CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

Board Agenda

Regular Meeting

Thursday, January 27, 2022
Via Teleconference
5:00 P.M.

TO BE HELD REMOTELY

In light of public health responses to the threat of COVID-19 and Governor Newsom's Executive Order N-25-20, the Camrosa office is still closed to the public. Board meetings are accessible to the public ***only*** *via web-based teleconference, as described below.*

To participate via the web to see the board meeting presentation, click https://us02web.zoom.us/j/9235309144 on your computer, tablet, or smartphone. You'll need to download and install the ZOOM app before logging on.

If you'd like to make a comment, you'll have to log in via the app so we can identify you and invite you to participate.

To listen in via phone, call **(669) 900-6833**; when prompted, enter the meeting ID: **923 530 9144**.

We are willing and able to make reasonable accommodation for individuals with disabilities. If you require assistance, please contact Ian Prichard at IanP@camrosa.com or 805.482.6562.

Call to Order

Public Comments

At this time, the public may address the Board on any item not appearing on the agenda that is subject to its jurisdiction. Persons wishing to address the Board must make themselves known directly after the Call to Order, through the chat to the host or verbally when the President asks for public comment. 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 Administrative 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 January 13, 2022**

2. ****Approve Vendor Payments**

   Objective: Approve the payments as presented by Staff.

   Action Required: Approve accounts payable in the amount of $1,018,707.26.

Primary Agenda

3. ****Review of District Investment Policy**

   Objective: Approve the District's Investment Policy.

   Action Required: Adopt a Resolution Adopting the District's Investment Policy.

4. ****Contracting Information/Operation Technology (IT/OT) Managed Services**

   Objective: Provide continuity for management of the District's informational and operational computer networks.

   Action Required: Authorize the General Manager to enter into an agreement with AllConnected of Simi Valley California for IT/OT managed services at a prorated cost not to exceed $111,297.20 for the remainder of this fiscal year (June 30, 2022), and at an annual cost of $191,873.28 for the following three years, ending June 30, 2025.

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

5. **Closed Session Conference with Legal Counsel – Personnel**

   Objective: Confer with and receive advice from counsel regarding personnel matters.

   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/

CAMROSA WATER DISTRICT

BUILDING WATER SELF-RELIANCE

January 27, 2022

Board of Directors Agenda Packet

CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

Board Minutes

Regular Meeting

Thursday, January 13, 2022
Via Teleconference
5:00 P.M.

Call to Order The meeting was convened at 5:00 P.M. as a web-based teleconference.

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

Staff: Tony Stafford, General Manager (via teleconference)
Ian Prichard, Assistant General Manager (via teleconference)
Tamara Sexton, Finance Manager (via teleconference)
Joe Willingham, I.T. and Special Projects Manager (via teleconference)
Jozi Zabarsky, Customer Service Manager (via teleconference)
Terry Curson, District Engineer (via teleconference)
Greg Jones, Legal Counsel (via teleconference)

Guest: Cindy Fanning, Fanning & Karrh (via teleconference)
Ed McCoy, representing Fairfield (via teleconference)

Public Comments

None

Consent Agenda

1. **Approve Minutes of the Special Meeting of December 9, 2021**

   The Board approved the Minutes of the Special Meeting of December 9, 2021.

   Motion: Brown **Second:** Fox
   Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

2. **Approve Minutes of the Regular Meeting of December 9, 2021**

   The Board approved the Minutes of the Regular Meeting of December 9, 2021.

   Motion: Brown **Second:** Fox
   Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

3. **Approve Vendor Payments**

A summary of accounts payable in the amount of $3,199,959.60 was provided for Board information and approval. The Board approved the payments to vendors as presented by staff in the amount of $3,199,959.60.

Motion: Brown **Second:** Fox
Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

4. **Teleconference Emergency Findings**

The Camrosa Board of Directors reconsidered the circumstances of the state of the emergency regarding COVID-19 and, having found that state and local officials continue to impose or recommend measures to promote social distancing, thereby determined to continue meeting via teleconference.

Motion: Brown **Second:** Fox
Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

Primary Agenda

5. **Reserves Reconciliation to Audited Cash & Cash Equivalents**

Cindy Fanning, Fanning & Karrh, updated the board on the District's Reserves Reconciliation to Audited Cash and Cash Equivalents for FY2019-20 and FY2020-21.

No action necessary; for information only.

6. **Real Estate Development Policy Discussion**

The Board discussed real estate developments occurring within the District service area and provided direction to staff on updating the District's policy regarding the provision of water to new real estate developments and how that fits into the District's moratorium on unmitigated demand during drought conditions.

Ed McCoy, representing Fairfield, addressed the Board.

7. **Reservoir 3C and 3D Slope Stability Analysis**

The Board authorized the General Manager to enter into an agreement with Oakridge Geoscience, in the amount of $23,800.00, to complete a geotechnical analysis of the Reservoir 3D and 3C sites.

Motion: Hoag **Second:** Fox
Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

8. **Pleasant Valley Well No. 2 Well Facility, Phase 3, Specification No. Ps 21-01**

The Board authorized the General Manager to issue a change order to Perliter & Ingalsbe, in the amount not-to-exceed $55,803.00 to provide additional engineering & construction support services, as needed.

Motion: Fox **Second:** Brown
Roll Call: Fox-Yes; Brown-Yes; Hoag-Yes; Foreman-Yes; West-Yes

9. **Grant Funding Opportunities**

Staff briefed the Board on near-term projects that may be eligible for grant funding.

No action necessary; for information only.

CLOSED SESSION: The Board cancelled the closed session to confidentially discuss litigation matters as authorized by Government code 54956.9.

10. **Closed Session Conference with Legal Counsel – Pending Litigation**

    Cancelled

Comments by General Manager

- Moving water between pump station 2 to 3 has improved reliance on local ground water and reduced the need to purchase imported water. However, moving well water into areas that historically received mostly, if not entirely, imported water has caused customers to contact the District regarding changes in water aesthetics (water quality, as regards primary MCLs, remains unchanged). Staff address these complaints as they come in, using the opportunity to educate customers about self-reliance.

Comments by Directors

- Director Fox reminded all of the upcoming AWA meetings.

Adjournment

There being no further business, the meeting was adjourned at 5:51 P.M.

_____	_____ (ATTEST)
Tony L. Stafford, Secretary/Manager	Eugene F. West, President
Board of Directors	Board of Directors
Camrosa Water District	**Camrosa Water District**

CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

Board Memorandum

January 27, 2022

To: General Manager

From: Sandra Llamas, Sr. Accountant

Subject: **Approve Vendor Payments**

Objective: Approve the payments as presented by Staff.

Action Required: Approve accounts payable in the amount of $1,018,707.26.

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

Payroll PR 1-1, 2022	$ 44,888.61
Accounts Payable 01/06/2022-01/19/2022	$ 973,818.65
Total Disbursements	$ 1,018,707.26

DISBURSEMENT APPROVAL

BOARD MEMBER DATE

BOARD MEMBER DATE

BOARD MEMBER DATE

Tony L. Stafford, General Manager

Month of : December-21

CAL-Card Monthly Summary

Date Purchased	Statement Date	Vendor Name	Purchase Total	Item Description	Staff
12/13/21	12/22/21	Amazon	$513.20	SCADA Server Racks	KW
12/10/21	12/22/21	Amazon	$135.12	SCADA KVM Switch	KW
12/10/21	12/22/21	Amazon	$479.00	Gate Closer Remotes	KW
12/08/21	12/22/21	Smart & Final	$170.57	Kitchen Supplies	KW
11/26/21	12/22/21	Home Depot	$423.80	Lynnwood Well	KW
11/24/21	12/22/21	ScadaMetrics	$1,272.82	Production Meter Communication	KW
12/14/21	12/22/21	Grainger	$81.84	Gaskets for RMWTP	JS
12/09/21	12/22/21	Valvoline	$85.75	Oil change for truck 37	JS
11/24/21	12/22/21	ColeParmer	$32.61	Lab Supplies	GM
12/14/21	12/22/21	California Water Environme	$675.00	P3S Conference	GM
12/15/21	12/22/21	Valvoline	$123.64	Oil Change	GM
12/17/21	12/22/21	Environmental Resources	$279.15	Lab Supplies	MP
12/16/21	12/22/21	adobe	$29.99	stock imagery for website/social media	IP
12/02/21	12/22/21	Thinking2	$80.00	web site hosting	IP
11/30/21	12/22/21	zoom	$89.94	teleconferencing for Board & staff meetings	IP
12/07/21	12/22/21	Surfside Prints	$131.89	Camrosa Hats	CP
12/03/21	12/22/21	Coastal Pipco	$170.53	Blind Flanges for CL2 tanks at CWRF	CP
12/13/21	12/22/21	The Wharf	$220.89	Safety Boots	JK
11/26/21	12/22/21	Central Communications	$397.75	After-Hours Call Center	JZ
12/06/21	12/22/21	Lowe's	$229.36	Lobby lights	JZ
12/12/21	12/22/21	Amazon	$128.60	Lobby cash registers	JZ
12/13/21	12/22/21	Amazon	$48.04	Lobby monitor arms	JZ
12/19/21	12/22/21	Amazon	$255.22	Lobby monitors	JZ
12/21/21	12/22/21	Amazon	$289.58	Meter parts/repair (gelcaps)	JZ
12/22/21	12/22/21	Central Communications	$412.75	After-Hours Call Center	JZ
12/16/21	12/22/21	CSMFO	$350.00	Virtual Conference	SLL
12/22/21	12/22/21	Verizon wireless	$76.45	Chargers for tablets	CC
12/15/21	12/22/21	CWEA	$50.00	Electrical / Instrumentation Certification Training	BR
12/10/21	12/22/21	Guanglianda Cadre	$5.00	CAD Read Only Software (1month non-reoccurring)	BR
12/06/21	12/22/21	CWEA	$195.00	Electrical / Instrumentation Grade 2 exam fee	BR
12/06/21	12/22/21	CWEA	$195.00	Collections System Maintenance Grade 2 exam fee	BR
11/30/21	12/22/21	AirGas USA	$198.87	Well sounding equipment	BR
11/26/21	12/22/21	AutoZone	$32.11	Parts and supplies for Honda generators	BR
11/26/21	12/22/21	CVS	$27.95	Stationery	BR
11/22/21	12/22/21	Amazon	$48.90	Wire magnets for CWRF PLC cabinet	BR
12/17/21	12/22/21	THE HOME DEPOT	$279.56	Dewalt Cut off tool/Towels/Tapcon Hexhead screws/mis	MS
12/20/21	12/22/21	Oil Stop	$66.16	Vehicle Service	TS
12/07/21	12/22/21	sparkling image	$56.99	monthly vehicle wash	TS
11/26/21	12/22/21	Spectrum Internet	$1,249.00	Spectrum Internet (200Mbps increased bandwidth)	JW
12/11/21	12/22/21	Callfire.com	$99.00	online IVR - Delinquent Call Out (Monthly Service Fee)	JW
12/19/21	12/22/21	Spectrum Cable News	$77.29	Cable TV News Service (2 Cable box feeds) monthly service fee	JW
12/13/21	12/22/21	Boot Barn	$161.61	Safety Boots	KK
12/13/21	12/22/21	The home depot	$114.08	Parts for CWRF	KK
12/08/21	12/22/21	Harbor freight	$252.02	Tools for truck	KK
11/30/21	12/22/21	The home depot	$48.75	Tools for truck	KK
12/03/21	12/22/21	Amazon	$22.97	Charge in error. Employee Reimbursement	TDS
12/06/21	12/22/21	Amazon	$19.29	Charge in error. Employee Reimbursement	TDS
12/07/21	12/22/21	Amazon	$46.79	Charge in error. Employee Reimbursement	TDS
12/07/21	12/22/21	Amazon	$21.42	Charge in error. Employee Reimbursement	TDS
11/25/21	12/22/21	Staples	$320.68	Premium Membership	DA
12/13/21	12/22/21	VC Metals	$29.63	Lab Counter Top Bracket	CS
12/09/21	12/22/21	VC Metals	$179.30	UPS Brackets x 4	CS
12/08/21	12/22/21	Lowes	$94.73	Bins for Brandon/Brian	CS
12/09/21	12/22/21	Big 5	$183.16	EZ Up for Rain Work	CS
12/03/21	12/22/21	Batteries Plus	$163.46	Unit #23 Truck Battery	CS
			$11,422.21		

Camrosa Water District

Accounts Payable Period:

01/06/2022-01/19/2022

Expense	Account Description	Amount
11100	Accounts Rec-Other	110.47
15773	Deferred Outflows-UAL Prep.	
11700	Meter Inventory	
11900	Prepaid Insurance	
11905	Prepaid Maintenance Ag	
13000	Land	
13400	Construction in Progress	413088.09
20053	Current LTD Bond 2016	
20052	Current LTD Bond 2012	
20400	Contractor's Retention	-12738.55
20250	Non-Potable Water Purchases	
23001	Refunds Payable	2809.47
50110	Payroll FLSA Overtime-Retro	
50010	Water Purchases & SMP	278332.66
50020	Pumping Power	142827.57
50100	Federal Tax 941 1st QTR	
50140	Unemployment	
50153	Social Security Tax	
50200	Utilities	17025.91
50210	Communications	3286.28
50220	Outside Contracts	39839.86
50230	Professional Services	7645.04
50240	Pipeline Repairs	16872.73
50250	Small Tool & Equipment	1892.42
50260	Materials & Supplies	24981.31
50270	Repair Parts & Equip Maint	10390.46
50280	Legal Services	2048.63
50290	Dues & Subscriptions	281.00
50300	Conference & Travel	1114.94
50310	Safety & Training	959.37
50330	Board Expenses	
50340	Bad Debt	
50350	Fees & Charges	18051.00
50360	Insurance Expense	
50500	Misc Expense	
50600	Fixed Assets	4999.99
50700	Interest Expense	
	TOTAL	**$973,818.65**

