnk-PPE#7	Contractor's retention		30959.45

Vendor *FRB* - First Republic Bank Total: **47433.25**

58305	08/03/2022	Frontier Communications	July 2022	VOIP- Land Lines	Communications		453.73
-------	------------	-------------------------	-----------	------------------	----------------	--	--------

Vendor: FRU01 - FRUIT GROWERS LAB. INC.

58306	08/09/2022	FRUIT GROWERS LAB. INC.	207516A	Outside Lab Analysis	Outsd contracts	150
58306	08/09/2022	FRUIT GROWERS LAB. INC.	210553A	Outside Lab Analysis	Outsd contracts	36
58306	08/09/2022	FRUIT GROWERS LAB. INC.	211517A	Outside Lab Analysis	Outsd contracts	36
58306	08/09/2022	FRUIT GROWERS LAB. INC.	211518A	Outside Lab Analysis	Outsd contracts	36
58306	08/09/2022	FRUIT GROWERS LAB. INC.	211519A	Outside Lab Analysis	Outsd contracts	36
58306	07/29/2022	FRUIT GROWERS LAB. INC.	211520A	Outside Lab Work	Outsd contracts	36
58306	08/09/2022	FRUIT GROWERS LAB. INC.	211896A	Outside Lab Analysis	Outsd contracts	36
58306	08/09/2022	FRUIT GROWERS LAB. INC.	211899A	Outside Lab Analysis	Outsd contracts	36
58306	08/09/2022	FRUIT GROWERS LAB. INC.	212194A	Outside Lab Analysis	Outsd contracts	36
Vendor FRU01 - FRUIT GROWERS LAB. INC. Total:						438

Vendor: GEN06 - GENERAL PUMP COMPANY, INC

58307	08/08/2022	GENERAL PUMP COMPANY, INC	29510	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	Construction in progress	FY22-0163-R1	64137
58307	08/08/2022	GENERAL PUMP COMPANY, INC	29511	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	Construction in progress	FY22-0163-R1	58872
58307	08/08/2022	GENERAL PUMP COMPANY, INC	29512	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	Construction in progress	FY22-0163-R1	58255
Vendor GEN06 - GENERAL PUMP COMPANY, INC Total:							181264
58308	08/09/2022	Golden State Labor Compliance	08-2022-04	Additional Labor Compliance	Construction in progress	FY22-0012-R1	1504

Vendor: HAC01 - HACH COMPANY

58309	08/03/2022	HACH COMPANY	13158626	Materilas & Supplies - Reagents - RMWTP	Materials & supplies		436.99
58309	08/03/2022	HACH COMPANY	13160924	HACH Sequential Chlorination CIP	Construction in progress	FY22-0329-R1	4741.14
58309	08/03/2022	HACH COMPANY	13163903	Reagents - RMWTP	Materials & Supplies-RMWTP		399.4
58309	08/09/2022	HACH COMPANY	13165911	Repair Parts for 5500 at TR Well-Hack Parts	Repair parts & equipment		1228.83
58309	08/03/2022	HACH COMPANY	13169046	Reagents- 5500 Woodcreek/TR Well Conejo	Materials & supplies		1339.37
58309	08/08/2022	HACH COMPANY	13179604	Repair Parts for 5500 Woodcreek/TR/Conejos	Repair parts & equipment		296.5
Vendor HAC01 - HACH COMPANY Total:							8442.23

58310	08/08/2022	HOSE-MAN, INC.	5297337-0001-05	Parts for Entrained Air Pilot- Penny Well-Degasifi	Construction in progress		500.05
58311	08/03/2022	IDEXX LABORATORIES, INC	3111251464	VOIP- Land Lines	Materials & supplies		3496.9
58312	08/10/2022	J&H Engineering	3903	Leak Repair 2" Blow Off	Pipeline repairs	FY23-0028	11256

Vendor: CUS05 - JAMES C. CUSHMAN, INC.

58267	07/26/2022	JAMES C. CUSHMAN, INC.	Pymt 6	GAC Construction	Construction in progress	FY22-0179-R1	329476
58267	07/26/2022	JAMES C. CUSHMAN, INC.	Retention-Pymt 6	Retention Pymt 6 (P.O. FY22-0179	Contractor's retention		-16473.8
58313	08/03/2022	JAMES C. CUSHMAN, INC.	PPE#7	GAC Construction	Construction in progress	FY22-0179-R1	619189
58313	08/03/2022	JAMES C. CUSHMAN, INC.	Retention-PPE#7	Retention-Inv Ref#PPE#7	Contractor's retention		-30959.45
Vendor CUS05 - JAMES C. CUSHMAN, INC. Total:							901231.75

58314	08/03/2022	Janitek Cleaning Solutions-Allstate Cleaning, Inc.	45427A	Cleaning Service	Outsd contracts		1772
58315	07/29/2022	JARED M DIXON	00006697-2	Deposit Refund Act 6697 - 5358 Corte Pico Verde	Refunds payable		92.63
58316	08/08/2022	JOHN SHUTT	00003708	Deposit Refund Act 3708 - 1426 Calle Lozano	Refunds payable		11.18
58317	08/08/2022	KAREN RAMIREZ	00001011	Deposit Refund Act 1011- 6034 Via Montanez	Refunds payable		39.51
58318	08/08/2022	KATHY SWENSON	00003254-2	Closed Overpayment Refund- 5734 Cherry Ridge	Refunds payable		80.51

Vendor: KEN04 - KENNEDY/JENKS CONSULTANTS

58268	07/26/2022	KENNEDY/JENKS CONSULTANTS	156562	Grant Program (Kennedy/Jenks)	Prof services	FY22-0271-R1	4355
58319	08/05/2022	KENNEDY/JENKS CONSULTANTS	#59	Grant Program (Kennedy/Jenks)	Prof services	FY22-0271-R1	6719
Vendor KEN04 - KENNEDY/JENKS CONSULTANTS Total:							11074

58320	08/10/2022	LANDMARK GRADING & PAVING, INC	2022-07427	24" Main Line Break Santa Rosa - Road Repair	Pipeline repairs	FY23-0023	22249.18
58321	07/29/2022	LAUREN LITTLE	00004442	Deposit Refund Act 4442 - 1844 Moonshadow Cir	Refunds payable		48.89
58322	08/08/2022	LEANN WILKIE	00002341	Deposit Refund Act 2341 - 6250 Calle Bodega	Refunds payable		33.84
58323	08/05/2022	LIBERTY COMPOSTING, INC	31067	Sludge Removal	Outsd contracts	FY23-0018	8803.24
58324	08/10/2022	Mackay Communications, Inc.	SB-202203-980-1	Satellite Phones	Communications		34.91
58325	07/29/2022	MARK JOHNSON	00000851	Final Account Overpayment Refund - 1134 Paquita	Refunds payable		84.65
58326	08/08/2022	McMASTER-CARR SUPPLY CO	79930448	Parts for Meter Station 5&7 Rehabilitation	Construction in progress		69.92

58327	07/29/2022	METTLER-TOLEDO, INC.	655072918	Maintenance for Adam PW Analytical Balance	Repair parts & equipment		408.87
Vendor: MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.							
58269	07/26/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	100935	GAC Project Management	Construction in progress	FY21-0120-R2	4441.36
58269	07/26/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	100936	GAC Construction Management	Construction in progress	FY22-0151-R1	31770.2
58269	07/26/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	100937	CO-01: add City traffic control plans	Outsd contracts	FY22-0155-R1	207.03
58328	08/04/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	101031	GAC Project Management	Construction in progress	FY21-0120-R2	1009.4
58328	08/04/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	101032	GAC Construction Management	Construction in progress	FY22-0151-R1	28391.76
Vendor MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC. Total:							65819.75
58329	07/29/2022	NICHOLE MCINTIRE	1463-2	Close Account Overpayment Refund - 4695 Colony Dr	Refunds payable		95
Vendor: NOH01 - NOHO CONSTRUCTORS							
58330	07/29/2022	NOHO CONSTRUCTORS	mt 5-PW21-02-Retentio	Retention on Pmt 5-PW21-02	Contractor's retention		-2149.85
58330	08/10/2022	NOHO CONSTRUCTORS	Pmt 8-Retention	Pump Station 2 Generator/CWRF Fuel Tank Retention	Contractor's retention		15357.81
58330	07/29/2022	NOHO CONSTRUCTORS	Pymt 5 (PW-21-02)	Reservoir 1B communication facility	Construction in progress	FY22-0068-R1	42997
Vendor NOH01 - NOHO CONSTRUCTORS Total:							56204.96
Vendor: NOR07 - NORTHSTAR CHEMICAL							
58331	08/03/2022	NORTHSTAR CHEMICAL	229751	Materials & Supplies - Chemicals - RMWTP	Materials & Supplies-RMWTP		4837.51
58331	08/03/2022	NORTHSTAR CHEMICAL	230117	Material and Supplies - Chemicals - Tierra Rejada	Materials & supplies		1405.02
Vendor NOR07 - NORTHSTAR CHEMICAL Total:							6242.53
58332	08/03/2022	OLIN CORP-CHLOR ALKALI	3000135184	Material and Supplies - Chemicals - CWRF	Materials & supplies		9710.23
58333	08/03/2022	PAPE MATERIAL HANDLING, INC	6443373	Vehicle Maint- Forklift -Replace Parking Brake Han	Repair parts & equipment		973.92
58334	08/04/2022	PROVOST & PRITCHARD CONSULTING GROUP	93588	GAC Engineering	Construction in progress	FY20-0326-R3	2700
1045	08/10/2022	PUBLIC EMPLOYEES	100000016886319	GASB 68 Reports FY2022-23 Classic & PEPRA	Fees & charges		700
Vendor: PUR01 - PURETEC INDUSTRIAL WATER							
58335	08/03/2022	PURETEC INDUSTRIAL WATER	1997586	Chemicals - RMWTP	Materials & Supplies-RMWTP		12749.23
58335	08/05/2022	PURETEC INDUSTRIAL WATER	2002342	Deionized Water Service	Materials & supplies		78.24
58335	08/05/2022	PURETEC INDUSTRIAL WATER	2002343	Deionized Water Service	Materials & supplies		78.24
Vendor PUR01 - PURETEC INDUSTRIAL WATER Total:							12905.71
58336	08/08/2022	RAY	00000729	Deposit Refund Act 729 - 6341 IRENA AVE	Refunds payable		48.35
Vendor: RMG01 - RMG COMMUNICATIONS							
58270	07/26/2022	RMG COMMUNICATIONS	1353	otutreach	Prof services	FY22-0305-R1	6077.04
58270	07/26/2022	RMG COMMUNICATIONS	1372	otutreach	Prof services	FY22-0305-R1	1391.25
58270	07/26/2022	RMG COMMUNICATIONS	1394	otutreach	Prof services	FY22-0305-R1	2337.5
58337	08/04/2022	RMG COMMUNICATIONS	1416	otutreach	Prof services	FY22-0305-R1	2730
Vendor RMG01 - RMG COMMUNICATIONS Total:							12535.79
Vendor: ROY03 - ROYAL INDUSTRIAL SOLUTIONS							
58338	08/10/2022	ROYAL INDUSTRIAL SOLUTIONS	1018920	VFD's - TR Well	Repair parts & equipment	FY23-0033	2561.6
58338	08/10/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1019020	Repair Parts RMWTP - Surge Protection	Repair Parts & Equipment-RMWTP FY23-0032		5197.34
58338	08/08/2022	ROYAL INDUSTRIAL SOLUTIONS	9009-1023984	Parts for Entrained Air Pilot - Penny Well Degasif	Construction in progress		983.14
Vendor ROY03 - ROYAL INDUSTRIAL SOLUTIONS Total:							8742.08
Vendor: SAM01 - SAM HILL & SONS, INC.							
58339	08/10/2022	SAM HILL & SONS, INC.	4230	24" Main Line Break Santa Rosa -Repair	Pipeline repairs	FY23-0022	50883.32
58339	08/10/2022	SAM HILL & SONS, INC.	4231	Leak Fire Hydrant Bury	Pipeline repairs	FY23-0021	7092.59
Vendor SAM01 - SAM HILL & SONS, INC. Total:							57975.91
58273	07/28/2022	SANDRA SANCHEZ	00002303	Refund of Miss Applied Payment ACH	Refunds payable		190.99
Vendor: SAN04 - Santa Paula Materials, Inc.							
58340	08/04/2022	Santa Paula Materials, Inc.	19931	Leak Repair-Santa Rosa Rd 24" Mainline Leak	Pipeline repairs		494.48
58340	08/04/2022	Santa Paula Materials, Inc.	19939	Leak Repair-Santa Rosa Rd 24" Mainline Leak	Pipeline repairs		521.27
Vendor SAN04 - Santa Paula Materials, Inc. Total:							1015.75

Vendor: SCF01 - SC Fuels						
58341	07/29/2022	SC Fuels	2178239IN	Material & Supplies -Fuel	Materials & supplies	1771.01
58341	08/03/2022	SC Fuels	2183869IN	Material & Supplies - Fuel	Materials & supplies	1566.02
58341	08/05/2022	SC Fuels	2188594IN	Material & Supplies- Fuel	Materials & supplies	2130.82
Vendor SCF01 - SC Fuels Total:						5467.85
58342	07/29/2022	SHEA HOMES SO CAL INC	00010661-2	Refund Closed Account Overpayment - FH Meter	Refunds payable	22.63
Vendor: TOM03 - S-MT SALES, INC.						
58343	08/04/2022	S-MT SALES, INC.	16176	Welding for MS7-Meter Station 5 and Rehabilitation	Construction in progress	405
58343	08/10/2022	S-MT SALES, INC.	16177	Ladder Hatch Repair - 4C/3C Tanks	Outsd contracts FY23-0030	1191.68
Vendor TOM03 - S-MT SALES, INC. Total:						1596.68
Vendor: SCG01 - SOUTHERN CALIFORNIA GAS						
1046	08/04/2022	SOUTHERN CALIFORNIA GAS	July 2022	July Usage Charges -Act#123-787-1794-1	Utilities	14.79
1046	08/08/2022	SOUTHERN CALIFORNIA GAS	July 2022-A	July 2022 Usage Charges- Act 170-013-9900-9	Utilities	7.79
Vendor SCG01 - SOUTHERN CALIFORNIA GAS Total:						22.58
58271	7/26/2022	SOUTHERN CALIFORNIA EDISON CO	467563	Line Extension Contract-PV Well	Construction in progress	4641.83
Vendor: HAT01 - THE HATHAWAY LAW FIRM, LLP						
58272	07/26/2022	THE HATHAWAY LAW FIRM, LLP	20156	Legal Services	Legal services	10144.63
58344	08/09/2022	THE HATHAWAY LAW FIRM, LLP	201647	Legal Services- PFAS	Prof services	15002.9
58344	08/08/2022	THE HATHAWAY LAW FIRM, LLP	201648	Legal Services	Legal services	2293.23
Vendor HAT01 - THE HATHAWAY LAW FIRM, LLP Total:						27440.76
58345	08/09/2022	Thermo Electron North America LLC	18717	Analytical Balance	Fixed Assets-Internal FY23-0020	2044.02
58346	08/10/2022	TRAVIS AGRICULTURAL, INC	22790	24" Main Line Break Santa Rosa - Landscape Repair	Pipeline repairs FY23-0024	18464.51
1047	08/10/2022	U.S. BANK CORPORATE	22-Jul	Credit Care Purchases	Credit Cards Payment	11258.67
Vendor: UND01 - UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA, INC						
58347	08/04/2022	UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA	22-2300151	Dig Alert Tickets Monthly	Outsd contracts	120.74
58347	08/04/2022	UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA	720220206	Dig Alert Tickets Monthly	Outsd contracts	402
Vendor UND01 - UNDERGROUND SERVICE ALERT OF SOUTHERN CALIFORNIA, INC Total:						522.74
Vendor: UNI12 - UNIFIED FIELD SERVICES CORPORATION						
58348	08/04/2022	UNIFIED FIELD SERVICES CORPORATION	CM0000381	Retention-Pymt12-PV Well2	Contractor's retention	-7787.73
58348	08/04/2022	UNIFIED FIELD SERVICES CORPORATION	Pymt 12-PV Well-2	PV Well No. 2 Construction Services	Construction in progress FY22-0010-R1	77877.25
Vendor UNI12 - UNIFIED FIELD SERVICES CORPORATION Total:						70089.52
58349	08/05/2022	UNION MATERIALS TESTING, INC	#37	GAC Materials Testing	Construction in progress FY22-0270-R1	5790
Vendor: USA01 - USA BLUE BOOK						
58351	08/08/2022	USA BLUE BOOK	062474	Small Tools and Equipment -Sludge Judge for Clarif	Small tools & equipment	222.08
58351	08/08/2022	USA BLUE BOOK	068993	Material & Supplies - PPE Bio;ogical Control	Materials & supplies	853.02
Vendor USA01 - USA BLUE BOOK Total:						1075.1
58352	08/08/2022	VCSDA	2022-2023 BnkFee	Bank Fee Related to Altered Cjecl-Positive Reject	Fees & charges	12
58353	07/29/2022	VENTURA COUNTY OVERHEAD DOOR	436545	Repair Front Gate	Repair parts & equipment	790
58354	07/29/2022	VENTURA REGIONAL SANITATION DISTRICT, INC	202200-063022	VRSD Sewer Cleaning	Outsd contracts FY22-0033	4940.25
58355	08/04/2022	VERIZON WIRELESS	9911733899	Cell Phones	Communications	2451.5
Vendor: WWG01 - W W GRAINGER, INC.						
58356	08/05/2022	W W GRAINGER, INC.	9390969666	Pump for Penny Well - Test	Construction in progress FY23-0019	2923.55
58356	08/04/2022	W W GRAINGER, INC.	9394993613	Small Tools & Equipment -Vehicle #22	Small tools & equipment	534.41
58356	08/04/2022	W W GRAINGER, INC.	9395201222	Penny Well Degasifier	Construction in progress	286.66
Vendor WWG01 - W W GRAINGER, INC. Total:						3744.62
58357	08/05/2022	WOODARD & CURRAN, INC.	207048	Strategic Plan	Prof services FY22-0322-R1	18885.07