Expense Approval Report

Camrosa Water District, CA

By Vendor Name

Payable Dates 1/6/2022 - 1/19/2022 Post Dates 1/6/2022 - 1/19/2022

Payment Numb	Post Date	Vendor Name	Payable Number	Description (Item)	Account Name	Purchase Or	Amount
46	01/18/2022	INTERA INCORPORATED	122124	Santa Rosa GSP	Prof services	FY22-0136	23420
TOTAL VENDOR PAYMENTS-GSA							**$ 23,420.00**
Vendor: *CAM* - DEPOSIT ONLY-CAMROSA WTR							
3311	01/13/2022	DEPOSIT ONLY-CAMROSA WTR	1-13-22-AP	Transfer to Disbursements Account -AP	Transfer to disbursements-holdi		883000
3312	01/13/2022	DEPOSIT ONLY-CAMROSA WTR	1-13-22-PR	Transfer to Disbursements Account-PR	Transfer to disbursements-holdi		158000
					Vendor *CAM* - DEPOSIT ONLY-CAMROSA WTR Total:		**1041000**
57546	01/19/2022	ACLARA TECHNOLOGIES	22100025	Maintenance Support - Aclara	Outsd contracts		8748
57547	01/18/2022	AMERICAN PUBLIC WORKS CONSULTING ENGINEERS, LI	2021-5	PV Well No. 2 Project Management Services	Construction in progress	FY22-0011	2790
Vendor: APE01 - APEX GENERAL CONTRACTORS, INC.							
57548	01/13/2022	APEX GENERAL CONTRACTORS, INC.	2139-04	Lobby Remodel	Construction in progress	FY22-0074	16603
57548	01/13/2022	APEX GENERAL CONTRACTORS, INC.	2139-04 Retentior	Retention on Invoice ref# 2139-4	Contractor's retention		-978.35
					Vendor APE01 - APEX GENERAL CONTRACTORS, INC. Total:		**15624.65**
57549	01/19/2022	BADGER METER INC	1481950	Meters	Repair Parts & Equipment Maint	FY22-0122	2629.01
57550	01/17/2022	BRENNTAG PACIFIC, INC.	BPI280840	Materials & Supplies - Chemicals RMWTP	Materials & Supplies-RMWTP		5923.89
57551	01/17/2022	CALIF WATER ENVIRONMENT ASSOCIATION	60913-Renewal	Dues & Subscriptions Customer Ref#60913	Dues & subscrip		91
Vendor: CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT							
930	01/17/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	129621	Water Purchase-Potable	Water purchases-Potable		170993.99
930	01/17/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	129621	Water Purchase	CMWD Fixed Charges		78026
930	01/17/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	129621	Water Purchase-NP	Water purchases Non Potable		13783.03
930	01/17/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	SMP122821	SMP CMWD- SMP Pipeline Fee	SMP CWD-RMWTP		14447.64
930	01/17/2022	CALLEGUAS MUNICIPAL WATER DISTRICT	SMP122821	SMP CMWD- SMP Pipeline Fee	SMP CMWD		1082
					Vendor CAL03 - CALLEGUAS MUNICIPAL WATER DISTRICT Total:		**278332.66**
Vendor: CAN03 - Cannon Corporation							
57552	01/19/2022	Cannon Corporation	78921	Design Generator and Fuel Tank	Construction in progress	FY20-0256-R	406
57552	01/19/2022	Cannon Corporation	78991	Reservoir 1B Communication Upgrades	Construction in progress	FY21-0035-R	1570.1
57552	01/19/2022	Cannon Corporation	79101	Contract Inspection Services	Outsd contracts	FY22-0081	290
57552	01/19/2022	Cannon Corporation	79102	Contract Inspection Services	Outsd contracts	FY22-0081	580
57552	01/19/2022	Cannon Corporation	79103	Contract Inspection Services	Outsd contracts	FY22-0081	2030
57552	01/19/2022	Cannon Corporation	79104	Contract Inspection Services	Outsd contracts	FY22-0081	125
57552	01/19/2022	Cannon Corporation	79105	Contract Inspection Services	Outsd contracts	FY22-0081	4859.25
57552	01/19/2022	Cannon Corporation	79106	Contract Inspection Services	Outsd contracts	FY22-0081	8494.5
					Vendor CAN03 - Cannon Corporation Total:		**18354.85**
57553	01/14/2022	CITY OF THOUSAND OAKS	1101-10122	Sewer Services for Read Rd Tract-City TO	Outsd contracts		1078.2
57554	01/17/2022	COUNTY OF VENTURA PUBLIC WORKS	327987	Annual Excavation Permit	Fees & charges		1625
Vendor: EJH01 - E.J. HARRISON & SONS INC							
57555	01/17/2022	E.J. HARRISON & SONS INC	5386	Trash Removal - CWRF	Outsd contracts		494.59
57555	01/17/2022	E.J. HARRISON & SONS INC	813	Trash Removal - Role Off Bins	Outsd contracts		803.04
					Vendor EJH01 - E.J. HARRISON & SONS INC Total:		**1297.63**
931	01/18/2022	ENTERPRISE FLEET SERV INC	FBN4374139	Vehicle Lease - January 2022	Outsd contracts		7178.77

Vendor: FAM01 - FAMCON PIPE & SUPPLY, INC							
57556	01/17/2022	FAMCON PIPE & SUPPLY, INC	S100069911-001	Angle Meterstops	Repair parts & equipment		952.38
57556	01/17/2022	FAMCON PIPE & SUPPLY, INC	S100070289-001	Tools for Truck 36	Small tools & equipment		171.6
					Vendor FAM01 - FAMCON PIPE & SUPPLY, INC Total:		**1123.98**
Vendor: FRU01 - FRUIT GROWERS LAB. INC.							
57557	01/14/2022	FRUIT GROWERS LAB. INC.	116588A	Outside Lab Analysis	Materials & supplies		172
57557	01/14/2022	FRUIT GROWERS LAB. INC.	118248A	Outside Lab Analysis	Outsd contracts		54
57557	01/19/2022	FRUIT GROWERS LAB. INC.	200045A	Outside Lab Work	Outsd contracts		109
57557	01/19/2022	FRUIT GROWERS LAB. INC.	200135A	Outside Lab Work	Outsd contracts		109
57557	01/19/2022	FRUIT GROWERS LAB. INC.	200200A	Outside Lab Work	Outsd contracts		109
57557	01/19/2022	FRUIT GROWERS LAB. INC.	200273A	Outside Lab Work	Outsd contracts		109
					Vendor FRU01 - FRUIT GROWERS LAB. INC. Total:		**662**
57558	01/17/2022	GEIGER ENTERPRISES, INC.	22132	Materials & Supplies - Fuel Pond 1	Materials & supplies		741.25
Vendor: GEN06 - GENERAL PUMP COMPANY, INC							
57559	01/19/2022	GENERAL PUMP COMPANY, INC	29047	Cleaning and Rehabilitation Penny Well	Construction in progress	FY22-0185	81251.93
57559	01/17/2022	GENERAL PUMP COMPANY, INC	29051	Rehabilitate Conejo Wells #2 #3 #4 and SR #8	Construction in progress	FY22-0163	4848
					Vendor GEN06 - GENERAL PUMP COMPANY, INC Total:		**86099.93**
57560	01/13/2022	HATHAWAY, PERRETT,WEBSTER, POWERS & CHRISMAN	115514	Legal Services	Legal services		2048.63
57561	01/17/2022	Janitek Cleaning Solutions-Allstate Cleaning, Inc.	43344A	Cleaning Service-Janitorial Services	Outsd contracts		1772
57562	01/13/2022	JIE CHEN	00008978	Deposit Refund Act 8978- 82 Calle Cataluna	Refunds payable		25.98
57563	01/13/2022	JUSTIN HAMES	00002157	Deposit Refund Act 2157 - 251 Calle Amorosa	Refunds payable		65.6
57564	01/13/2022	MARK RODDY	00000008-3	Fire Hydrant Meter Deposit Refund - FH#8	Refunds payable		668.61
Vendor: MCM01 - McMASTER-CARR SUPPLY CO							
57565	01/17/2022	McMASTER-CARR SUPPLY CO	70791939-Credit	Hardware Returned - Credit	Materials & supplies		-110.57
57565	01/17/2022	McMASTER-CARR SUPPLY CO	70791950-Credit	Fuses Returned- Credit	Materials & supplies		-68.43
57565	01/17/2022	McMASTER-CARR SUPPLY CO	70806746	Tools for Brandon Truck	Small tools & equipment		638.41
57565	01/18/2022	McMASTER-CARR SUPPLY CO	71335714	Materials & Supplies - Brass Fittings	Materials & supplies		395.58
					Vendor MCM01 - McMASTER-CARR SUPPLY CO Total:		**854.99**
57566	01/13/2022	MICHAEL ANTRIM	00000269	Refund Overpayment Active Act 269 - 312 Appletree	Refunds payable		1072.01
Vendor: MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC.							
57567	01/18/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	10100	AWIA ERP	Prof services	FY22-0107	1565.04
57567	01/18/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	10122	GAC Project Management	Construction in progress	FY21-0120-R	3513.33
57567	01/18/2022	MICHAEL K. NUNLEY & ASSOCIATES, INC.	10125	GAC Construction Management	Construction in progress	FY22-0151	760.14
					Vendor MKN01 - MICHAEL K. NUNLEY & ASSOCIATES, INC. Total:		**5838.51**
Vendor: MNS01 - MNS ENGINEERS, INC.							
57568	01/18/2022	MNS ENGINEERS, INC.	79221	Engineering Support services during construction	Construction in progress	FY21-0254-R	87.5
57568	01/18/2022	MNS ENGINEERS, INC.	79222	Out of Scope Work	Construction in progress	FY18-0055-R	631.25
57568	01/18/2022	MNS ENGINEERS, INC.	79339	Penny Well Entrained Air Engineering Services	Construction in progress	FY22-0121	50181
57568	01/18/2022	MNS ENGINEERS, INC.	79391	Out of Scope Work	Construction in progress	FY18-0055-R	806.25
57568	01/18/2022	MNS ENGINEERS, INC.	79523	Out of Scope Work	Construction in progress	FY18-0055-R	575
					Vendor MNS01 - MNS ENGINEERS, INC. Total:		**52281**
57569	01/13/2022	MONICA O'HEARN	00001659	Depsit Refund Act 1659 - 5059 Galano Dr	Refunds payable		1.15
57570	01/18/2022	NBS GOVERNMENT FINANCE GROUP	1221000093	Develop In Lieu Mitigation Fee schedule	Prof services	FY22-0104	6080
57571	01/13/2022	NICK OSTROVSKY	00010551	Deposit Refund Act 10551- 3030 Palo Verde Cir	Refunds payable		456.25

Vendor: NOH01 - NOHO CONSTRUCTORS							
57572	01/18/2022	NOHO CONSTRUCTORS	Pymt 1	Reservoir 1B communication facility	Construction in progress	FY22-0068	200000
57572	01/18/2022	NOHO CONSTRUCTORS	Pymt1-Retention 1	Retention Pymt 1-Reservoir 1B Project	Contractor's retention		-10000
57572	01/18/2022	NOHO CONSTRUCTORS	Pymt-4	CWRF - Diesel Fuel Tank Installation	Construction in progress	FY21-0220-R	35204
57572	01/18/2022	NOHO CONSTRUCTORS	Pymt 4-Retention	Retention Payment 4	Contractor's retention		-1760.2
					Vendor NOH01 - NOHO CONSTRUCTORS Total:		**223443.8**
Vendor: NOR07 - NORTHSTAR CHEMICAL							
57573	01/17/2022	NORTHSTAR CHEMICAL	214230	Materials Chemicals - RMWTP	Materials & Supplies-RMWTP		4305.55
57573	01/18/2022	NORTHSTAR CHEMICAL	214828	Materials Chemicals - CWRF	Materials & supplies		4398.89
57573	01/18/2022	NORTHSTAR CHEMICAL	214829	Materials Chemicals RMWTP	Materials & Supplies-RMWTP		2232.27
					Vendor NOR07 - NORTHSTAR CHEMICAL Total:		**10936.71**
57574	01/19/2022	OAKRIDGE GEOSCIENCE, INC.	04-008-06	Supplemental Geotech Inspection	Construction in progress	FY22-0181	530.82
57575	01/18/2022	PERLITER & INGALSBE	18658	Engineering Support Services	Construction in progress	REQ00057-R	9344.75
57576	01/13/2022	PETER NEWMAN	00007301	Deposit Refund Act 7301 - 4547 Calle Argolla	Refunds payable		78.37
Vendor: PRI04 - PRIORITY SAFETY SERVICES							
57577	01/19/2022	PRIORITY SAFETY SERVICES	21-2036	Gas Detector Inspection	Outsd contracts		350
57577	01/19/2022	PRIORITY SAFETY SERVICES	21-2041	Gas Detector Inspection	Outsd contracts		350
					Vendor PRI04 - PRIORITY SAFETY SERVICES Total:		**700**
57578	01/17/2022	PURETEC INDUSTRIAL WATER	1946515	Deionized Water Service	Materials & supplies		72.93
57579	01/17/2022	RAYCO SECURITY LOSS PREVENTION	36691	Alarm Service	Outsd contracts		170.21
57580	01/13/2022	ROZANNE CHAVEZ	00002988	Deposit Refund Act 2988 - 5363 Maple View Cir	Refunds payable		17.15
57581	01/19/2022	RT LAWRENCE CORPORATION	46917	Processing Dec-21 Payments-Lockbox Services	Outsd contracts		764.15
57582	01/13/2022	RUMICO, LLC.	00008568-2	Final Acct Overpayment- Act 8568- 807B Camarillo S	Refunds payable		13.26
Vendor: SAM01 - SAM HILL & SONS, INC.							
57583	01/19/2022	SAM HILL & SONS, INC.	3993	1" Service Line Leak	Pipeline repairs	FY22-0194	10074.96
57583	01/19/2022	SAM HILL & SONS, INC.	3994	1' Service Line Leak	Pipeline repairs	FY22-0193	6797.77
					Vendor SAM01 - SAM HILL & SONS, INC. Total:		**16872.73**
Vendor: SCF01 - SC Fuels							
57584	01/17/2022	SC Fuels	2034510IN	Material & Supplies - Fuel	Materials & supplies		867.31
57584	01/17/2022	SC Fuels	2039344IN	Material & Supplies - Fuel	Materials & supplies		1605.95
57584	01/17/2022	SC Fuels	2040384IN	Material & Supplies - Fuel Pond 1	Materials & supplies		1251.58
57584	01/17/2022	SC Fuels	2040386IN	Material & Supplies - Fuel Pond 1	Materials & supplies		427.71
					Vendor SCF01 - SC Fuels Total:		**4152.55**
57585	01/13/2022	SLIMJIM GENERAL CONSTRUCTION	1803	Network Cabling for Customer Service Area	Construction in progress	FY22-0188	2900
Vendor: SCE01 - SOUTHERN CALIF. EDISON							
934	01/17/2022	SOUTHERN CALIF. EDISON	Jan22	Current Usage Charges	Pumping power		95062.82
934	01/17/2022	SOUTHERN CALIF. EDISON	Jan22	Current Usage Charges	Pumping Power-RMWTP		47764.75
934	01/17/2022	SOUTHERN CALIF. EDISON	Jan22	Current Usage Charges	Utilities		17025.91
					Vendor SCE01 - SOUTHERN CALIF. EDISON Total:		**159853.48**
Vendor: STA05 - STATE WATER RESOURCES CONTROL BOARD							
57586	01/13/2022	STATE WATER RESOURCES CONTROL BOARD	T2-Renewal-Jorge	Treatment Cert Renewal (T2) for Jorge Navarro	Dues & subscrip		60
57587	01/13/2022	STATE WATER RESOURCES CONTROL BOARD	D4-Exam-JorgeNa	Distribution Exam D4 for Jorge Navarro	Dues & subscrip		130
					Vendor STA05 - STATE WATER RESOURCES CONTROL BOARD Total:		**190**
Vendor: SWR01 - SWRCB-Drinking Water Program Fees							
57588	01/17/2022	SWRCB-Drinking Water Program Fees	WD0196741	CWRF Annual Discharge Permit Fee	Fees & charges		15663
57588	01/17/2022	SWRCB-Drinking Water Program Fees	WD0197308	Water System Fees	Fees & charges		763
					Vendor SWR01 - SWRCB-Drinking Water Program Fees Total:		**16426**