TOTAL VENDOR PAYMENTS-CAMROSA

\$2,498,125.03

1038	08/01/2022	ACWA/JPIA	7-22 PR ME	Health, Dental & Vision Premiums	Medical, Dental & Vision ins.	46590.24
DFT0004139	07/28/2022	CAL PERS 457 PLAN	INV0011934	Deferred Compensation	Deferred comp - ee paid	2466.46
DFT0004135	07/28/2022	COLONIAL SUPPLEMENTAL INS	INV0011930	Colonial Benefits	Colonial benefits	279.22
Vendor: EDD01 - EMPLOYMENT DEVELOP. DEPT.						
DFT0004130	07/22/2022	EMPLOYMENT DEVELOP. DEPT.	INV0011921	Payroll-SIT	P/R-sit	239.21
DFT0004134	07/28/2022	EMPLOYMENT DEVELOP. DEPT.	INV0011928	Payroll-SIT	P/R-sit	37.57
DFT0004155	07/28/2022	EMPLOYMENT DEVELOP. DEPT.	INV0011959	Payroll-SIT	P/R-sit	5128.75
					Vendor EDD01 - EMPLOYMENT DEVELOP. DEPT. Total:	5405.53
Vendor: HEA02 - HealthEquity						
DFT0004142	07/28/2022	HealthEquity	INV0011939	HSA-Employee Contribution	HSA Contributions Payable	438.46
DFT0004143	07/28/2022	HealthEquity	INV0011940	HSA Contributions	HSA Contributions Payable	200
					Vendor HEA02 - HealthEquity Total:	638.46
1037	07/28/2022	LINCOLN FINANCIAL GROUP	INV0011935	Deferred Compensation	Deferred comp - ee paid	2183
1036	07/28/2022	LINCOLN FINANCIAL GROUP	INV0011953	Profit Share Contribution	Profit share contributions	2632.33
DFT0004125	07/22/2022	PUBLIC EMPLOYEES	INV0011916	CalPERS Retirement	P/R-state ret.	17571.85
DFT0004144	07/28/2022	SYMETRA LIFE INS CO.	INV0011941	Life Insurance	Life ins.	270.25
DFT0004128	07/22/2022	UNITED STATES TREASURY	INV0011919	FIT	P/R-fit	18552.3
58274	07/28/2022	UNITED WAY OF VENTURA CO.	INV0011929	Charity-United Way	P/R-charity	20
1039	08/01/2022	UNUM LIFE INSURANCE	7-22 PR ME	Premium Adjustment Brandon Roth	Long term dis. human resources	1370.44
TOTAL PAYROLL VENDOR PAYMENTS-CAMROSA						\$ 97,980.08

Board Memorandum

August 18, 2022

To: General Manager

From: Kevin Wahl, Superintendent of Operations

Subject: Purchase of Meters

Objective: Purchase meters and related equipment.

Action Required: Authorize the General Manager to spend up to \$225,000.00 from the Fiscal Year 2022-23 budgeted amount for the purchase of meters and related equipment.

Discussion: It is the goal of the District to reduce lost revenue due to “apparent” water loss by routinely replacing aging and damaged water meters. There are approximately 8,600 meters in use throughout the District.

The purchase of meters and related equipment is an approved operations line item in the Fiscal Year 2022-23 budget.

Board Memorandum

August 18, 2022

To: General Manager

From: Kevin Wahl, Superintendent of Operations

Subject: Biosolids Processing

Objective: Dewater the biosolids drying beds at the Camrosa Water Reclamation Facility (CWRF).

Action Required: Authorize the General Manager to enter into an annual agreement with WBI, Inc., and issue a purchase order, in an amount not to exceed \$93,650.00, for dewatering of the biosolids drying beds.

Discussion: The CWRF produces biosolids as a byproduct of wastewater treatment. The CWRF drying beds often reach their capacity during wet periods of the year and need to be emptied. To accomplish this, WBI, Inc. will bring a belt press to dewater the existing biosolids and stockpile it for offsite hauling. WBI, Inc. has been providing a turnkey solution for the biosolids dewatering operation for the past 16 years. The existing multi-year agreement expired June 30, 2022. WBI, Inc. has been a reliable service provider and staff recommends entering into a one-year agreement.

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 5. For your protection, make sure that you read and understand all provisions before signing. The terms on pages 2 through 5 are incorporated in this document and will constitute a part of the agreement between the parties when signed.

TO:

W.B.I. Inc.
526 Kingwood Dr. #279
Kingwood, TX 77339

DATE:

July 28, 2022

Agreement No. 2023-59

The undersigned Contractor offers to furnish the following:

Provide dewatering pressing services for Camrosa at the Camrosa Water Reclamation Facility, per proposal dated 05/17/2022.

Contract price \$: Per Attached Proposal, not to exceed \$96,650.00

Contract Term: July 28, 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.

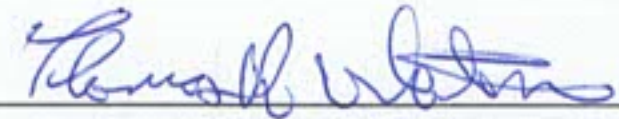
Accepted: Camrosa Water District

Contractor: W.B.I. Inc.

By:

Tony L. Stafford

By:

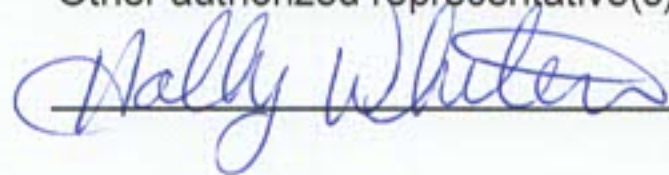

Thomas R. Whitener

Title: General Manager

Title: President

Other authorized representative(s):

Other authorized representative(s):



Workers' Compensation Insurance - By his/her signature hereunder, Contractor certifies that he/she is aware of the provisions of Section 3700 of the California Labor Code which require every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of that code, and he/she will comply with such provisions before commencing the performance of the work of this agreement.

Indemnification - To the fullest extent permitted by law, Contractor shall indemnify and hold harmless and immediately defend Camrosa Water District, its directors, officers, employees, or authorized volunteers, and each of them from and against:

- a. Any and all claims, demands, causes of action, damages, costs, expenses, losses or liabilities, in law or in equity, of every kind or nature whatsoever for, but not limited to, injury to or death of any person including, but not limited to, Camrosa Water District and/or Contractor, or any directors, officers, employees, or authorized volunteers of Camrosa Water District or Contractor, and damages to or destruction of property of any person, including but not limited to, Camrosa Water District and/or Contractor or their directors, officers, employees, or authorized volunteers, arising out of or in any manner directly or indirectly connected with the work to be performed under this agreement, however caused, regardless of any negligence of Camrosa Water District or its directors, officers, employees, or authorized volunteers, except the sole negligence or willful misconduct of Camrosa Water District or its directors, officers, employees, or authorized volunteers; and
- b. Any and all actions, proceedings, damages, costs, expenses, penalties or liabilities, in law or equity, of every kind or nature whatsoever, arising out of, resulting from, or on account of the violation of any governmental law or regulation, compliance with which is the responsibility of Contractor; and
- c. Any and all losses, expenses, damages (including damages to the work itself), attorneys' fees, and other costs, including all costs of defense, which any of them may incur with respect to the failure, neglect, or refusal of Contractor to faithfully perform the work and all of the Contractor's obligations under the agreement. Such costs, expenses, and damages shall include all costs, including attorneys' fees, incurred by the indemnified parties in any lawsuit to which they are a party; and
- d. Contractor shall immediately defend, at Contractor's own cost, expense and risk, any and all such aforesaid suits, actions, or other legal proceedings of every kind that may be brought or instituted against Camrosa Water District or its directors, officers, employees, or authorized volunteers, notwithstanding whether Contractor's liability is or can be established Contractor's obligation to indemnify shall not be restricted to insurance proceeds, if any received by Camrosa Water District, or its directors, officers, employees, or authorized volunteers.