57589	01/17/2022	TALLEY COMMUNICATIONS	10404355	Repair Parts - Endpoint Radio Antennas	Repair parts & equipment		498.12
57590	01/19/2022	Trusted Tech Team, Inc	100649	Windows 2019 Upgrade - for existing EPYC2 Host Svr	Fixed Assets-Internal	FY22-0186	4999.99
935	01/19/2022	U.S. BANK CORPORATE	21-Dec	Charge in error. Employee Reimbursement	Accounts receivable - other		11422.21
Vendor: UNI08 - UNIFIRST CORPORATION							
57591	01/17/2022	UNIFIRST CORPORATION	328-1337019	Uniform Cleaning Service	Outsd contracts		258
57591	01/17/2022	UNIFIRST CORPORATION	328-1337026	Office Cleaning Supplies- Towe-Mat Service	Outsd contracts		64.58
57591	01/17/2022	UNIFIRST CORPORATION	328-1338916	Uniform Cleaning Service	Outsd contracts		258
57591	01/17/2022	UNIFIRST CORPORATION	328-1338923	Office Cleaning Supplies- Towe-Mat Service	Outsd contracts		66.14
57591	01/17/2022	UNIFIRST CORPORATION	328-1340847	Uniform Cleaning Service	Outsd contracts		258
57591	01/17/2022	UNIFIRST CORPORATION	328-1340854	Office Cleaning Supplies- Towe-Mat Service	Outsd contracts		66.14
					Vendor UNI08 - UNIFIRST CORPORATION Total:		**970.86**
Vendor: USA01 - USA BLUE BOOK							
57593	01/19/2022	USA BLUE BOOK	838182	Repair Parts - Well Sounding Equipment	Repair parts & equipment		814.54
57593	01/14/2022	USA BLUE BOOK	843900	Lab Supplies	Materials & supplies		291.51
57593	01/18/2022	USA BLUE BOOK	845437	PH Standard for CWRF	Materials & supplies		73.83
57593	01/19/2022	USA BLUE BOOK	848098	Flouride Standard for Drinking Water Lab	Materials & supplies		90.68
57593	01/19/2022	USA BLUE BOOK	848152	Alkalinity Standard for the Lab	Materials & supplies		132.09
57593	01/19/2022	USA BLUE BOOK	849278	Dechlor Tablets for the Diffuser	Materials & supplies		593.46
					Vendor USA01 - USA BLUE BOOK Total:		**1996.11**
57594	01/17/2022	VERIZON BUSINESS, INC	72071618	VOIP T1 (Verizon)	Communications		1226.78
Vendor: WWG01 - W W GRAINGER, INC.							
57595	01/17/2022	W W GRAINGER, INC.	9168115740	Hand Tools for Brandon's Truck	Small tools & equipment		102.2
57595	01/17/2022	W W GRAINGER, INC.	9169877967	Repair Parts - RMWTP	Repair Parts & Equipment-RMW		786.01
57595	01/17/2022	W W GRAINGER, INC.	9171099220	Hand Tools for Brandon's Truck	Small tools & equipment		980.21
57595	01/17/2022	W W GRAINGER, INC.	9172320674	Material & Supplies - Binder Chains	Materials & supplies		457.61
					Vendor WWG01 - W W GRAINGER, INC. Total:		**2326.03**
57596	01/19/2022	WIENHOFF DRUG TESTING	103429	DOT Annual Queries for Commercial Drivers	Outsd contracts		35
Vendor: \Z105 - Z POWER LLC							
57597	01/13/2022	Z POWER LLC	00000042	Deposit Refund Act 42 - 4765 Calle Quetzal	Refunds payable		349.51
57597	01/13/2022	Z POWER LLC	00006654	Deposit Refund Act 6654 - Calle Plano-Fire Service	Refunds payable		61.58
					Vendor \Z105 - Z POWER LLC Total:		**411.09**
TOTAL VENDOR PAYMENTS-CAMROSA							**$ 973,818.65**

Vendor: PER05 - CAL PERS 457 PLAN						
DFT0003726	01/13/2022	CAL PERS 457 PLAN	INV0011008	Deferred Compensation	Deferred comp - ee paid	50
DFT0003727	01/13/2022	CAL PERS 457 PLAN	INV0011009	Deferred Compensation	Deferred comp - ee paid	3404.46
					Vendor PER05 - CAL PERS 457 PLAN Total:	**3454.46**
DFT0003742	01/13/2022	EMPLOYMENT DEVELOP. DEPT.	INV0011026	Payroll-SIT	P/R-sit	4259.42
Vendor: HEA02 - HealthEquity						
DFT0003730	01/13/2022	HealthEquity	INV0011013	HSA-Employee Contribution	HSA Contributions Payable	528.84
DFT0003731	01/13/2022	HealthEquity	INV0011014	HSA Contributions	HSA Contributions Payable	250
					Vendor HEA02 - HealthEquity Total:	**778.84**
933	01/13/2022	LINCOLN FINANCIAL GROUP	INV0011010	Deferred Compensation	Deferred comp - ee paid	1958
932	01/13/2022	LINCOLN FINANCIAL GROUP	INV0011022	Profit Share Contribution	Profit share contributions	2618.42
DFT0003728	01/13/2022	PUBLIC EMPLOYEES	INV0011011	PERS-Retirement	P/R-state ret.	17388.58
Vendor: UNI10 - UNITED STATES TREASURY						
DFT0003739	01/13/2022	UNITED STATES TREASURY	INV0011023	FIT	P/R-fit	11312.01
DFT0003740	01/13/2022	UNITED STATES TREASURY	INV0011024	Payroll-Social Security Tax	P/R - ee social security	87.2
DFT0003741	01/13/2022	UNITED STATES TREASURY	INV0011025	Payroll- Medicare Tax	P/R - ee medicare	3011.68
					Vendor UNI10 - UNITED STATES TREASURY Total:	**14410.89**
57592	01/13/2022	UNITED WAY OF VENTURA CO.	INV0011007	Charity-United Way	P/R-charity	20

TOTAL PAYROLL VENDOR PAYMENTS-CAMROSA $ 44,888.61

CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

Board Memorandum

January 27, 2022

To: General Manager

From: Tamara Sexton, Manager of Finance

Subject: **Review of District Investment Policy**

Objective: Approve the District's Investment Policy.

Action Required: Adopt a Resolution Adopting the District's Investment Policy.

Discussion: Annually, the Board reviews the District's Investment Policy for adequacy and formally adopts the Policy with revisions as necessary. The Ad-Hoc Committee reviewed the Policy and there are no recommended changes. The District's Investment Policy was re-adopted with no changes in February 2021. Staff has reviewed the Policy for compliance with current regulations and has found that no changes were required by law. The Resolution and Policy are attached for re-adoption by the Board.

CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

Resolution No: 22-01

A Resolution of the Board of Directors
of Camrosa Water District

Adopting a District Investment Policy

Whereas, The Board of Directors has established a District Investment Policy to provide guidelines for the prudent investment of the District's temporarily idle cash; and,

Whereas, It is in the best interests of the District to review that investment policy from time to time to ensure maximum yield while maintaining criteria to ensure safety and liquidity; and,

Whereas, The Investment Policy has been presented to the full Board for review and comment;

Now, Therefore, Be It Resolved by the Camrosa Water District Board of Directors that the attached Investment Policy is hereby adopted and made effective this date.

Adopted, Signed, and Approved this 27th day of January 2022.

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

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

CAMROSA WATER DISTRICT
STATEMENT OF INVESTMENT POLICY
January 2022

PURPOSE:

This statement is intended to provide guidelines for prudent investment of the District's temporarily idle cash, and outline policies for maximizing efficiency of the District's cash management system. The ultimate goal is to enhance the economic status of the District while protecting its cash resources.

SCOPE:

This investment policy applies to all financial assets of the District, as well as other funds that may be created from time to time which shall also be administered in accordance with the provisions of this policy. Funds held by the Ventura County Treasurer during tax collection periods shall be governed by the County's investment policy, and are not subject to the provisions of this policy.

THE INVESTMENT PROCESS:

The investment of public funds is a professional discipline. The investment process has the following components:

- A written investment policy explicitly identifying the District's opportunities, constraints, preferences, and capabilities.
- An Investment Strategy identifying Investment opportunities and overall objectives of the District.
- A Market Analysis identifying the District’s circumstances and market conditions.
- A Portfolio Analysis identifying adjustments needed in response to changing circumstances, results and new objectives.

POLICY:

The Camrosa Water District shall invest its pooled, temporary idle cash investments in a manner that affords the District a broad spectrum of investment opportunities as long as the investment is deemed prudent and is allowable under current legislation of the State of California (Water Code Section 31303 and 31336 and Government Code Section 53600 et seq.). Investments shall be made with judgment and care, under circumstances then prevailing, which persons of prudence, discretion and intelligence, who are familiar with those matters, exercise in the management of their own affairs, not for speculation, but for investment considering the probable safety and liquidity of capital, as well as reasonable income to be derived.

The Board of Directors and the General Manager, acting in accordance with procedures and exercising due diligence, shall be relieved of personal responsibility for an individual security's credit risk or market price changes, provided that deviations from expectations are reported in a timely fashion, and appropriate actions are taken to control adverse developments.

The General Manager shall establish a system of internal controls to be reviewed by the Investment Committee and with the independent auditor. The controls shall be designed to prevent losses of public funds arising from fraud, employee error, and misrepresentation by third parties, unanticipated changes in financial markets or imprudent actions by District Staff.

INVESTMENT STRATEGY

Temporarily idle or surplus funds of the Camrosa Water District shall be invested in accordance with principles of sound treasury management and in accordance with the provisions of the California Government Code Sections 53600 et seq, the Water Code and this Investment Policy. The basic objectives of the District's investment program are, in order of priority,

1) Safety of invested funds; and
2) Maintenance of sufficient liquidity to meet cash flow needs; and
3) Attainment of the maximum return possible consistent with the first two objectives.

These objectives will be accomplished using the following procedures

1. Safety – The District shall ensure the safety of its invested funds by limiting credit and interest rate risks. Credit risk is the risk of loss due to the failure of the security issuer or backer. Interest rate risk is the risk that the market value of portfolio securities will fall due to an increase in general interest rates.

   Credit risk will be mitigated by:
   a. Limiting investments to safer types of securities; and
   b. Diversifying the investment portfolio so that the failure of any one issuer or backer will not place undue financial burden on the District; and
   c. Monitoring all of the Districts investments to anticipate and respond appropriately to a significant reduction of creditworthiness of any of the issuers. The relative health of issuers shall be evaluated by the Investment Committee at least annually.

   Interest rate risk will be mitigated by:
   a. Structuring the District's portfolio so that securities mature to meet the District's cash requirements for ongoing operations, thereby avoiding the need to sell securities on the open market prior to their maturity; and
   b. Investing primarily in short-term securities; and
   c. Occasionally restructuring the portfolio to minimize the loss of market value and/or to maximize cash flows.

2. Liquidity – The District's financial portfolio must be structured in a manner which will provide that securities mature at approximately the same time as cash is needed to meet anticipated demands. Additionally, since all possible cash demands cannot be anticipated, the portfolio should consist largely of securities with active secondary or resale markets. As a general rule, and subject to annual review by the Investment Committee, the average maturity of the investment portfolio will not exceed two (2) years. No investment will have a maturity of more than five (5) years from its date of purchase.

3. Return – The investment portfolio shall be designed with overall objective of obtaining a total rate of return throughout economic cycles, commensurate with investment risk constraints and cash flow needs.