Contractor shall pay and satisfy any judgment, award or decree that may be rendered against Camrosa Water District or its directors, officers, employees, or authorized volunteers, in any and all such suits, actions, or other legal proceedings.

Contractor shall reimburse Camrosa Water District or its directors, officers, employees, or authorized volunteers, for any and all legal expenses and costs incurred by each of them in connection therewith or in enforcing the indemnity herein provided.

GENERAL CONDITIONS

Laws, Regulations and Permits - The Contractor shall give all notices required by law and comply with all laws, ordinances, rules and regulations pertaining to the conduct of the work. The Contractor shall be liable for all violations of the law in connection with work furnished by the Contractor. If the Contractor performs any work knowing it to be contrary to such laws, ordinances, rules or regulations and without giving notice to Camrosa Water District engineer, the Contractor shall bear all costs arising therefrom.

Safety - The Contractor shall execute and maintain his/her work so as to avoid injury or damage to any person or property. The Contractor shall comply with the requirements of the specifications relating to safety measures applicable in particular operations or kinds of work.

In carrying out his/her work, the Contractor shall at all times exercise all necessary precautions for the safety of employees appropriate to the nature of the work and the conditions under which the work is to be performed, and be in compliance with all applicable federal, state and local statutory and regulatory requirements including, but not limited to, California Department of Industrial Relations (Cal/OSHA) regulations; and the U.S. Department of Transportation Omnibus Transportation Employee Testing Act, related to their scope of work and operations. In case of conflict in regulations, the most stringent shall apply

Commercial General Liability and Automobile Liability Insurance - The Contractor shall provide and maintain the following commercial general liability and automobile liability insurance:

Coverage - Coverage for commercial general liability and automobile liability insurance shall be at least as broad as the following:

1. Insurance Services Office (ISO) Commercial General Liability Coverage (Occurrence Form CG 0001)
2. Insurance Services Office (ISO) Business Auto Coverage (Form CA 0001), covering Symbol 1 (scheduled autos)
3. Insurance Service Office (ISO) Excess Liability (if necessary)

Limits - The Contractor shall maintain limits no less than the following:

1. General Liability - Two million dollars (\$2,000,000) per occurrence for bodily injury, personal injury and property damage. If Commercial General Liability Insurance or other form with a general aggregate limit or products-completed operations aggregate limit is used, either the general aggregate limit shall apply separately to the project/location (with the ISO CG 2503, or ISO CG 2504, or insurer's equivalent endorsement provided to Camrosa Water District) or the general aggregate limit and products-completed operations aggregate limit shall be twice the required occurrence limit.
2. Automobile Liability - One million dollars (\$1,000,000) for bodily injury and property damage each accident limit.
3. Excess Liability (if necessary) - The limits of Insurance required in this agreement may be satisfied by a combination of primary and umbrella or excess Insurance. Any umbrella or excess Insurance shall contain or be endorsed to contain a provision that such coverage shall also apply on a primary and non contributory basis for the benefit of the District (if agreed to in a written contract or agreement) before the District's own primary or self Insurance shall be called upon to protect it as a named insured.

Required Provisions - The general liability, auto liability and excess liability policies are to contain, or be endorsed to contain, the following provisions:

1. Camrosa Water District, its directors, officers, employees, and authorized volunteers are to be given insured status at least as broad as ISO endorsement CG 2010 11 85; or both CG 20 10 10 01 and CG 20 37 04 13, specifically naming all of the District parties required in this agreement, or using language that states "as required by contract". All subcontractors hired by Contractor must also have the same forms or coverage at least as broad; as respects (via CG 20 38 04 13): liability arising out of activities performed by or on behalf of the Contractor; products and completed operations of the Contractor; premises owned, occupied or used by the Contractor; and automobiles owned, leased, hired or borrowed by the Contractor. The coverage shall contain no special limitations on the scope of protection afforded to Camrosa Water District, its directors, officers, employees, or authorized volunteers.
2. It is understood and agreed to by the parties hereto and the insurance company(s), that the Certificate(s) of Insurance and policies shall so covenant and shall be construed as primary, and

Camrosa Water District insurance and/or deductibles and/or self-insured retentions or self-insured programs shall not be construed as contributory using the ISO endorsement CG 20 01 04 13 or coverage at least as broad.

3. Any failure to comply with reporting or other provisions of the policies including breaches of warranties shall not affect coverage provided to Camrosa Water District, its directors, officers, employees, or authorized volunteers.
4. The Contractor's insurance shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.
5. Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to the Camrosa Water District.
6. Such liability insurance shall indemnify the Contractor and his/her subcontractors against loss from liability imposed by law upon, or assumed under contract by, the Contractor or his/her subcontractors for damages on account of such bodily injury (including death), property damage, personal injury, completed operations, and products liability.
7. The general liability policy shall cover bodily injury and property damage liability, owned and non-owned equipment, blanket contractual liability, completed operations liability, explosion, collapse, underground excavation, and removal of lateral support.
8. The automobile liability policy shall cover all owned, non-owned, and hired automobiles.

All of the insurance shall be provided on policy forms and through companies satisfactory to Camrosa Water District.

Deductibles and Self-Insured Retentions - Any deductible or self-insured retention must be declared to and approved by Camrosa Water District. At the option of Camrosa Water District, the insurer shall either reduce or eliminate such deductibles or self-insured retentions. Camrosa Water District may require the Contractor to provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. Policies containing any self-insured retention (SIR) provision shall provide or be endorsed to provide that the SIR may be satisfied by either the named or additional insureds.

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

Workers' Compensation and Employer's Liability Insurance - The Contractor and all subcontractors shall insure (or be a qualified self-insured) under the applicable laws relating to workers' compensation insurance, all of their employees working on or about the construction site, in accordance with the "Workers' Compensation and Insurance Act", Division IV of the Labor Code of the State of California and any Acts amendatory thereof. The Contractor shall provide employer's liability insurance with limits of no less than \$1,000,000 each accident, \$1,000,000 disease policy limit, and \$1,000,000 disease each employee.

Contractor shall assume the immediate defense of and indemnify and save harmless Camrosa Water District and its officers and employees, agents, and consultants from all claims, loss, damage, injury, and liability of every kind, nature, and description brought by any person employed or used by Contractor, or any subcontractor, to perform the Work under this contract regardless of responsibility or negligence. Contractor hereby agrees to waive rights of subrogation which any insurer of Contractor may acquire from Contractor by virtue of the payment of any loss. Contractor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation. The Workers' Compensation Policy shall be endorsed with a waiver of subrogation in the favor of the Camrosa Water District for all work performed by the Contractor, its employees, agents and subcontractors.

Evidences of Insurance - Prior to execution of the agreement, the Contractor shall file with Camrosa Water District a certificate of insurance (Acord Form 25-S or equivalent) signed by the insurer's representative evidencing the coverage required by this agreement. Such evidence shall also include (1) attached additional insured endorsements with primary & non-contributory wording, (2) Workers' Compensation waiver of subrogation, and (3) a copy of the CGL declarations

or endorsement page listing all policy endorsements, and confirmation that coverage includes or has been modified to include Required Provisions 1-8 above. The District reserves the right to obtain complete, certified copies of all required insurance policies, at any time. Failure to continually satisfy the Insurance requirements is a material breach of contract.

The Contractor shall, upon demand of Camrosa Water District, deliver to Camrosa Water District such policy or policies of insurance and the receipts for payment of premiums thereon.

Continuation of Coverage - If any of the required coverages expire during the term of this agreement, the Contractor 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 - In the event that the Contractor employs other contractors (subcontractors) as part of the work covered by this agreement, it shall be the Contractor's responsibility to require and confirm that each contractor or subcontractor meets the minimum insurance requirements specified above, and Contractor shall ensure that Camrosa Water District, its directors, officers, employees, and authorized volunteers are an additional insured on Commercial General Liability Coverage.

Camrosa Water District reserves the right to modify these insurance requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage or other circumstances.

Payment, unless otherwise specified on Page 1, is to be 30 days after acceptance by Camrosa Water District.

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

W.B.I. Inc.

526 Kingwood Dr. #279, Kingwood, TX. 77339
Ofc. 713-907-7200 Fax

To: Camrosa Water
1900 Lewis St.
Camarillo, Cal. 93012
Fax: 805-987-4797
Ofc: 805-469-6401

Attn: Mr. Kevin Wahl

Date: 5/17/2022

Gentlemen,

Thank you for your inquiry. The following is an agreement for dewatering five (5) drying beds @ 2% sludge (Total 1,000,000 gallons) for the year 2023. The net cost for processing will be \$93,650.00 (Ninety-Three Thousand Six Hundred Fifty dollars). This proposal is good for forty-five (45) days.

WBI Inc. will supply:

1-Polymer pump for polymer solution.
1-Sludge pump
1 Water booster pump.
1-60 ft.-2" Water hose for booster pump
1-60 ft.-4" Suction hose for the sludge pump
1-60 ft.-4" Drain line for the filtrate
1-60-ft. #8 Electrical cable for 480 volts hook up.
1- Belt press
Polymer
Operator for front end loader
WBI Inc. will furnish copies of insurance by fax or E-mail.

Insurance: Camrosa will furnish all liability insurance required and
Workmen's compensation for their employees.

.

Terms for lease

Terms for lease:

Camrosa Water will supply:

Clean water source [min. 80 gpm @70 psi.

Stable and level site for trailer.

Front- end Loader, Fuel

Camrose to pay if any taxes, permits and lab work.

To accept this agreement please issue a purchase order number or name.

If you have any questions, please call me at office 713-907-7200.

Sincerely,

Thomas R. Whitener

WBI Inc.

Owner/President

Board Memorandum

August 18, 2022

To: Board of Directors

From: General Manager

Subject: Commending Al E. Fox for His Service to the Camrosa Water District

Objective: Commend Al E. Fox for his years of service to the Camrosa Water District.

Action Required: Adopt a resolution of the Board of Directors commending Al E. Fox for his service on the District's Board of Directors.

Discussion: Director Fox has informed the General Manager of his decision to resign, and his last board attendance is August 18, 2022.

Resolution No: 22-13

A Resolution of the Board of Directors
of Camrosa Water District

**Commending Al E. Fox for His Service on the
District's Board of Directors**

Whereas, Al E. Fox was elected to the Camrosa Water District Board of Directors representing Division 1 in December 11, 1997; and

Whereas, Al E. Fox has served with notable distinction for a period of more than 24 years from his election to his retirement on August 18, 2022; and

Whereas, Al E. Fox has represented Division 1 as a Board Member and served as Vice-President in 2000 and 2001 and serviced as President in 2002 thru 2012; and

Whereas, Al E. Fox has served on numerous water, wastewater, and special district agency committees and boards, including American Water Works Association, Association of Water Agencies of Ventura County, Association of California Water Agencies, California Association of Sanitation Agencies, Ventura County Special Districts Association, and Ventura Regional Sanitation District; and

Whereas, Al E. Fox was instrumental in the development of non-potable water supplies to provide a renewable water resource to the District to protect against imported water restrictions, drought, and rising water rates; and

Whereas, the community served by the Camrosa Water District has and will benefit well into the future from Al E. Fox's work and dedication as a Member of the Board;

Now, Therefore, Be It Resolved that the Camrosa Water District Board of Directors commends Al E. Fox for his public service on behalf of the customers served by Camrosa Water District.

Adopted, Signed, and Approved this 18th day of August 2022.

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

(ATTEST)
Tony L. Stafford, Secretary
Board of Directors
Camrosa Water District

Board Memorandum

August 18, 2022

To: General Manager

From: Joe Willingham, I. T. & Special Projects Manager

Subject: Information Technology (IT) Plan Adoption

Objective: Adopt the District's Information Technology Plan.

Action Required: Adopt a Resolution of the Board of Directors Adopting an Information Technology Plan.

Discussion: A draft of IT Plan was presented to the Board for review at the July 14, 2022 Board meeting. The plan outlines the organization of the District's IT Department and defines the roles and responsibilities of IT staff members and contracted support. The plan also includes a comprehensive set of policies that govern the acquisition and proper use of IT systems (both planned and operational). These policies have been developed to align (at a policy level) with the recommended cybersecurity controls of the American Water Works Association (AWWA), Water Sector Cybersecurity Risk Management Guidance and the National Institute of Standards and Technology (NIST), Cybersecurity Framework. The policies in this plan are namely:

- Information Technology Procurement, Acquisition, and Support Policy
- Acceptable use of Information Systems Policy
- User Account/Password Management Policy
- Anti-Malware/Endpoint Detection and Response (EDR) Policy
- Email Policy
- Firewall Policy
- Hardware and Electronic Media Disposal Policy
- Security Incident Management Policy
- Internet Use Policy
- Log Management Policy
- Safeguarding Customer Information Policy
- Network Security and Virtual Private Network (VPN) Acceptable Use Policy and Agreement
- Bring Your Own Device (BYOD) Policy and Agreement
- Patch Management Policy
- Physical Access Control Policy
- Cloud Computing Policy
- Server Security Policy
- Social Media Acceptable Use Policy
- System Monitoring and Auditing Policy
- Vulnerability Assessment Policy

- Website Operation Policy
- Workstation Configuration Security Policy
- Wireless (WiFi) Connectivity Policy
- Telecommuting Policy and Agreement
- Data Backup and Recovery Policy
- Personal Storage Backup and Recovery Policy and Procedure
- Internet of Things Policy

Resolution No: 22-14

A Resolution of the Board of Directors
of Camrosa Water District

Adopting of an Information Technology Plan

Whereas, the District acknowledges the importance of leveraging on the effective use of Information Technology to achieve its goal of maximizing organizational productivity; and

Whereas, the District also recognizes that careful consideration must be given in the procurement and acquisition of new IT systems to control costs, ensure compatibility and future supportability; and

Whereas, the District also recognizes the importance of maintaining a strong cybersecurity posture to mitigate any risks to IT systems or illegal access or exfiltration of District or customer information; and

Whereas, this IT Plan includes policies necessary to govern both IT Acquisition and Cybersecurity and includes the following specific policies:

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

- Data Backup and Recovery Policy
- Personal Storage Backup and Recovery Policy and Procedure
- Internet of Things Policy

Now, Therefore, Be It Resolved by the Camrosa Water District Board of Directors that the attached **Camrosa Water District Information Technology Plan** is hereby adopted effective August 18, 2022.

Adopted, Signed, and Approved this 18th day of August 2022.

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

(ATTEST)
Tony L. Stafford, Secretary
Board of Directors
Camrosa Water District

Board of Directors

Al E. Fox

Division 1

Jeffrey C. Brown

Division 2

Timothy H. Hoag

Division 3

Eugene F. West

Division 4

Terry L. Foreman

Division 5

General Manager

Tony L. Stafford

Camrosa Water District Information Technology Plan

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 and Agreement ..	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.....	59
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 (IT) Plan 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, and the procedures to follow when necessary. The District will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify or amend this plan.

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 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

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 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 and Agreement

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:

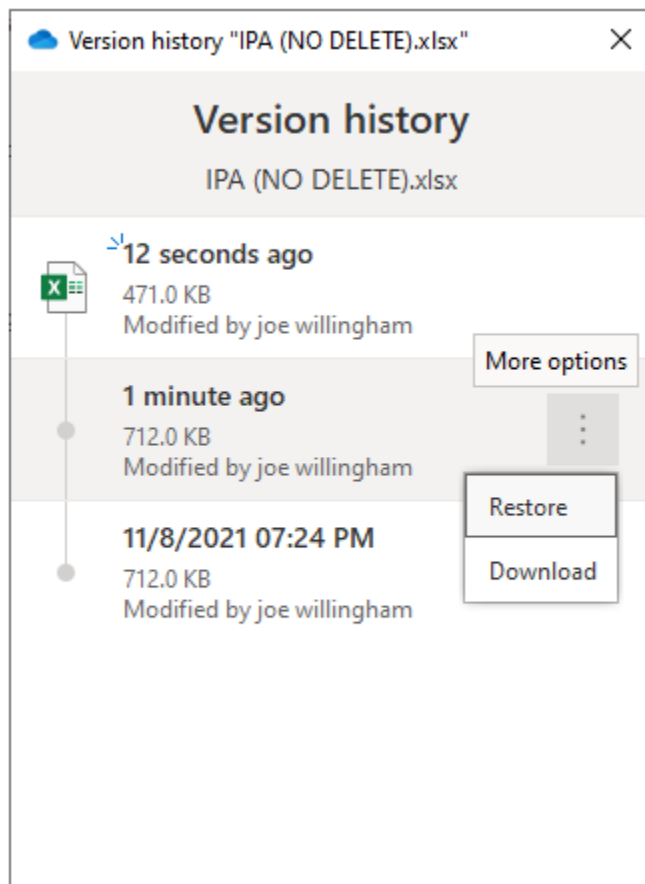
 OneDrive - camrosawater

 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:		
<u>ITEM</u>	<u>DATE CHECKED OUT</u>	<u>DATE RETURNED</u>

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

August 18, 2022

To: General Manager

From: Joe Willingham, I. T. & Special Projects Manager

Subject: Purchase Meter Transmission Units for the Zone2 MTU Upgrade CIP

Objective: Purchase a quantity of 1,850, Model 3451, Meter Transmission Units (MTUs) from Aclara as part of the Fiscal Year 2022-23, AMR AclaraOne + MTU Upgrade Zone 2 capital improvement project.