ELIGIBLE INVESTMENT INSTRUMENTS

Camrosa shall invest only in investment instruments and media approved by Resolution of Camrosa's Board of Directors. The Board of Directors may consider additions or deletions to the approved investment instruments and media list at any time by resolution and shall include in each resolution the entire list of approved investments. This policy shall be used to evaluate recommended additions to the approved list. Additions to the approved list shall not be made unless there is a strong likelihood that the addition will be utilized within the near future. The attached Addendum contains examples of typical investment instruments which may be included on an approved list.

INVESTMENT CONSTRAINTS

General Guidelines - Temporarily idle operating cash shall be invested in instruments whose average maturity does not exceed two (2) years. Reserves established for the replacement of utility (water, sewer) facilities may be invested for a longer term if a higher yield may be achieved. Funds held for capital replacement shall be invested in securities that reasonably can be expected to produce enough income to offset inflationary construction cost increases. Such funds shall not be exposed to market price risks or default risks that would jeopardize the assets available to accomplish their stated objective. Such would be the case with obligations of the U.S. Government or its agencies.

Diversification - It is the District's policy to diversify its investment portfolio to control credit risk. Diversification strategies shall be determined and revised periodically. Maturities shall be staggered to provide for liquidity and stability of income. At least 25% of the portfolio will be invested in securities which can be liquidated on one (1) day's notice in order to control liquidity risk. No more than one-third (33%) of Camrosa's portfolio shall be held by any single investment firm or institution. The sole exception shall be the State of California Investment Pool (L.A.I.F.).

Prohibited Investments - Investments by the District in securities permitted by the California Government Code, but not specifically approved by Board Resolution is prohibited without the prior approval of the Board of Directors. The District shall not invest any funds such as inverse floaters, range notes, and other instruments outlined in California Government Code Section 53601 nor in any security that could result in zero interest if held to maturity. No representative of the District is authorized to engage in margin transactions, derivatives nor reverse repurchase agreements on behalf of the District. Finally, while it may occasionally be necessary or strategically prudent of the District to sell a security prior to maturity to either meet unanticipated cash needs or to restructure the portfolio, no investment may be made for the sole purpose of speculating or taking an unhedged position on the future direction of interest rates.

Security Dealers and Depositories - The District shall seek to conduct its investment transactions with several competing, reputable security dealers and brokers as the need may arise. The selection process shall screen out institutions that lack viability or whose past practices suggest the safety of public capital, directed to or through such firms, would be impaired.

Ethics and Conflict of Interest - Officers and employees involved in the investment process shall refrain from personal business activity that could conflict with proper execution of the investment program, or which could impair their ability to make impartial investment decisions. Such employees and investment officials shall disclose to the Board of Directors and the General Manager any material financial interests in financial institutions that conduct business within this jurisdiction, and they shall further disclose any large personal financial investment positions that could be related to the performance of the District's

portfolio. Such employees and officers shall subordinate their personal investment transactions to those of the District, particularly with regard to the time of purchases and sales.

RESPONSIBILITIES

General Manager - The General Manager is charged with responsibility for maintaining custody of all public funds and securities belonging to or under the control of the District and for the deposit and investment of those funds in accordance with principles of sound fiscal management and in conformance with applicable laws and ordinances. The General Manager shall develop an investment procedures manual to implement this Investment Policy for establishing and maintaining an internal control structure designed to ensure that the assets of the District are protected from loss, theft or misuse as approved by the Board of Directors.

Details of the internal controls system shall be documented in an investment procedures manual and shall be reviewed and updated annually. The internal control structure shall be designed to provide reasonable assurance that these objectives are met. The concept of reasonable assurance recognized that (1) the cost of a control should not exceed the benefits likely to be derived and (2) the valuation of costs and benefits requires estimates and judgments by management.

The internal controls structure shall address the following:

1. Control of collusion
2. Separation of transaction authority from accounting and record keeping
3. Custodial safekeeping
4. Avoidance of physical delivery securities
5. Clear delegation of authority to subordinate staff members
6. Written confirmation of transactions for investments and wire transfers
7. Dual authorizations of wire transfers
8. Development of a wire transfer agreement with the lead bank and third-party custodian

The internal controls are further defined in the Investment Procedure attached.

The General Manager is responsible for keeping the Board of Directors fully advised as to the financial condition of the District.

District's Auditing Firm - The District's auditing firm's responsibilities shall include, but not be limited to, the examination and analyses of fiscal procedures and the examination, checking and verification of accounts and expenditures. A review of the District's investment program is to be performed, under a separate engagement for services, in conjunction with the annual financial audit.

Board of Directors - The Board of Directors shall consider and adopt a written Investment Policy. As provided in that Policy, the Board shall receive, review, and accept monthly Cash Position Reports and quarterly Investment Reports.

Investment Committee - An Investment Committee consisting of two (2) members of the Board of Directors appointed by the President, will meet with the District General Manager as required to develop the general strategies, allocate reserve assets among various approved investment instruments, and to monitor results. The Committee shall include in its deliberations, potential risks to District funds, authorized depositors, brokers and dealers, and target rate of return on investments, and any other topics as it may determine or as

directed by the Board of Directors. The Committee shall report to the full Board of Directors the results of the Investment Committee Meeting including any recommended actions. Payment for any transaction which requires the transfer of funds from one investment to another shall require the signature of at least two (2) Members of the Board.

REPORTING

The General Manager, will provide the Board of Directors with monthly cash position and quarterly reports of investments. Such reports will provide at least the following: Type of investment, institution, date of maturity, amount of deposit, current market value of all securities maturing beyond one (1) year after reporting date, rate of interest and such other data as from time to time may be required by the Board.

ANNUAL REVIEW

This investment policy shall be reviewed annually by the Investment Committee to ensure its consistency with respect to the overall objectives of safety, liquidity and yield. Proposed amendments to the policy shall be prepared by the Investment Committee and be forwarded to the Board of Directors for Consideration.

ADDENDUM

GLOSSARY:

U.S. GOVERNMENT SECURITIES

U.S. Treasury Obligations - Treasury bills, Treasury bonds, and Treasury notes issued by the U.S. Treasury. The maturity on these investments shall not exceed five (5) years without the prior approval of the Investment Committee. Per Gov't. Code no maturity greater than five (5) years and no portfolio limits.

U.S. Government Agency Obligations - Any obligation of, or obligation that is insured as to principal and interest by the United States or any agency or corporation thereof, and any obligation and security of the United States sponsored enterprises, including, without limitation:

1) Federal Farm Credit Banks (FFCB)
2) Federal Home Loan Bank System (FHLB)
3) Federal Home Loan Mortgage Corporation (FHLMC)
4) Federal National Mortgage Association (FNMA)
5) Federal Agriculture Mortgage Association (FAMA)
6) Tennessee Valley Authority (TVA)

Per Gov't. Code no maturity greater than five (5) years and no portfolio limits.

FINANCIAL INTERMEDIARIES

CERTIFICATES OF DEPOSIT

Commercial Bank Certificates of Deposit – Time Certificates of Deposit provided that the depository is a member of the FDIC and the amount does not exceed the current FDIC insured limit. Per Gov't. Code no maturity greater than five (5) years and no portfolio limit.

Negotiable Certificates of Deposit – Bank Deposit Notes issued by a nationally or state charted bank or by a state-licensed branch of a foreign bank provide and is a member of the FDIC. Per Gov't Code limits maturity to five (5) years and 30% of portfolio.

Savings and Loan Association (S&L) Deposits – Investments in any Savings and Loan (S&L) institution and bank shall be limited to FDIC Limitations. Collateralization for uninsured S&L deposits is required.

RELATED INSTRUMENTS

Repurchase Agreements – An agreement with an approved broker/dealer that provides for, sell, and simultaneous purchase of an allowable collateral security. The difference in the sales and purchase price is the earning rate on the agreement. A master repurchase agreement must be in place with the approved broker/dealer. Per Gov't. Code no maturity greater than one (1) year, and no portfolio limits.

Bankers' Acceptances - Bills of exchange or time drafts drawn on and accepted by commercial banks, which are eligible for purchase by the Federal Reserve System, are known as bankers' acceptances. Purchases of these instruments may not exceed 180 bankers days maturity per Gov't Code and 40% portfolio limit.

State Investment Pool - Offering a governmental alternative to money market funds, California has created the Local Agency Investment Fund (LAIF). Such funds are operated directly by the State Treasurer who commingles state and local funds. Rates of return fluctuate daily and are reported as a monthly average yield rate. Same day or next day liquidity, by telephone communication. The State Treasurer requests voluntary compliance with no more than fifteen (15) transactions per month. Authorized by Gov't. Code Section 16429.1(b), with no maximum maturity or maximum % of portfolio.

Ventura County Investment Pool - The Ventura County Investment Pool is an additional alternative to money market funds. Similar to the State LAIF, invested funds are commingled with County and other local agency funds for investment purposes and yields are reported monthly. Liquidity provisions are consistent with the State's provisions, and withdrawals can also be made by telephone by authorized personnel. Authorized by Gov't. Code Section 53684(a) with no maximum maturity or maximum % of portfolio.

CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

Board Memorandum

January 27, 2022

To: General Manager

From: Joe Willingham

Subject: Contracting Information/Operation Technology (IT/OT) Managed Services

Objective: Provide continuity for management of the District's informational and operational computer networks.

Action Required: Authorize the General Manager to enter into an agreement with AllConnected of Simi Valley California for IT/OT managed services at a prorated cost not to exceed $111,297.20 for the remainder of this fiscal year (June 30, 2022), and at an annual cost of $191,873.28 for the following three years, ending June 30, 2025.

Discussion: As part of the District's succession planning, staff evaluated alternatives to ensure sustainability of IT duties through loss of employees through attrition and/or turnover.

From 1997 to 2008, the District maintained both in-house and contracted support of its computer and network infrastructure. Starting in 2008, the District moved this function completely in-house. If approved, this board action would move most of IT/OT services, including the computer/network infrastructure, Chief Information Officer (CIO) functions, IT/OT road mapping, and policy development, to contracted services.

Proposals for Managed IT/OT Services were solicited via a targeted RFP process during the month of October 2021, with six firms submitting. Proposals were evaluated on the following criteria:

- Completeness of solution
- Pertinent expertise and comparable experience
- Demonstrated customer service quality and support
- Vendor strength and stability
- Reporting capabilities
- Financial consideration

Out of the six firms that submitted, two finalists were selected to provide follow-up presentations to staff and answer any additional questions. Staff found AllConnected of Simi Valley, California to be the most qualified firm.

Staff has asked AllConnected to prorate their proposed annual contract cost to align with the District's current fiscal year ending June 30, 2022. The $111,297.20 cost outlined below would provide these managed services from January 27 – June 30, 2022:

Service	Description	Cost
Smart Connect	This is a managed monthly service that includes: • 8X5 Help Desk/Desktop • Support • Server & Network System Monitoring • Patch Management • Preventative Maintenance • Business Continuity • Cloud Backup • Email/Collaboration System Mgmt • Email Advanced Threat Protection • Antivirus, Antispam Protection • Monthly End-User Security Awareness Training	Total Smart Connect Service Cost Not to Exceed **$52,447.20** broken down as follows: • Monthly Recurring: $7,489.44 (5 months) • Startup/Setup Fee: $15,000.00
Auxiliary Support	These are "AS NEEDED" services and include but are not limited to: • Custom software support (DevOps) • Help desk issues beyond the help desk technician and TAM's abilities • Issues requiring onsite support or the assistance of a L1, L2 or L3 System/Network/Data Center/Security Engineer • Backup/Recovery Testing • Security Remediation • PC deployment • Printers/Scanners • Moves, Adds, or Changes (MAC) • Project Specific tasks • Virtual Chief Information Officer (vCIO) tasks as needed.	Total Auxiliary Support Cost Not to Exceed **$58,850.00** broken down as follows: • Billed monthly, as needed based on $8500.00 per month for five months (which is based on 14 hours per week X 5 months) • $16,350.00 startup fee

The remaining fiscal years, FY2023-FY2025 under this contract would be automatically renewed with an annual cost not to exceed $191,873.28 per year.

The AllConnected proposal is attached for the Board's review.

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:AMBER

Product ID: A20-350B

December 16, 2021

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

SUMMARY

This joint Cybersecurity Advisory (CSA)—authored by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)—provides an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.

CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations listed below and detailed in the Mitigations section. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation.

Actions critical infrastructure organizations should implement to immediately strengthen their cyber posture.

- Patch all systems. Prioritize patching known exploited vulnerabilities.
- Implement multi-factor authentication.
- Use antivirus software.
- Develop internal contact lists and surge support.

1. **Be prepared**. Confirm reporting processes and minimize personnel gaps in IT/IO security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and

---

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.

continuity of operations plan so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline.

2. **Enhance your organization's cyber posture**. Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
3. **Increase organizational vigilance**. Stay current on reporting on this threat. Subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.

CISA, the FBI, and NSA encourage critical infrastructure organization leaders to review CISA Insights: Preparing for and Mitigating Cyber Threats for information on reducing cyber threats to their organization.

TECHNICAL DETAILS

Note: this advisory uses the MITRE ATT&CK® for Enterprise framework, version 10. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

Historically, Russian state-sponsored advanced persistent threat (APT) actors have used common but effective tactics—including spearphishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security—to gain initial access to target networks. Vulnerabilities known to be exploited by Russian state-sponsored APT actors for initial access include:

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 VMWare (note: this was a zero-day at time.)
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

Russian state-sponsored APT actors have also demonstrated sophisticated tradecraft and cyber capabilities by compromising third-party infrastructure, compromising third-party software, or developing and deploying custom malware. The actors have also demonstrated the ability to maintain persistent, undetected, long-term access in compromised environments—including cloud environments—by using legitimate credentials.

In some cases, Russian state-sponsored cyber operations against critical infrastructure organizations have specifically targeted operational technology (OT)/industrial control systems (ICS) networks with

destructive malware. See the following advisories and alerts for information on historical Russian state-sponsored cyber-intrusion campaigns and customized malware that have targeted ICS:

- ICS Advisory ICS Focused Malware – Havex
- ICS Alert Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)
- ICS Alert Cyber-Attack Against Ukrainian Critical Infrastructure
- Technical Alert CrashOverride Malware
- CISA MAR HatMan: Safety System Targeted Malware (Update B)
- CISA ICS Advisory Schneider Electric Triconex Tricon (Update B)

Russian state-sponsored APT actors have used sophisticated cyber capabilities to target a variety of U.S. and international critical infrastructure organizations, including those in the Defense Industrial Base as well as the Healthcare and Public Health, Energy, Telecommunications, and Government Facilities Sectors. High-profile cyber activity publicly attributed to Russian state-sponsored APT actors by U.S. government reporting and legal actions includes:

- **Russian state-sponsored APT actors targeting state, local, tribal, and territorial (SLTT) governments and aviation networks, September 2020, through at least December 2020.** Russian state-sponsored APT actors targeted dozens of SLTT government and aviation networks. The actors successfully compromised networks and exfiltrated data from multiple victims.
- **Russian state-sponsored APT actors' global Energy Sector intrusion campaign, 2011 to 2018.** Russian state-sponsored APT actors conducted a multi-stage intrusion campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.
- **The Russian General Staff Main Intelligence Directorate's (GRU's) Main Center of Special Technologies (GTsST) campaign against Ukrainian critical infrastructure, 2015 and 2016.** GTsST or Unit 74455 has previously been attributed as Sandworm Team by Mandiant, VOODOO BEAR by CrowdStrike, and ELECTRUM by Dragos. GTsST actors conducted a cyberattack against Ukrainian energy distribution companies, leading to multiple companies experiencing unplanned power outages in December 2015. The actors deployed BlackEnergy malware to steal user credentials and used its destructive malware component, KillDisk, to make infected computers inoperable. In 2016, GTsST actors conducted a cyber-intrusion campaign against a Ukrainian electrical transmission company and deployed CrashOverride malware specifically designed to attack power grids.

For more information on recent and historical Russian state-sponsored malicious cyber activity, see the referenced products below or the CISA webpage cisa.gov/Russia.

- Joint FBI-DHS-CISA CSA Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
- Joint NSA-FBI-CISA CSA Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments
- Joint FBI-CISA CSA Russian APT Actors Compromise U.S. Government Targets

- Joint CISA-FBI CSA APT Actors Chaining Vulnerabilities against SLTT, Critical Infrastructure, and Elections Organizations
- CISA's webpage Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise
- CISA Alert Russian Government Cyber Activity Targeting Energy Sector and Other Critical Infrastructure Sectors
- CISA ICS: Alert Cyber-Attack Against Ukrainian Critical Infrastructure

Table 1 provides common, publicly known TTPs employed by Russian state-sponsored APT actors, which map to the MITRE ATT&CK for Enterprise framework, version 10. **Note**: these lists are not intended to be all inclusive. Russian state-sponsored actors have modified their TTPs before based on public reporting.[1] Therefore, CISA, the FBI, and NSA anticipate the Russian state-sponsored actors may modify their TTPs as they deem necessary to reduce their risk of detection.

Table 1: Common Tactics and Techniques Employed by Russian State-Sponsored APT Actors

Tactic	Technique	Procedure
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Russian state-sponsored APT actors have performed large-scale scans in an attempt to find vulnerable servers.
	Phishing for Information [T1598]	Russian state-sponsored APT actors have conducted spearphishing campaigns to gain credentials of target networks.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Russian state-sponsored APT actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Russian state-sponsored APT actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.
	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	Russian state-sponsored APT actors have gained initial access to victim organizations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Russian state-sponsored APT actors have used `cmd.exe` to execute commands on remote machines. They have also used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands.

Tactic	Technique	Procedure
Persistence [TA0003]	Valid Accounts [T1078]	Russian state-sponsored APT actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Russian state-sponsored APT actors have conducted brute-force password guessing and password spraying campaigns.
	OS Credential Dumping: NTDS [T1003.003]	Russian state-sponsored APT actors have exfiltrated credentials and exported copies of the Active Directory database `ntds.dit`.
	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	Russian state-sponsored APT actors have performed "Kerberoasting," whereby they obtained the Ticket Granting Service (TGS) Tickets for Active Directory Service Principal Names (SPN) for offline cracking.
	Credentials from Password Stores [T1555]	Russian state-sponsored APT actors have used previously compromised account credentials to attempt to access Group Managed Service Account (gMSA) passwords.
	Exploitation for Credential Access [T1212]	Russian state-sponsored APT actors have exploited Windows Netlogon vulnerability CVE-2020-1472 to obtain access to Windows Active Directory servers.
	Unsecured Credentials: Private Keys [T1552.004]	Russian state-sponsored APT actors have obtained private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Russian state-sponsored APT actors have used virtual private servers (VPSs) to route traffic to targets. The actors often use VPSs with IP addresses in the home country of the victim to hide activity among legitimate user traffic.

For additional enterprise TTPs used by Russian state-sponsored APT actors, see the ATT&CK for Enterprise pages on APT29, APT28, and the Sandworm Team, respectively. For information on ICS TTPs see the ATT&CK for ICS pages on the Sandworm Team, BlackEnergy malware, CrashOveride malware, BlackEnergy's KillDisk component, and NotPetya malware.

DETECTION

Given Russian state-sponsored APT actors demonstrated capability to maintain persistent, long-term access in compromised enterprise and cloud environments, CISA, the FBI, and NSA encourage all critical infrastructure organizations to:

- **Implement robust log collection and retention.** Without a centralized log collection and monitoring capability, organizations have limited ability to investigate incidents or detect the threat actor behavior described in this advisory. Depending on the environment, examples include:
    - Native tools such as M365's Sentinel.
    - Third-party tools, such as Sparrow, Hawk, or CrowdStrike's Azure Reporting Tool (CRT), to review Microsoft cloud environments and to detect unusual activity, service principals, and application activity. **Note**: for guidance on using these and other detection tools, refer to CISA Alert Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments.
- **Look for behavioral evidence or network and host-based artifacts** from known Russian state-sponsored TTPs. See table 1 for commonly observed TTPs.
    - To detect password spray activity, review authentication logs for system and application login failures of valid accounts. Look for multiple, failed authentication attempts across multiple accounts.
    - To detect use of compromised credentials in combination with a VPS, follow the below steps:
        - Look for suspicious "impossible logins," such as logins with changing username, user agent strings, and IP address combinations or logins where IP addresses do not align to the expected user's geographic location.
        - Look for one IP used for multiple accounts, excluding expected logins.
        - Look for "impossible travel." Impossible travel occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e., a person could not realistically travel between the geographic locations of the two IP addresses during the time period between the logins). **Note**: implementing this detection opportunity can result in false positives if legitimate users apply VPN solutions before connecting into networks.
        - Look for processes and program execution command-line arguments that may indicate credential dumping, especially attempts to access or copy the `ntds.dit` file from a domain controller.
        - Look for suspicious privileged account use after resetting passwords or applying user account mitigations.
        - Look for unusual activity in typically dormant accounts.
        - Look for unusual user agent strings, such as strings not typically associated with normal user activity, which may indicate bot activity.

- For organizations with OT/ICS systems:
    - Take note of unexpected equipment behavior; for example, unexpected reboots of digital controllers and other OT hardware and software.
    - Record delays or disruptions in communication with field equipment or other OT devices. Determine if system parts or components are lagging or unresponsive.

INCIDENT RESPONSE

Organizations detecting potential APT activity in their IT or OT networks should:

1. Immediately isolate affected systems.
2. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
3. Collect and review relevant logs, data, and artifacts.
4. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
5. Report incidents to CISA and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Note: for OT assets, organizations should have a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment. Refer to the Mitigations section for more information.

See the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for guidance on hunting or investigating a network, and for common mistakes in incident handling. CISA, the FBI, and NSA encourage critical infrastructure owners and operators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch (FCEB) agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability response.

Note: organizations should document incident response procedures in a cyber incident response plan, which organizations should create and exercise (as noted in the Mitigations section).

MITIGATIONS

CISA, the FBI, and NSA encourage all organizations to implement the following recommendations to increase their cyber resilience against this threat.

Be Prepared

Confirm Reporting Processes and Minimize Coverage Gaps

- Develop internal contact lists. Assign main points of contact for a suspected incident as well as roles and responsibilities and ensure personnel know how and when to report an incident.
- Minimize gaps in IT/OT security personnel availability by identifying surge support for responding to an incident. Malicious cyber actors are known to target organizations on weekends and holidays when there are gaps in organizational cybersecurity—critical infrastructure organizations should proactively protect themselves by minimizing gaps in coverage.
- Ensure IT/OT security personnel monitor key internal security capabilities and can identify anomalous behavior. Flag any identified IOCs and TTPs for immediate response. (See table 1 for commonly observed TTPs).

Create, Maintain, and Exercise a Cyber Incident Response, Resilience Plan, and Continuity of Operations Plan

- Create, maintain, and exercise a cyber incident response and continuity of operations plan.
- Ensure personnel are familiar with the key steps they need to take during an incident and are positioned to act in a calm and unified manner. Key questions:
    - Do personnel have the access they need?
    - Do they know the processes?
- For OT assets/networks,
    - Identify a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment.
        - Identify OT and IT network interdependencies and develop workarounds or manual controls to ensure ICS networks can be isolated if the connections create risk to the safe and reliable operation of OT processes. Regularly test contingency plans, such as manual controls, so that safety critical functions can be maintained during a cyber incident. Ensure that the OT network can operate at necessary capacity even if the IT network is compromised.
    - Regularly test manual controls so that critical functions can be kept running if ICS or OT networks need to be taken offline.
    - Implement data backup procedures on both the IT and OT networks. Backup procedures should be conducted on a frequent, regular basis. Regularly test backup procedures and ensure that backups are isolated from network connections that could enable the spread of malware.

- In addition to backing up data, develop recovery documents that include configuration settings for common devices and critical OT equipment. This can enable more efficient recovery following an incident.

Enhance your Organization's Cyber Posture

CISA, the FBI, and NSA recommend organizations apply the best practices below for identity and access management, protective controls and architecture, and vulnerability and configuration management.

Identity and Access Management

- Require multi-factor authentication for all users, without exception.
- Require accounts to have strong passwords and do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access.
- Secure credentials. Russian state-sponsored APT actors have demonstrated their ability to maintain persistence using compromised credentials.
  - Use virtualizing solutions on modern hardware and software to ensure credentials are securely stored.
  - Disable the storage of clear text passwords in LSASS memory.
  - Consider disabling or limiting New Technology Local Area Network Manager (NTLM) and WDigest Authentication.
  - Implement Credential Guard for Windows 10 and Server 2016 (Refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
  - Minimize the AD attack surface to reduce malicious ticket-granting activity. Malicious activity such as "Kerberoasting" takes advantage of Kerberos' TGS and can be used to obtain hashed credentials that attackers attempt to crack.
- Set a strong password policy for service accounts.
- Audit Domain Controllers to log successful Kerberos TGS requests and ensure the events are monitored for anomalous activity.
  - Secure accounts.
  - Enforce the principle of least privilege. Administrator accounts should have the minimum permission they need to do their tasks.
  - Ensure there are unique and distinct administrative accounts for each set of administrative tasks.
  - Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).

Protective Controls and Architecture

- Identify, detect, and investigate abnormal activity that may indicate lateral movement by a threat actor or malware. Use network monitoring tools and host-based logs and monitoring tools, such as an endpoint detection and response (EDR) tool. EDR tools are particularly

useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.

- Enable strong spam filters.
    - Enable strong spam filters to prevent phishing emails from reaching end users.
    - Filter emails containing executable files to prevent them from reaching end users.
    - Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments.

Note: CISA, the FBI, and NSA also recommend, as a longer-term effort, that critical infrastructure organizations implement network segmentation to separate network segments based on role and functionality. Network segmentation can help prevent lateral movement by controlling traffic flows between—and access to—various subnetworks.

- Appropriately implement network segmentation between IT and OT networks. Network segmentation limits the ability of adversaries to pivot to the OT network even if the IT network is compromised. Define a demilitarized zone that eliminates unregulated communication between the IT and OT networks.
- Organize OT assets into logical zones by taking into account criticality, consequence, and operational necessity. Define acceptable communication conduits between the zones and deploy security controls to filter network traffic and monitor communications between zones. Prohibit ICS protocols from traversing the IT network.

Vulnerability and Configuration Management

- Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner. Prioritize patching known exploited vulnerabilities, especially those CVEs identified in this CSA, and then critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
    - Consider using a centralized patch management system. For OT networks, use a risk-based assessment strategy to determine the OT network assets and zones that should participate in the patch management program.
    - Consider signing up for CISA's cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IP addresses for accessible services and vulnerabilities.
- Use industry recommended antivirus programs.
    - Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures.
    - Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- Implement rigorous configuration management programs. Ensure the programs can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses.

- Disable all unnecessary ports and protocols
  - Review network security device logs and determine whether to shut off unnecessary ports and protocols. Monitor common ports and protocols for command and control (C2) activity.
  - Turn off or disable any unnecessary services (e.g., PowerShell) or functionality within devices.
- Ensure OT hardware is in read-only mode.

Increase Organizational Vigilance

- Regularly review reporting on this threat. Consider signing up for CISA notifications to receive timely information on current security issues, vulnerabilities, and high-impact activity.

RESOURCES

- For more information on Russian state-sponsored malicious cyber activity, refer to cisa.gov/Russia.
- Refer to CISA Analysis Report Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services for steps for guidance on strengthening your organizations cloud security practices.
- Leaders of small businesses and small and local government agencies should see CISA's Cyber Essentials for guidance on developing an actionable understanding of implementing organizational cybersecurity practices.
- Critical infrastructure owners and operators with OT/ICS networks, should review the following resources for additional information:
  - NSA and CISA joint CSA NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
  - CISA factsheet Rising Ransomware Threat to Operational Technology Assets for additional recommendations.