Action Required: Authorize the General Manager to issue a purchase order with Aclara Technologies (a division of Hubbell Inc.), in an amount not to exceed \$216,450.00, for purchase of quantity 1,850, Model 3451 MTUs.

Discussion: As part of the AMR AclaraOne + MTU Upgrade Zone 2 Capital Improvement Project (CIP), all 1,450 MTUs in the District's potable pressure zone 2 will be upgraded to the latest model MTU which provides hourly reads and a 30-day read-caching feature. This upgrade will allow staff to perform daily production vs. usage analysis within pressure zone 2. This capability will provide for data analytics utilization to better find and reduce water loss, determine water use patterns, and improve other operational and infrastructure issues. This will assist in reclaiming lost water revenue.

This purchase also includes a quantity of 400 MTUs which will be installed in the Camarillo Springs area, which are still read manually.

This is an approved project in the Fiscal Year 2022-23 CIP budget.



Quotation

Quote #:
Created Date:
Expiration Date:

Q-23660-1
8/4/2022 12:36 PM
3/25/2022

Aclara

77 West Port Plaza, Suite 500
St. Louis, MO 63146
US
Phone: (800) 297-2728

Bill To

Jozi Scholl
Camrosa Water District (CA)
7385 Santa Rosa Rd
Camarillo, CA 93012
(805) 256-3330
(805) 987-4797
jozis@camrosa.com

End Customer

Camrosa Water District (CA)

Prepared By	Phone	EMAIL	PAYMENT METHOD
J.D. McQuiston		jmcquiston@hubbell.com	Net 30

Water MTUs

Product Description	Part No.	Qty	Net Unit Price	Extended Price
Series 3450 Water MTU: Encoder, Single Port, Extended Range, 1' Badger Twist Tight Connector Cable	3451-801-DBW	1,850	USD 117.00	USD 216,450.00

Sub-Total	USD 216,450.00
------------------	-----------------------

Total	USD 216,450.00
--------------	-----------------------

Notes

Camrosa 3450 Series MTU Quote Q-21630

TERMS & CONDITIONS

General Note:

This Proposal/Quotation is based upon the terms and conditions set forth in the Aclara Standard Terms and Conditions of Sales for Equipment and certain services that are available on Aclara's website at:

<http://www.aclara.com/terms-and-conditions/>

1. **ADDITIONAL TERMS:**
Each Line Item will be shipped within the number of weeks staged after receipt of an acceptable order.
2. This quotation is based upon receipt and acceptance of an order by the earlier of the Expiration Date in the upper right or 60-days after the Proposal Date contained herein.
3. Seller shall deliver Equipment to Buyer FCA Seller's Facility or warehouse (Incoterms 2010.) Seller will arrange freight on Buyer's behalf.
4. Buyer shall pay Seller's standard Material Handling charges.
5. Sales tax will be charged unless the customer provides/has provided a valid Sales Tax Exemption or Reseller certificate.
6. Total Extended price shown excludes any applicable Sales Tax.
7. IF BUYER ACCEPTS THIS QUOTE AND WILL ISSUE ACLARA A SEPARATE PURCHASE ORDER BASED THEREON, DO NOT RETURN A SIGNED COPY OF THIS QUOTE
. RETURNING BOTH A SIGNED QUOTE AND SEPARATE PURCHASE ORDER WILL RESULT IN THE BUYER BEING BILLED FOR TWO ORDERS.

To place an order, please send a signed copy of your Purchase Order referencing this quotation to

AclaraOrders@hubbell.com

or simply reply to your sales rep via email with the fully executed PO attached.

If there is no Purchase Order, enter N/A in PO Number, your signature, and your Ship To Street Address (P.O. Box not allowed) to acknowledge that this quote form will be used in lieu of PO.

Signature:

Effective Date:

_____/_____/_____

Name (Print):

Title:

PO Number *:

* Ship To:

Street:

City, State Zip:

* If there is no purchase order, Ship To address must be entered.

Aclara Confidential / Proprietary Information

Seller's above quote is expressly made conditional on the Buyer's assent to all of the terms and conditions located at <http://www.aclara.com/terms-and-conditions/> . By issuing a Purchase Order or Order to Seller based on this Quote, Buyer hereby represents and affirms that it has reviewed and assents to these terms and conditions. ADDITIONAL TERMS CONTAINED ON ANY PURCHASE ORDER ARE HEREBY REJECTED UNLESS SPECIFICALLY AGREED TO IN WRITING BY ACLARA (SELLER) and BUYER.

Board Memorandum

August 18, 2022

To: Tony Stafford, General Manager
From: Kevin Wahl, Superintendent of Operations
Subject: Local Production Update

Objective: Receive a briefing on local water production through the fourth quarter of Fiscal Year 2021-22.

Action Required: No action necessary; for information only.

Discussion: The District tracks production of its various water sources electronically via the Supervisory Control and Data Acquisition (SCADA) system. Kevin Wahl, Superintendent of Operations, will present a report on local water production for Fiscal Year 2021-22.

Board Memorandum

August 18, 2022

To: General Manager

From: Terry Curson, District Engineer

Subject: Public Works Contract Inspection Services

Objective: Outsource construction inspection services.

Action Required: It is recommended that the Board of Directors authorize the General Manager to enter into an agreement with Cannon Corporation, in an amount not to exceed \$249,937.00, for on-call inspection services.

Discussion: With the retirement of the District's long-time construction inspector last year, Camrosa Board of Directors authorized the General Manager to negotiate a contract with Cannon Corporation for on-call inspection services in a June 10, 2021, Board Memo. This contractual arrangement has worked out well and staff recommends continuing these services on an annual basis.

The District has an extensive workload in place with several projects underway and a few more in the queue that require observation and inspection to ensure projects are built in accordance with the contract plans, specifications, and District Standards. The contract inspector began work on a part-time basis beginning July 6, 2021, and to date has been extensively involved in current projects, including:

- CWRP Chemical Feed System Rehabilitation
- Effluent Pond Rehabilitation
- Tierra Rejada Well Rehabilitation
- Reservoir 1B Communication Facility
- Pleasant Valley Well No. 2 Facility
- Development Projects (Shea Homes & misc. projects)
- Street valve and manhole raising
- CamSprings Waterline Replacement
- Penny Well
- AG 3 Tank Replacement

The not-to-exceed amount in Cannon's proposal is based on full-time status; the District will adjust the inspector's hours week to week based on the current workload.

California Public Contract Code requires that contracted construction inspectors assigned to public work's projects be paid at the prevailing rate established by the Department of Industrial Relations. Projects not directly classified as public works, such as residential developments, can be paid at a non-prevailing wage rate.

Cannon submitted a fee schedule as follows:

Job Description	Wage Classification	Rate/Hr.
Project Inspector II	Non-Prevailing Wage	\$136.00
Project Inspector II	Prevailing Wage	\$145.00

The rate includes the consultant's burden, insurance, vehicle, and mileage costs. The District Engineer will be the point of contact for the contract inspector and will coordinate capital, development, and operational projects, as needed, as well as oversee and manage the inspector's time and wage classifications payments.

Funding is available from the District's Operations Budget and has been specifically budgeted in Fiscal Year 2022-23.

**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: Cannon Corporation
1050 Southwood Drive
San Luis Obispo, CA 93401

DATE: August 18, 2022

Agreement No.: 2023-73

The undersigned Consultant offers to furnish the following: on-call construction inspection and general engineering support services on a as-needed basis.

Contract price \$: Per construction management and inspection rates (attached)
Not to exceed \$249,937.00

Contract Term: August 18, 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: Cannon Corporation

By: _____
Tony L. Stafford

By: _____
Patrick Riddell, PE

Title: General Manager

Title: Director, Construction Management
Services

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.
- 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.



July 19, 2022

Terry Curson, P.E.
District Engineer
Camrosa Water District
7385 Santa Rosa Rd.
Camarillo, CA 93012

PROJECT: COST PROPOSAL – CAMROSA WATER DISTRICT ON-CALL INSPECTION

Dear Mr. Curson:

Thank you for the opportunity to submit a cost proposal to provide inspection and construction administrative tasks for the scope of work shown below. We have based this scope of work on our recent conversations and correspondence with Camrosa Water District.