REWARDS FOR JUSTICE PROGRAM

If you have information on state-sponsored Russian cyber operations targeting U.S. critical infrastructure, contact the Department of State's Rewards for Justice Program. You may be eligible for a reward of up to $10 million, which DOS is offering for information leading to the identification or location of any person who, while acting under the direction or control of a foreign government, participates in malicious cyber activity against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA). Contact +1-202-702-7843 on WhatsApp, Signal, or Telegram, or send information via the Rewards for Justice secure Tor-based tips line located on the Dark Web. For more details refer to rewardsforjustice.net/malicious_cyber_activity.

CAVEATS

The information you have accessed or received is being provided “as is” for informational purposes only. CISA, the FBI, and NSA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA, the FBI, or NSA.

REFERENCES

[1] Joint NCSC-CISA UK Advisory: Further TTPs Associated with SVR Cyber Actors
https://www.ncsc.gov.uk/news/joint-advisory-further-ttps-associated-with-svr-cyber-actors

December 20, 2021

U.S. ENVIRONMENTAL PROTECTION AGENCY-WaterISAC ADVISORY

To: Water and Wastewater Systems, SLTT Governments and Private Sector Stakeholders

(TLP:AMBER) Cybersecurity Recommendations in Consideration of the CISA/FBI/NSA Advisory on Russian State-Sponsored Cyber Operations Against U.S. Critical Infrastructure

On December 16, 2021, the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and the National Security Agency (NSA) issued a joint advisory on Russian state-sponsored cyber operations against United States critical infrastructure (see attachment for advisory AA21-350B).

What is the Purpose of the CISA/FBI/NSA Joint Advisory?

The joint advisory describes commonly observed tactics, techniques, and procedures; detection actions; incident response guidance; and mitigations. It is intended to help critical infrastructure reduce the risk presented by these threats and to encourage the adoption of a heightened state of awareness during the holidays (a time when many disconnect from work).

The joint advisory complemented a December 15, 2021 CISA Insights publication - Preparing For and Mitigating Potential Cyber Threats. It asserted that due to persistent cyber-threats from sophisticated actors, including nation-states and their proxies, critical infrastructure owners and operators should take immediate steps to strengthen their computer network defenses. These actors have the capability to leverage network access for targeted operations with the potential to disrupt critical infrastructure functions.

What Actions are Recommended for Water and Wastewater Systems?

Water and wastewater system owners and operators should review the attached joint advisory and assess how to apply the recommended detection, incident response, and mitigation actions to their operations. Key actions for water and wastewater systems include the following:

1) **Require Strong, Unique Passwords.** Malicious cyber actors repeatedly use stolen or easily guessed credentials. Consider forcing a global reset of all passwords in your environment before staff begin taking time off.
2) **Implement Multi-Factor Authentication.** After changing passwords, make implementing multi-factor authentication (MFA) a priority. MFA significantly reduces your risk from almost all opportunistic attempts to gain entry into your systems.
3) **Address known exploited vulnerabilities.** This could include patching and/or additional controls such as network segmentation to protect vulnerable devices that cannot effectively be patched. CISA maintains a catalog of Known Exploited Vulnerabilities that utilities are encouraged to review to identify vulnerable systems. Also, prioritize network segmentation to prevent unauthorized access to your operational technology (OT) systems from the internet and to reduce connectivity between OT and vulnerable information technology (IT) systems.
4) **Surge Support.** Identify surge support for responding to an incident. Malicious cyber actors are known to target organizations on weekends and holidays when there are gaps in organizational cybersecurity.

5) **Network/Systems Awareness.** Be alert for unusual behavior in OT and IT systems, such as unexpected reboots of digital controllers and other OT hardware and software, and delays or disruptions in communication with field equipment or other OT devices. Enhance logging to investigate anomalous activity – including collecting more logs and increasing storage capacity and retention time.
6) **Backup Data.** Implement and test data backup procedures on both IT and OT networks and ensure copies of backups are isolated (stored offline) from the network.
7) **Incident Response Plans.** Create, maintain, and exercise a cyber incident response and continuity of operations plans.
8) **Manual Operations.** Have a resilience plan that addresses how to operate your system if you lose access to or control of critical OT or IT systems – including the ability to sustain manual operations for extended periods.

How Can I Learn More About the CISA/FBI/NSA Joint Advisory?

WaterISAC and EPA, in conjunction with water sector associations, will hold a TLP:AMBER webinar on the dates/times listed below to present and discuss the joint advisory. The webinar is intended for water and wastewater system owners and operators, along with state, local, tribal, and territorial (SLTT) government officials and private sector organizations that directly support water and wastewater system operations. Registration links for the webinar are provided. For those unable to join live, the webinar will be recorded and posted to the WaterISAC website for members and trial members.

- Date 1: Wednesday, December 29, 2021, 2:00 – 3:00 pm EST.
  Register: https://attendee.gotowebinar.com/register/8355582904364747792
- Date 2: Wednesday, January 5, 2022, 2:00 – 3:00 pm EST.
  Register: https://attendee.gotowebinar.com/register/5595566826088940559

Additional Resources

- Protecting Against Malicious Cyber Activity before the Holidays (White House; 12/16/21)
- Joint Cybersecurity Advisory Ongoing Cyber Threats to U.S. Water and Wastewater Systems (CISA, FBI, NSA, EPA; 10/14/21)
- WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- U.S. EPA Cybersecurity Best Practices for the Water Sector
- AWWA Resources on Cybersecurity

WaterISAC Incident Reporting
WaterISAC encourages all utilities that have experienced malicious or suspicious activity to email analyst@waterisac.org, call 866-H2O-ISAC, or use the confidential online incident reporting form. Reporting to WaterISAC helps utilities and stakeholders stay aware of the threat environment of the sector.

TLP:AMBER Definition: *Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.*

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 4. For your protection, make sure that you read and understand all provisions before signing. The terms on Page 2 through 4 are incorporated in this document and will constitute a part of the agreement between the parties when signed.

TO: AllConnected, Inc.
4514 Ish Drive
Simi Valley, CA 93063

DATE: January 27, 2022

Agreement No.: 2022-126

The undersigned Consultant offers to furnish the following: IT/OT managed services for Camrosa Water District per attached AllConnected Master Service Agreement, smartConnect Statement of Work, and Auxiliary Support Attachment(s).

Contract price $:

1. SmartConnect billed monthly $7,489.44* plus Startup/Setup Fees $15,000.00, not to exceed $52,447.20 for current fiscal year, and $89,873.28 for subsequent years.
2. Auxiliary Support Services $16,350 start-up fee, plus billed as needed not to exceed $58,850.00 for current fiscal year, and not to exceed $102,000 per year for subsequent years.

* Assumes 25 named users, 85 endpoints, 15TB.

Contract Term: SmartConnect effective for 41-month contract term thru June 30, 2025 and may be renewed on an annual basis thereafter.
Auxiliary Support Services effective for 41-month contract term thru June 30, 2025 and may be renewed on an annual basis thereafter.
Master Service Agreement may be terminated with or without cause with 90 days written notice.

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: AllConnected, Inc.
By: _____	By: _____
Tony L. Stafford	Alan McDonald
Title: General Manager	Title: President, CEO
Date: _____	Date: _____

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 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 parties to this Agreement mutually agree to waive all rights of subrogation against the other party and its directors, officers, employees, and authorized volunteers for losses paid under the terms of this policy which arise from work performed pursuant to this Agreement ; but this provision applies regardless of whether or not the party has received a waiver of subrogation from its insurer.

   5. **Professional Liability** - (also known as Errors & Omission) Insurance appropriate to the Consultant profession, with limits no less than $1,000,000 per occurrence or claim, and $2,000,000 policy aggregate.

   6. **Cyber Liability Insurance (Technology Professional Liability – Errors and Omissions),** with limits not less than $2,000,000 per occurrence or claim, and $2,000,000 aggregate or the full per occurrence limits of the policies available, whichever is greater. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in this Agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

d. **If Claims Made Policies:**

   1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.

   2. Insurance must be maintained and evidence of insurance must be provided **for at least five (5) years after completion of the contract of work.**

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

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

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

a. **Additional Insured Status:** District, its directors, officers, employees, and authorized volunteers are to be given insured status (at least as broad as ISO Form CG 20 10 10 01), with respect to liability arising out of work or operations performed by or on behalf of the Consultant including materials, parts, or equipment furnished in connection with such work or operations.

b. **Primary Coverage:** For any claims related to this project, the Consultant's insurance coverage shall be primary at least as broad as ISO CG 20 01 04 13 as respects to the District, its directors, officers, employees, and authorized volunteers. Any insurance or self-insurance maintained by the District, its directors, officers, employees, and authorized volunteers shall be excess of the Consultant's insurance and shall not contribute with it.

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

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

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

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

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

Other Requirements:

a. Consultant shall not accept direction or orders from any person other than the General Manager or the person(s) whose name(s) is (are) inserted on Page 1 as "other authorized representative(s)."

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

c. Permits required by governmental authorities will be obtained at Consultant's expense, and Consultant will comply with applicable local, state, and federal regulations and statutes including Cal/OSHA requirements.

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

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

MASTER SERVICE AGREEMENT v1.24c

THIS MASTER SERVICE AGREEMENT ("Agreement") is made this 27th day of January 2022 ("Effective Date") by and between AllConnected, Inc. ("Master Service Provider", "MSP" or AllConnected), 4514 Ish Drive, Simi Valley, CA 93063 and Camrosa Water District, 7385 Santa Rosa Road, Camarillo, CA 93012 ("Client").

1. SCOPE OF AGREEMENT. This Agreement serves as a master agreement and applies to Client's purchases from AllConnected, of product including hardware, support and maintenance services, licenses for software & hardware, and/or subscription services, ("Product") and of services including but not limited to Support Connect, Recovery Solutions, Disaster Recovery, Cloud Backup and IT Infrastructure Services ("Services"). Client hereby engages and retains AllConnected to render Services as more particularly set forth in the SmartConnect agreement and/or subsequent addendums (the "Statement of Work") attached hereto and incorporated herein by reference. No Product or Services will be provided under this Agreement alone, but may require the execution of a written or electronic purchase order form, or other mutually acceptable order documentation, which contains terms relating to this Agreement, each of which must be executed by both parties and, upon such execution, is deemed incorporated in this Agreement for all purposes. Each subsequent Addendum or Statement of Work incorporate all the provisions within this Agreement. The parties hereby further agree that the parties may execute multiple Orders and Statements of Work under this Agreement. In the event of any conflict between the terms of the Purchase Order and Statement of Work and those of this Agreement, the terms of the Purchase Order or Statement of Work will prevail over this Agreement.

2. TERM AND TERMINATION. This Agreement will begin on the Effective Date and will continue until each Order and/or SOW expires, is completed, or is terminated. AllConnected may: (a) terminate a specific Order if Client fails to pay any applicable fees due for that Order within 30 days after receipt of written notice from AllConnected of non-payment; and/or (b) terminate this Agreement or an Order if Client commits any other material breach of this Agreement and fails to cure such breach within fifteen (15) days after receipt of written notice from AllConnected. If an Order for Services is terminated, Client will promptly pay AllConnected for Services rendered, and expenses incurred through the termination date.

Client may (a) terminate this Agreement or an Order if AllConnected commits any other material breach of this Agreement and fails to cure such breach within fifteen (15) days after receipt of written notice from Client; and/or (b) terminate for any reason with ninety (90) days written notice to AllConnected. If applicable, early termination fees will be defined in each Order and/or SOW.

2.1 Termination of Cloud Service by AllConnected. (a) FOR CAUSE. AllConnected may immediately (and without prior notice) suspend or terminate all or part of the Cloud Services by sending Client a written notice of termination if one or more of the following occurs: (i) AllConnected discovers that you provided us with false information when you registered for Cloud Services; (ii) AllConnected determines, in our sole discretion, that your use of the Cloud Services poses a threat to the security or performance of our network or to any of our clients or suppliers; (iii) we determine, in our sole discretion, that your use of the Cloud Services is illegal, or that it misappropriates or infringes the property rights of a third party; (iv) you become the subject of an involuntary or voluntary bankruptcy or similar proceeding, or you assign all or substantially all of your assets for the benefit of creditors; (v) you fail to make any payment when due or if your credit card is declined; or (vi) you use cloud resources in an attempt to gain unauthorized access to computer systems (i.e., "hacking"). Notwithstanding any provision in this Agreement to the contrary, in the event AllConnected terminates or suspends Client's

Cloud Services without prior notice, and the factual basis upon which AllConnected based its suspension or termination of Client's Cloud Services is shown to be incorrect, AllConnected shall be responsible for any damages suffered by Client as a proximate result of the suspension or termination of Client's Cloud Services.

2.2 Termination of Cloud Service by Client. You may terminate your Cloud Service at any time and for any reason (or no reason at all) with ninety (90) days written notice to AllConnected.

If you do not renew your Cloud Service, terminate your Cloud Service or if AllConnected terminates your Cloud Service, unless sent to you in writing stating otherwise, our current policy is to keep your data for up to 30 days after the expiration or termination of your service, allowing you time to change your mind. After 30 days, we remove the backed up data associated with your Cloud Service and it will no longer be available for restore.

3. PAYMENT. Client will pay AllConnected all fees within 30 days of the invoice date which specifies the amounts due ("Fees"). All Fees payable under this Agreement are exclusive of sales, use, excise, and any other applicable transaction taxes, which Client will pay (excluding taxes based upon the net income of AllConnected). If payment is not received on or before any invoice due date, interest shall begin to accrue and be payable at the lesser of the maximum rate permitted under applicable law or at the rate of one and one-half percent (1.5%) (or any other interest rate in accordance with the state's law) per month from the date due until paid in full. In the event of litigation, or arbitration, the non-prevailing party shall pay all expenses, including reasonable attorneys' fees, incurred by prevailing party or its representatives in enforcing its rights under this Agreement. Client's obligation to pay undisputed amounts due for Services and AllConnected's right to all such amounts are absolute and unconditional. Client is not entitled to setoff of such amounts. All Fees will be detailed in an Order. All such Fees, including any potential overage fee, will be agreed upon by both parties prior to the service being provided by AllConnected. Unless otherwise stated in a Purchase Order, Client agrees to pay or reimburse AllConnected for all actual, necessary, and reasonable expenses incurred by AllConnected in performance of such Purchase Order, which are capable of verification by receipt. AllConnected will submit invoices to Client for such fees and expenses either upon completion of the Services, or at stated intervals, in accordance with the applicable Purchase Order or Statement of Work.

4. CONFIDENTIALITY AND NON-DISCLOSURE. Both Parties to this Agreement recognize that, from time to time, they may come into contact with information that the other Party considers confidential. Confidential Information is defined for this Agreement as all information (whether written or oral) that comes into a Party's possession under or in connection with this Agreement that is reasonably considered by the disclosing Party to be confidential and is clearly identified as confidential. The Parties shall keep all Confidential Information in strict confidence.

The recipient will use a reasonable standard of care in protecting Confidential Information, which will not be less than the standard of care the recipient uses to protect its own confidential information; only use Confidential Information to perform its obligations and exercise its rights under this Agreement; not disclose Confidential Information to any third party; when requested by the disclosing Party, return or destroy the Confidential Information.

5. NO-HIRE AGREEMENT. In the event Client directly or indirectly employs any AllConnected consultant(s) or engineer(s) who provided service to Client, whether on-site or remotely, Client agrees

to pay AllConnected a recruitment and training fee of 50% of the total annual salary or $50,000, whichever is greater.

6. PROVISION OF MATERIALS AND SERVICES TO AllConnected. Client agrees to timely furnish, at its own expense, all personnel, all necessary computer hardware, software and related materials and appropriate and safe workspaces for purposes of AllConnected performing the services. Client will also provide AllConnected with access to all information, passwords and facilities requested by AllConnected that is necessary for AllConnected to perform the services. Access may be denied for any reason at any time, however if access to information, passwords or facilities is denied, Client understands that the AllConnected may be unable to perform their duties adequately and if such a situation should exist, the AllConnected will be held harmless.

7. WORKING ENVIRONMENT. Client shall provide a suitable working environment for any Equipment located at Client's facility. Such environment includes, but is not limited to the appropriate temperature, static electricity and humidity controls and properly conditioned electrical supply for each piece of Equipment. Client shall bear the risk of loss of any Equipment located at Client's facility.

8. CLIENT IS RESPONSIBILE FOR EQUIPMENT. Client acknowledges that from time to time (a) AllConnected may identify additional items that need to be purchased by Client, and (b) changes in Client's systems may be required in order for AllConnected to meet Client's requirements. In connection therewith, Client agrees to work in good faith with AllConnected to effectuate such purchases or changes. In the event that AllConnected is required to purchase any assets deployed at client site, including computer hardware and/or software, in connection with AllConnected providing the services, all such assets will remain the sole property of AllConnected unless specifically stated otherwise in writing. Client will be responsible for the quality, completeness and workmanship of any item or service furnished by it and for ensuring that the materials provided to AllConnected do not infringe or violate the rights of any third party. Unless Client has engaged AllConnected for Co-Managed Cloud Backup or Disaster Recovery, Client will maintain adequate backup for all data and other items furnished to AllConnected.

9. CLIENT DATA OWNERSHIP AND RESPONSIBILITY. Client shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use any data, information or material submitted by Client to AllConnected.

9.1. Software Installation or Replication. If AllConnected is required to install or replicate Client software as part of the Services, Client will independently verify that all such software is properly licensed. Client's act of providing any software to AllConnected will be deemed Client's affirmative acknowledgement to AllConnected that Client has a valid license that permits AllConnected to perform the Services related thereto. In addition, Client will retain the duty and obligation to monitor Client's equipment for the installation of unlicensed software unless AllConnected in a written statement of work ("SOW") expressly agrees to conduct such monitoring. Client will indemnify and hold harmless AllConnected against all damages and expenses it may incur (including reasonable attorney's fees and disbursements) related to Client providing infringing materials to AllConnected or any Client breach of this Section.

9.2. Data Encryption. Unless otherwise set forth in the SOW and/or SLA personal data and non-public data shall be encrypted at rest (public or multi-tenant), and in transit (traversing public networks). The

SOW and/or SLA will specify which party is responsible for encryption. If the SOW and/or SLA are silent then the Client is responsible for encryption.

10. INTELLECTUAL PROPERTY. AllConnected retains all intellectual property rights in any property invented or composed in the course of or incident to the performance of this Agreement, as well as any software, materials, or methods created prior to or after conclusion of any work. Client acquires no right or interest in any such intellectual property, by virtue of this Agreement or the work performed under this Agreement.

10.1. Client may only use and disclose Product in accordance with the terms of this Agreement and applicable Order. AllConnected reserves all rights in and to the Product not expressly granted in this Agreement. Client may not disassemble or reverse engineer any software Product, or decompile or otherwise attempt to derive any software Product's source code from executable code, except to the extent expressly permitted by applicable law despite this limitation, or provide a third party with the results of any functional evaluation, or benchmarking or performance tests on the Products, without AllConnected's prior written approval. Except as expressly authorized in this Agreement or an Order, Client may not (a) distribute the Product to any third party (whether by rental, lease, sublicense or other transfer), or (b) operate the Product in an outsourcing or AllConnected business to process the data of third parties. Additional usage restrictions may apply to certain third-party files or programs embedded in the Product - applicable installation instructions or release notes will contain the relevant details.

10.2. License Agreements.

(a) License. Subject to the terms of this Agreement, AllConnected grants Client a perpetual, non-exclusive, non-transferable license to use and modify all programming, documentation, reports, and any other product provided as part of the Services solely for its own internal use.

(b) Pre-Existing License Agreements. Any software product provided to Client by AllConnected as a reseller for a third party, which is licensed to Client under a separate software license agreement with such third party, will continue to be governed by the third party license agreement.

(c) EULA. Client hereby consents permission to AllConnected to sign all EULA's necessary for any software product installed on Client's computer system.

10.3. Third-Party Products. Product warranties for third party products, if any, are provided by the manufacturers thereof and not by AllConnected. AllConnected's sole obligation is to act on behalf of Client to assist in the satisfaction of any such warranty.

11. WARRANTY. AllConnected warrants that it will perform the Services substantially in accordance with the specifications set forth whether under this Agreement, a purchase order, other work order, SOW or otherwise in connection with any of them. For any breach of the foregoing warranty, AllConnected will exercise commercially reasonable efforts to re-perform any non-conforming services that were performed within the ten (10) business day period immediately preceding the date of Client's written notice to AllConnected specifying in reasonable detail such non-conformance. If AllConnected concludes that conformance is impracticable, then AllConnected will refund all fees paid by Client to AllConnected hereunder, if any, allocable to such nonconforming Services.

Notwithstanding the above, AllConnected does not warrant its products or services beyond a

reasonable standard or skill consistent with industry standards. AllConnected does not guarantee or promise any cost savings, profits, or returns on investment.

12. SOFTWARE, HARDWARE & SECURITY. Client understands and agrees that data loss, security breaches, or network failures may occur, whether or not foreseeable, if the Client fails to maintain proper security for its computer and information system including software and hardware updates. Client therefore agrees that it will follow software and hardware updates and maintain specific security standards, policies, procedures set forth in Addendum A ("Network Security & Data Protection Policy") attached hereto and incorporated herein by reference.

13. TERRORISM AND CYBER TERRORISM. In no event, shall AllConnected, whether under this Agreement, a purchase order, other work order or otherwise in connection with any of them, be liable in contract, tort, third-party liability, breach of statutory duty or otherwise, in respect of any direct, indirect or consequential losses or expenses, including without limitation loss of anticipated profits, company shut-down, third-party loss or injury, any loss because of data breach, any loss of personally identifiable or protected information, goodwill, use, market reputation, business receipts or contracts or commercial opportunities, whether or not foreseeable, if such loss was the result of or arose from any act of terrorism, strike or similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, or any action taken in controlling, preventing or suppressing any of these things, including any such act or series of acts of any person or group(s) or persons, whether acting alone or on behalf of or in connection with any organization(s), committed for political, religious or ideological purposes including but not limited to the intention to influence any government and/or to put the public in fear for such purposes by using activities perpetrated electronically that are directed towards the destruction, disruption or subversion of communication and information systems, infrastructure, computers, telecommunications or electronic networks and/or its content thereof or sabotage and or threat therefrom.

14. TELEMARKETING & UNSOLICITED EMAILS. In no event, shall AllConnected, whether under this Agreement, a purchase order, other work order or otherwise in connection with any of them, be liable in contract, tort, third-party liability, breach of statutory duty or otherwise, in respect of any direct, indirect or consequential losses or expenses, including without limitation loss of anticipated profits, company shut-down, third-party loss or injury, any loss because of data breach, any loss of personally identifiable or protected information, goodwill, use, market reputation, business receipts or contracts or commercial opportunities, whether or not foreseeable, if the Client's data is breached because of the distribution of unsolicited email, direct mail, facsimiles, telemarketing or because of the collection of information by means of electronic "spiders", "spybots", "spyware", wiretapping, bugging, video cameras or identification tags.

15. EXTRAORDINARY EVENTS. In no event, shall AllConnected, whether under this Agreement, a purchase order, other work order or otherwise in connection with any of them, be liable in contract, tort, third-party liability, breach of statutory duty or otherwise, in respect of any direct, indirect or consequential losses or expenses, including without limitation loss of anticipated profits, company shut-down, third-party loss or injury, any loss because of data breach, any loss of personally identifiable or protected information, goodwill, use, market reputation, business receipts or contracts or commercial opportunities, whether or not foreseeable, if such loss was the result of or arose from any failure or malfunction of electrical or telecommunications infrastructure or services not under AllConnected's control, any satellite failure, or from any fire, flood, earthquake, volcanic eruption, explosion, lighting, wind, hail, tidal wave, landslide, act of God or other physical event.

16. LIMITATIONS OF LIABILITY. THIS PARAGRAPH LIMITS THE LIABILITIES ARISING UNDER THIS AGREEMENT OR ANY SOW AND IS A BARGAINED-FOR AND MATERIAL PART OF THIS AGREEMENT. CLIENT ACKNOWLEDGES AND AGREES THAT ALLCONNECTED WOULD NOT ENTER INTO THIS AGREEMENT UNLESS IT COULD RELY ON THE LIMITATIONS DESCRIBED IN THIS PARAGRAPH. EXCEPT FOR ALLCONNECTED'S FRAUD, WILLFUL MISCONDUCT, OR GROSS NEGLIGENCE, CLIENT AND ANY OF THEIR AFFILIATES AND EACH OF THEIR RESPECTIVE AGENCIES, EMPLOYEES, OFFICERS, DIRECTORS, MEMBERS, SHAREHOLDERS, NOMINEES, CONSULTANTS, SUCCESSORS AND ASSIGNS (COLLECTIVELY, THE "RELEASOR PARTIES") AGREES TO THE FULLEST EXTENT PERMITTED BY LAW AND EXCEPT AS OTHERWISE NOTED IN THIS AGREEMENT, TO RELEASE ALLCONNECTED AND EACH OF THEIR RESPECTIVE EMPLOYEES, OFFICERS, DIRECTORS, MEMBERS, SHAREHOLDERS, SUCCESSORS AND ASSIGNS (COLLECTIVELY, THE "RELEASED PARTIES") FOR SPECIAL DAMAGES, OR FOR INDIRECT DAMAGES, LOSS OF GOOD WILL OR EXEMPLARY OR PUNITIVE DAMAGES. ALLCONNECTED'S AGGREGATE LIABILITY ARISING FROM OR OUT OF OR RELATING TO BREACH OF THIS AGREEMENT SHALL NOT EXCEED THE FEES CONTRACTED UNDER THIS AGREEMENT FOR TWELVE (12) MONTHS. HOWEVER, THE LIMITATIONS ON LIABILITY PROVIDED HEREIN SHALL NOT APPLY TO ANY CLAIMS THAT ARE COVERED BY ALLCONNECTED'S INSURANCE.

17. INSURANCE. AllConnected agrees to maintain sufficient insurance coverage to enable it to meet its obligations created by this Agreement and by law. Without limiting the foregoing, to the extend this Agreement creates exposure generally covered by the following insurance policies, AllConnected will maintain at its own sole cost and expense at least the following insurance covering its obligations under this Agreement: (a) Commercial General Liability including (i) bodily injury, (ii) property damage, (iii) contractual liability coverage, and (iv) personal injury, not less than Two Million Dollars ($2,000,000) per occurrence; (b) Business Automobile Liability for owned, hired and non-owned vehicles in an amount of not less than One Million Dollars ($1,000,000) for each accident; (c) Workers Compensation not less than One Million Dollars ($1,000,000); (d) Professional Liability and Cyber Security Insurance covering errors and omissions and wrongful acts in the performance of the Services. Such insurance will bear a combined single limit per occurrence of not less than Two Million Dollars ($2,000,000).

18. INDEMNIFICATION. AllConnected will indemnify, defend and hold harmless the Client and its directors, officers, employees and authorized volunteers (collectively, the "Indemnified Party") from and against any and all costs, expenses, liabilities, losses and damages (including reasonable attorneys' fees) (collectively, "Losses") resulting from any claim, suit, action, demand or proceeding (each, an "Action") brought by any third party against the Indemnified Party arising from negligent acts, errors or omissions of AllConnected or its officers, agents, or employees in rendering services under this Agreement, excluding, however, such liability, claims, losses, damages or expenses arising from Client's negligence or willful acts or(i) a Default by the Client, (ii) the intentional misconduct of the Client or its employees, contractors, consultants or agents, or (iii) any failure by the Client or its employees, contractors, consultants or agents to comply with applicable laws and regulations.

19. DISCLAIMERS. The express remedies set forth in this Agreement will constitute Client's exclusive remedies, and AllConnected's sole obligation and liability, for any claim (a) that a Service or deliverable provided hereunder does not conform to specifications or is otherwise defective, or (b) that the Services were performed improperly.