Scope of Work:

1. General construction inspection
 - a. Capital Projects
 - b. Development Projects
 - c. Operations Projects
2. Assist with other inspection related services as requested by the District

It is our understanding that this agreement will begin August 2022 and end June 2023. We understand that 80% of the time will be inspecting Capital and Operations projects with the remaining 20% reserved for inspection of development and other projects. The hourly rates for inspecting Capital and Operations projects will be under prevailing wage rates; inspecting development and other related projects will be under non-prevailing wage rates.

Cannon will provide a Construction Inspector that would be working with Camrosa Water District to provide the inspection service and report on-site observations. The total cost for this proposal is not-to-exceed \$249,937. Please see our attached staffing plan for detailed labor and rates.

Please feel free to contact me at the number or email address below if you have any questions regarding this proposal. We look forward to the opportunity to provide these inspection services for your organization.

Sincerely,

Patrick Riddell, PE
Director of Construction Management



Staffing Plan and Cost Estimate



CAMROSA FEE SCHEDULE

Cannon
1050 Southwood Drive
San Luis Obispo, CA 93401
805.544.7407
July 19th, 2022

				2022					2023						Est.	Estimated	
				July	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	Hours	Cost
Working days in Month =					8	21	21	19	21	20	19	23	20	22	22		
Role	Labor Type	Rate Distribution	Rate per Hour														
Construction Inspector III	Prevailing Wage	80%	\$145.00		50	134	134	122	134	128	122	147	128	141	141	1381	\$200,245
Construction Inspector III	Non-Prevailing Wage	20%	\$136.00		14	34	34	30	34	32	30	37	32	35	35	347	\$47,192
Total Estimated Hours				0	64	168	168	152	168	160	152	184	160	176	176	1728	
Total Estimated Cost of Labor																\$247,437	
	Basis																Estimated Cost
Reimbursable	Misc. reimbursable, field materials, photo copies, software																\$ 2,500.00
						Total Estimated Direct Expenses											\$2,500.00
Total Estimated Cost of Inspection Services																\$249,937	

Board Memorandum

August 18, 2022

To: Board of Directors

From: General Manager

Subject: Drought Update

Objective: Receive an update on the drought.

Action Required: No action necessary; for information only.

Discussion: As mandated by MWD, Camrosa remains in a Stage Three Water Supply Shortage and limits residential potable outdoor irrigation of nonfunctional turf to ten minutes per station one day a week. Commercial, Industrial, and Institutional potable water customers are prohibited from irrigating nonfunctional turf.

MWD may move all affected agencies to a “zero outdoor watering” scenario after September 1, 2022, if there is a need for more conservation. Noncompliance with the “zero outdoor watering” requirements at that time would result in moving the noncompliant agency to the volumetric pathway.

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

Staff will brief the Board on our latest conservation numbers.

Board Memorandum

August 18, 2022

To: Board of Directors

From: General Manager

Subject: Closed Session Conference with Legal Counsel – Pending Litigation

Objective: To confer with and receive advice from counsel regarding pending litigation.

Action Required: No action necessary; for information only.

Discussion: The Board will enter into closed session to confer regarding pending litigation pursuant to Government Code 54956.9(d)(4).



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. Change Order Listing
- B. 2022 Board Calendar

CURRENT PROJECT CHANGE ORDERS												
Project #	PW/Agreement#	Project	Total Budget	Available Budget	Contractor	Award Date	Brd/Gmgr	Change Order	Original Bid	Negotiated Value	Scope of Services/Change Order Description	
900-18-01		CWRF Chemical Storage & Feed System	\$ 1,057,500.00	\$ 40,090.32								
	2019-58				Cannon Corporation	12/13/2018 BD			\$ 100,705.00	\$ 71,765.00	engineering services to rehabilitate the CRWF's chemical storage and feed system- Originally a combined project to include equipment storage shed. The project scope was reduced to eliminate storage shed and price for the Chemical Feed System was negotiated.	
						9/19/2019 GM		CO #1	\$ 1,700.00	\$ 1,700.00	Engineeering for 3 additional pumps	
						12/12/2019 BD		CO #2	\$ 24,553.00	\$ 18,944.00	Construction support services	
						6/23/2020 GM		CO #3	\$ 4,407.00	\$ 4,407.00	Construction support services	
										\$ 96,816.00		
	S 19-05				Travis Ag	12/12/2019 BD			\$ 747,862.00	\$ 747,862.00	Construction	
						5/26/2020 GM		CO #1	\$ 5,520.00	\$ 5,520.00	Modify single to dual chemical feed pump	
						8/28/2020 GM		CO #2	\$ 2,840.00	\$ 2,840.00	Provide additional skid mounting supports (total of 16)	
						2/16/2021 GM		CO #3	\$ 8,335.02	\$ 7,324.51	Provide Foundation Soil Stability for Canopy Footing	
						11/23/2021 GM		CO #4	\$ 11,335.55	\$ 11,335.55	Install 2 additional 4inch flange on top of tanks fosr ultrasonic sensor installation	
										\$ 774,882.06		
900-18-03		Effluent Pond Relining	\$ 1,501,500.00	\$ 215,365.90								
	2017-30				MNS Engineers, Inc	7/27/2017 BD			\$ 71,988.00	\$ 69,208.00	Award and up to \$14,000 out-of-scope	
						7/27/2017 GM		CO #1	\$ 7,165.00	\$ 7,165.00	Geotechnical Investigations (Included in 7/27/20 BM)	
						7/27/2017 GM		CO #2	\$ 1,380.00	\$ 1,380.00	Groundwater management alternatives (Included in 7/27/20 BM)	
						2/28/2019 BD		CO #3	\$ 19,795.00	\$ 19,795.00	Additional project elements, slope stabilization and surface water management	
						5/28/2020 BD		CO #4	\$ 11,330.00	\$ 11,330.00	Services to amend and update plans and specs	
						5/13/2021 BD		CO#5	\$ 15,355.00	\$ 15,355.00	Engineering support services during construction	
										\$ 124,233.00		
											uuuuuuuuuwb	
					Oakridge Geoscience, Inc.	5/13/2021 BD				\$ 22,200.00	compaction and material testing services	
						10/11/2021 GM		CO#1	\$ 3,360.00	\$ 3,360.00	supplemental materials testing services	
										\$ 25,560.00		
	RW21-01				BOSCO Constructors, Inc.	5/13/2021 BD			\$ 1,055,401.00	\$ 1,055,401.00	Construction of CWRF Effluent Storage Basin Improvements	
						1/6/2022 GM		CO #1		\$ 2,746.03	Grinding and patching existing catch basin	
						1/6/2022 GM		CO #2		\$ 7,968.23	Install Concrete Curb in lieu of Berm	
										\$ 1,066,115.26		
900-18-02		CWRF Dewatering Press	\$ 2,158,000.00	\$ 1,994,063.42								
	2017-33				MNS Engineers, Inc.	8/31/2017 BD			\$ 97,932.00	\$ 97,932.00	Award and up to \$10,000 contingency	
						12/8/2017 GM		CO #1	\$ 5,370.00	\$ 5,370.00	Surveying services	
						5/28/2020 BD		CO #2	\$ (44,900.00)	\$ (44,900.00)	Credit	
						5/28/2020 BD		CO #3	\$ 87,911.00	\$ 87,911.00	professional engineering services to amend and update existing plans and specifications	
						9/24/2020 BD		CO #4	\$ 24,670.00	\$ 24,670.00	Modify plans to rotate solids handling building 90 degrees	
										\$ 170,983.00		
650-15-01		PV Well (Lynwood Well)	\$ 5,967,000.00	\$ 347,021.14								
	2014-56				Perliter & Ingalsbe	10/22/2014 BD			\$ 156,600.00	\$ 156,600.00	Award and to amend up to \$15,000 for out-of-scope	
						5/26/2015 GM		CO #1	\$ 2,950.00	\$ 2,950.00	Additional work field locating	
						11/15/2016 GM		CO #2	\$ 3,821.00	\$ 3,821.00	PV well rendering	
						11/7/2017 GM		CO #3	\$ 14,922.00	\$ 14,922.00	Prepare Pre-bid documents for pump and motor	
						7/26/2018 BD		CO #4	\$ 8,826.00	\$ 8,826.00	Construction services to pump only installation	
						12/12/2019 BD		CO #5	\$ 34,956.00	\$ 34,956.00	Review iron and manganese filter & finalize contract plans & specs	
						9/2/2020 GM		CO #6	\$ 3,090.00	\$ 3,090.00	T&M Future FE/MN revisions	
						3/11/2021 BD		CO #7	\$ 4,935.00	\$ 4,935.00	Finalize plans and specifications	
						3/11/2021 BD		CO #8	\$ 795.00	\$ 795.00	engineering design of the removal of filters and reconfiguration of the diesel generator	
						3/11/2021 BD		CO #9	\$ 7,182.00	\$ 7,182.00	engineering design of the removal of filters and reconfiguration of the diesel generator	
						6/24/2021 BD		CO #10	\$ 76,062.00	\$ 76,062.00	engineering & construction support services	
						1/13/2022 BD		CO #11	\$ 55,803.00	\$ 55,803.00	construction support services- additonal work	
									\$ 369,942.00	\$ 369,942.00		
					Unified Field Services	6/24/2021 BD			\$ 2,965,198.00	\$ 2,965,198.00	PV Well construction services	
						2/15/2022 GM		CO #1	\$ -	\$ -	Add 23 working days no cost	
						5/31/2022 GM		CO#2	\$ 18,515.19	\$ 18,515.19	PLC cost sharing	
										\$ 2,983,713.19		
					American Public Works Consulting Engineers	6/24/2021 BD				\$ 68,200.00	construction management services	
						5/3/2022 GM		CO #1		\$ 15,500.00	construction management services @ 100 hours	
										\$ 83,700.00		
					Golden State Labor Compliance	7/16/2015 GM				\$ 3,900.00	labor compliance support	
						7/26/2018 BD		CO #1		\$ 4,700.00	labor compliance support	
						6/24/2021 BD		CO#2		\$ 24,500.00	labor compliance support	
						5/3/2022 GM		CO# 3		\$ 9,024.00	labor compliance support	
										\$ 42,124.00		
600-20-02		Conejo Wellfield Treatment	\$ 11,275,000.00	\$ 1,021,101.21								
	2020-86				Provost & Pritchard	6/11/2020 BD			\$ 437,000.00	\$ 375,000.00	GAC Engineering Design	
						9/4/2020 GM		CO#1	\$ 5,000.00	\$ 5,000.00	alternative design evaluation	
						9/29/2020 GM		CO#2	\$ 7,000.00	\$ 7,000.00	second survey for modified footprint and land acquisition	
						2/25/2021 BD		CO#3	\$ 58,200.00	\$ 58,200.00	Environmental compliance	
						10/14/2021 BD		CO#4	\$ (10,200.25)	\$ (10,200.25)	Enviromental compliance credit	
						10/14/2021 BD		CO#5	\$ 10,200.25	\$ 10,200.25	Phase CDFW/MMRP	
										\$ 445,200.00		

900-20-01	CWRF Emergency Generator Fuel Tank	\$	288,000.00	\$	49,242.60
800-20-02	Pump Station #2 Generator Fuel Tank	\$	363,000.00	\$	7,810.57
2020-80					
	Cannon	4/9/2020 BD			
		2/11/2021 BD	CO#1	105,382.00 \$	95,772.00 Engineering design services
				25,072.00 \$	12,734.00 Construction support services
				\$	108,506.00
	Noho Constructors	2/11/2021 BD		297,701.00 \$	297,701.00 installation emergency standby generator and replacement fuel tank
		5/20/2021 GM	CO#1	2,667.00 \$	2,667.13 undergrounding conduits
		8/30/2021 GM	CO#2	2,360.00 \$	2,360.00 exchange 8 OCAL LB fittings for 8 OCAL explosion fittings
		12/7/2021 GM	CO#3	644.00 \$	644.00 drill and anchor an all-thread rod for pull test
		4/4/2022 GM	CO#4	3,784.06 \$	3,784.06 upsize fuel supply & return, fuel price differential, credit fuel dispensing equipment
				\$	307,156.19
400-20-02	Reservoir 1B Comm Facility	\$	670,000.00	\$	23,038.14
	Cannon	10/24/2019 BD		\$	70,752.00 Design services for various communication improvements at Res1B radio site
		7/22/2021 BD	CO# 1	\$	14,268.00 construction support services
				\$	85,020.00
PW 21-02					
	Noho	7/22/2021 BD		\$	505,101.00 Rehailitate Reservoir 1B Communication Facility
		8/2/2022 GM		\$	15,346.06 Various out of scope improvements, demo install fencing, raise pull box
				\$	520,447.06
650-22-02	Tierra Rejada Well	\$	475,000.00	\$	16,461.52
	Hopkins Groundwater Consultants	11/16/2020 GM		3,960.00 \$	3,960.00 Task 1 Well Information Review and Analysis
		2/1/2021 GM	CO#1	12,720.00 \$	12,720.00 Task 2,3,& 4
		6/25/2021 GM	CO#2	3,540.00 \$	3,540.00 Technical Support. Review update specifications Task 5
		7/14/2021 GM	CO#3	3,240.00 \$	3,240.00 Additional technical support Task 2 & Task 3
		12/9/2021 BD	CO#4	5,490.00 \$	5,490.00 Additional inspection services/spinner overview
		5/26/2022 BD	CO#5	17,810.00 \$	17,810.00 Additional hydrogeological Design/Inspection Services
				\$	46,760.00
	General Pump	8/15/2021 BD		\$	222,223.00 Rehabilitation of Tierra Rejada Well
		10/21/2021 GM	CO#1	\$	950.00 Conduct dynamic video and provide report
		12/9/2021 BD	CO#2	\$	32,925.50 Additional cleaning
		12/9/2021 BD	CO#3	\$	29,765.73 additional pump installation/removal
		6/29/2022 BD	CO#4	\$	139,733.00 cleanding and redevelopment
				\$	425,597.23
2021-106	Construction Inspection Services	\$	150,000.00		
	Cannon	6/10/2022 BD		\$	150,000.00 Construction Inspection Services
		6/8/2022 GM	CO#1	\$	20,000.00 Construction Inspection Services
				\$	170,000.00
600-20-02	Conejo Wellfied Treatment	\$	11,275,000.00	\$	1,021,101.21
	James C. Cushman, Inc.	11/18/2021 BD		\$	5,792,150.00 GAC construction
		8/9/2022 GM	CO#1	\$	4,184.00 Drain inlet box
				\$	5,796,334.00

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)						
						1				1	2	3	4	5			1	2	3	4	5	February 21 st - President's Day					
2	3	4	5	6	7	8	6	7	8	9	10	11	12	6	7	8	9	10	11	12	May 30 th - Memorial Day						
9	10	11	12	13	14	15	13	14	15	16	17	18	19	13	14	15	16	17	18	19	July 4 th - Independence Day						
16	17	18	19	20	21	22	20	21	22	23	24	25	26	20	21	22	23	24	25	26	September 5 th - Labor Day						
23	24	25	26	27	28	29	27	28						27	28	29	30	31			November 11 th - Veteran's Day						
30	31																				November 24 th & 25 th - Thanksgiving						
																					December 23 rd & 26 th - Christmas						
																					December 30 th - New Year's Eve						
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						
					1	2	1	2	3	4	5	6	7	5	6	7	8	9	10	11	ACWA Spring Conf. (Sacramento) - May 3 rd - 6 th						
3	4	5	6	7	8	9	8	9	10	11	12	13	14	12	13	14	15	16	17	18	CASA 67th Annual Conf. (Squaw Creek) - Aug. 10 th - 12 th						
10	11	12	13	14	15	16	15	16	17	18	19	20	21	19	20	21	22	23	24	25	ACWA Fall Conf. (Indian Wells) - Nov. 29 th - Dec. 2 nd						
17	18	19	20	21	22	23	22	23	24	25	26	27	28	22	23	24	25	26	27	28							
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.)						
					1	2		1	2	3	4	5	6					1	2	3	Waterwise Breakfast (See yellow on calendar)						
3	4	5	6	7	8	9	7	8	9	10	11	12	13	4	5	6	7	8	9	10	AWA Board Meetings (See orange on calendar)						
10	11	12	13	14	15	16	14	15	16	17	18	19	20	11	12	13	14	15	16	17	August - DARK (No Meetings or Events)						
17	18	19	20	21	22	23	21	22	23	24	25	26	27	18	19	20	21	22	23	24	September 29 th - Reagan Library Reception						
24	25	26	27	28	29	30	28	29	30	31				25	26	27	28	29	30		**DATE ?? - Annual Symposium**						
31																					December 8 th - Holiday Mixer						
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						
						1			1	2	3	4	5					1	2	3	April 5 th						
2	3	4	5	6	7	8	6	7	8	9	10	11	12	4	5	6	7	8	9	10	June 7 th						
9	10	11	12	13	14	15	13	14	15	16	17	18	19	11	12	13	14	15	16	17	August 2 nd						
16	17	18	19	20	21	22	20	21	22	23	24	25	26	18	19	20	21	22	23	24	October 4 th						
23	24	25	26	27	28	29	27	28	29	30				25	26	27	28	29	30	31	December 6 th						
30	31																										
Camrosa Water District							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.																				
7385 Santa Rosa Road																											
Camarillo, CA 93012																											