AllConnected shall not be responsible for impairments to the Services caused by acts within the control of Client or its employees, agents, contractors, suppliers or licensees, the interoperability of Client applications, or other cause reasonably within Client's control and not reasonably related to services provided under this Agreement.

EXCEPT FOR THE WARRANTIES MADE BY ALLCONNECTED IN SECTION 11, WHICH ARE LIMITED WARRANTIES AND THE ONLY WARRANTIES PROVIDED TO CLIENT, THE SERVICES AND DELIVERABLES ARE PROVIDED STRICTLY "AS-IS." ALLCONNECTED DOES NOT MAKE ANY ADDITIONAL WARRANTIES, EXPRESSED, IMPLIED, ARISING FROM COURSE OF DEALING OR USAGE OF TRADE, OR STATUTORY, AS TO THE DELIVERABLES OR SERVICES PROVIDED HEREUNDER, OR ANY MATTER WHATSOEVER. THE PARTIES DISCLAIM ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE AND NON-INFRINGEMENT.

ALLCONNECTED DOES NOT WARRANT THAT THE SERVICES OR ANY DELIVERABLES WILL MEET ANY CLIENT REQUIREMENTS NOT SET FORTH HEREIN, THAT ANY DELIVERABLES WILL OPERATE IN THE COMBINATIONS THAT CLIENT MAY SELECT FOR USE, THAT THE OPERATION OF ANY DELIVERABLES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL ERRORS WILL BE CORRECTED. IF PRE-PRODUCTION (E.G., "ALPHA" OR "BETA") RELEASES OF SOFTWARE ARE PROVIDED TO CLIENT, SUCH COPIES ARE PROVIDED "AS-IS" WITHOUT WARRANTY OF ANY KIND.

No statement by any AllConnected employee or agent, orally or in writing, will serve to create any warranty or obligation not set forth herein or to otherwise modify this Agreement in any way whatsoever.

20. SEVERABILITY. If any provision of this Agreement is determined by a court of competent jurisdiction to be illegal or unenforceable, such provision shall be automatically reformed and construed so as to be valid, operative and enforceable, to the maximum extent permitted by law or equity while preserving its original intent. The invalidity of any part of this Agreement shall not render invalid the remainder of this Agreement.

21. AMENDMENT. This Agreement may not be amended except by a writing executed by an authorized individual at AllConnected.

22. RELATIONSHIP. The Parties are independent parties; and this Agreement does not make the Parties principal and agent, partners, employer and employee; nor does it create a joint venture.

23. LAW. This Agreement shall be governed by and construed in accordance with the laws of the State of California without reference to principles of conflicts of laws. The Parties irrevocably submit to the exclusive jurisdiction of the courts of the State of California.

24. WAIVER. Failure by either Party to insist upon strict performance of any provision herein shall not be deemed a waiver by such Party of its rights or remedies, or a waiver by it of any subsequent default by the other Party.

25. FORCE MAJEURE. With the exception of Client payment for service rendered, neither party shall be responsible for any failure to perform or delay caused where such failure or delay is due to circumstances reasonably beyond the party's control. This includes fire, flood, earthquake, volcanic eruption, explosion, lightening, wind, hail, tidal wave, landslide, act of God or any other physical event.

26. ASSIGNMENT. Client may not assign its rights or obligations under this Agreement without AllConnected's prior written consent which shall not be unreasonably withheld.

27. COUNTERPART AND ELECTRONIC SIGNATURES. This Agreement may be executed in any number of counterparts, each of which shall be deemed to be an original and all of which together shall be deemed to be one and the same instrument. The Client's electronic signature of this Agreement shall have the same validity and effect as a signature affixed by the Client's hand.

28. ENTIRE AGREEMENT. This Agreement constitutes the entire agreement by and between the Parties regarding the subject matter contained herein, and supersedes all prior and contemporaneous undertakings and agreement of the Parties, whether written or oral, with respect to such subject matter.

Company: Camrosa Water District

Print Name:

By: _____

Date:

Print Name:

By: _____

Date:

AllConnected, Inc.

Print Name:

By: _____

Date:

ADDENDUM A

NETWORK SECURITY & DATA PROTECTION POLICY v1.24

Client understands and agrees that data loss, security breaches, or network failures may occur, whether or not foreseeable, if the Client fails to maintain proper security for its computer and information system including software and hardware updates. Client therefore warrants that, unless otherwise set forth in a separate SOW and/or SLA, it will follow software and hardware updates and maintain specific security standards, policies, procedures meeting or exceeding those set forth below:

- Business Grade Anti-Virus Software will be Installed on all desktops, laptops and servers.
- Ensure that all Critical or Security Related Operating System & 3rd Party Software Patches are Installed on desktops within 2 to 7 Days and are installed on Servers within 30 days of their release. This Includes, but is not limited to Anti-Virus Software, Operating System Updates and 3rd Party Application Patches such as Adobe, Java, Flash etc.
- All External Network Gateways (including the Cloud) are Protected by a Business Grade Firewall with a Comprehensive Security Subscription including Intrusion Detection, and that such subscription is licensed at all times and is downloading and applying new signatures as they are made available.
- All Critical Data is Backed Up on at least a Daily Basis & Test Restores of all Back-Ups are Verified on a Quarterly Basis. All Back-Ups are Stored in a Secure Location Offsite or in a Fireproof Safe (Minimum 2 Hour).

If applicable Protected Health Information (PHI) is stored on client computer and information system:

- All Systems (Laptops, Workstations, And Servers) and Devices (Smartphones, USB Drives) Storing Personally Identifiable or Protected Health Information must be Securely Overwritten or Wiped Using an Approved Secure File Deletion Utility or Third Party Company that maintains Industry Certifications such as ISO-27001, ISO-14001, ISO-9001 upon decommission of the device to ensure that the information cannot be recovered.
- All Portable Devices (such as Laptops, Tablets and Smartphones) containing Personally Identifiable or Protected Health Information will use Industry-Accepted Full-Disk Encryption Technologies*.
- All Removable and Easily Transported Storage Media (such as USB Drives or CDS/DVDS) containing Personally Identifiable or Protected Health Information must use Industry-Accepted Encryption Technologies*.

* "Industry-Accepted" Means Accepted by the Cryptographic Community.

smartCONNECT PROPOSAL

allconnected

Phone: +01.805.526.1455
E-mail: help@allconnected.com
www. allconnected.com

Co- Managed IT Solution for

Camrosa Water District

CAMROSA WATER DISTRICT

Prepared for
Camrosa Water District

7385 Santa Rosa Road
Camarillo, CA 93012

Alan McDonald

CEO
805.475.5001
alanm@allconnected.com

Proposal issued:
Dec 1, 2021

Proposal valid
to: Jan 31, 2022

Alan Mcdonald
President & CEO

AllConnected ensures that our clients are prepared to defend against and operate during today's threats to IT Infrastructure. We prevent 3 of the top IT risks facing organizations:

Data Loss Downtime Security Breaches

4514 Ish Drive
Simi Valley. CA
USA, 93063

Phone: +01.805.526.1455

E-mail: help@allconnected.com
www. allconnected.com

CONTENT

Contents

ALLCONNECTED

SUCCESS

Our team of about 30 employees has an average tenure of nearly 10 years with the organization and are organized into functional teams that report directly to a team manager. In addition, we retain a North American bench of thousands
of engineering resources through the Ingram Micro Trust X Alliance network. We have been members of this network since 2002 and leverage it to deliver services outside of our coverage areas, during emergencies, or when clients request services that are not part of our core expertise.

OUR STORY

AllConnected
Preparing IT for Survival

Alan (CEO) and Richard (CTO) designed our managed IT services around the prevention of data loss, downtime, and security breaches. AllConnected's roots began in 1993 when our founder, Alan McDonald, began a consulting practice focused on the healthcare industry. Back then, we were known as Integrated Computer Systems.

As connectivity continued to have a more significant impact on the way businesses collaborate and access information, we changed our name to AllConnected in 1998.

AllConnected participates in networking and collaborating with our vendors, our peers, and manufacturer partners at a national and North American level. Our active participation in the Trust X Alliance network gives us immediate access to resources within this group of nearly 400 IT Service Providers, representing over $2B in annual sales, as well as the Ingram Micro Service Network with thousands of certified professionals we can dispatch to supplement projects we manage throughout North America.

Our President & CEO, Alan McDonald, previously served as the Co-President for the VentureTech North American network, and has sat on multiple advisory councils, including Cisco, N-able, and Asigra. This is one way that we focus on staying very involved in our industry.

AllConnected

Management Team

Our company operates on critical core values that form the basis for our relationships, our approach to technology, and our passion to provide great service to our customers.

Alan McDonald

President & CEO

Alan is responsible for providing the strategic direction, leadership, and vision for AllConnected. As President, he focuses AllConnected's team on delivering managed network services, as well as private cloud and business continuity solutions.

Richard Pressler

CTO

With an extensive background in data center and security, Richard drives AllConnected's best practices, project design, and architecture. Richard also identifies the relevant education technology investments necessary to ensure our clients can become efficient, competitive, and secure.

Charles Takahashi

DRaaS Director

Charles leads AllConnected's efforts in providing advanced Recovery Services to our clients. With a specific focus on Disaster Recovery Testing, and the creation of DR Runbooks, Charles efforts ensure clients are always ready to meet predefined RPOs and RTOs.

Taylor Herlihy

Service Manager

Taylor supports the NOC and service desk by coordinating the technical teams at AllConnected. Working with our technical leads at our clients, his job is to ensure a successful deployment and transition of the new AllConnected Service Solution.

Dominik Azam

Technical Alignment Manager

Dom is one of our senior TAMs, responsible for managing all aspects of the relationships we maintain with our managed clients. He works closely with our CTO and Service Manager to ensure our client's strategic and technical needs are met.

Eddie Cardenas

Controller

For over a decade, Eddie has helped AllConnected by providing guidance in regard to financial decisions. He monitors and enforces important policies and procedures related to our accounting and purchasing departments.

RECURRING MAINTENANCE SCHEDULE

Systems

24x7: Monitoring of up/down status; Hardware Health; AVD licensing, monitoring and management
Weekly: Supported Microsoft systems critical and security patching; covered third party patching
Quarterly: Hardware Lifecycle Planning; Asset Inventory
As Needed: Basic Remediation Management (i.e. device failure)

Network

24x7: Monitoring of up/down status; Hardware Health; ISP Monitoring
Quarterly: Hardware Lifecycle planning; Firmware Vulnerability Reporting; Capacity/Performance Reporting; Firmware update management; External security scan and brief analysis (up to 50IPs); Asset Inventory
As Needed: Basic Remediation Management (i.e. device failure)

Datacenter

24x7: Monitoring of up/down status; Environment monitoring; UPS monitoring
Quarterly: Hardware Lifecycle planning; SAN-Capacity monitoring/ reporting; San-Performance monitoring/ reporting; SAN Fabric - Performance monitoring/reporting; Update VMware VCenter and ESXi Servers; Update storage infrastructure to recommended firmware; Firmware update management; Asset Inventory
As Needed: Update existing data center documentation

SCOPE OF WORK

Monitoring, Alerting and Remediation

ACI performs 24x7 monitoring on all protected devices. During their shift the NOC team will be alerted of trends that may be negatively impacting your network and work towards a solution. Critical Issues are escalated to our NOC 24x7

Routine Maintenance

Your monitoring and maintenance solution is configured according to best practices. We have developed and continually update our comprehensive set of policies covering proper support and maintenance such as: threshold monitoring of CPUs disk-space, RAID arrays and more.

Support Contract Management

To maximize a stable network, we may recommend the replacement of critical items to mitigate high-risk vulnerabilities or unstable devices in your network. Any new upgrades, installations or other changes to your environment need to be coordinated with our service desk to ensure we are aware of approved changes to your environment.

Technical Review, Reporting and Planning

We provide your organization with the data and analysis necessary to proactively operate the environment. We provide this info during our Technical Business Review meetings. These reports come from the data gathered through our monitoring tools, manufacturer alerts and reports, and our knowledge and experience in the industry.

AllConnected agrees to provide client with the services described in this Scope of Work. Our smartConnect contract is designed to support your organization, ensuring that key critical components of your network infrastructure are monitored, critical issues are escalated, and critical patches for supported Windows-based operating systems, network equipment, hypervisors, storage arrays, and UPS gear are kept current.

MANAGED SERVICES

DELIVERING SOLUTIONS FOR CLIENT NEEDS

AllConnected is a trusted CMAS (California Multiple Awards Schedule) supplier of IT Services with examples of multiple projects in municipalities, water districts, private businesses, and educational facilities. We also participate in networking and collaborating with our vendors, peers, and manufacturing partnersacross North America.

Cyber-Security Solution

NIST CYBERSECURITY FRAMEWORK

The Cybersecurity threat landscape has become much more sophisticated in recent years. While proactive and defensive technologies help to protect critical network infrastructure and sensitive data sets, the NIST 800-171 Cybersecurity framework outlines how organizations should Detect and Respond to breaches.

Barracuda Email Essentials (ESS)

Email Security: a comprehensive and affordable cloud-based email security service with a granular series of filters and malware management components, allowing greater flexibility and stronger threat protection. It protects both inbound and outbound email against the latest spam, viruses, worms, phishing, and denial of service attacks.
Advanced Threat Protection (ATP): analyzes inbound email attachments and publicly accessible direct download links in a separate, secured cloud sandbox, protecting against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Service virus scanning features. ATP is included with all Essentials bundles.

PhishLine End-User Training

Barracuda email protection stops over 20K spear phishing attacks every day. PhishLine leverages that extensive threat intelligence to create real-world simulation and training content aligned with all identified email threat types. Users will learn to spot business email compromise, impersonation attacks and other top emails threats. Educate to mitigate risk, analyze user behavior, and simulate email threats.

Anti-Virus Defense (AVD)

Our toolset leverages Bitdefender, a leader in cybersecurity delivering best-in-class threat prevention, detection and response toolsets worldwide. Bitdefender labs discovers 300 new threats eachminute and validates 30 billion threat queries daily.
With customer in 170 countries around the world Bitdefender guards millions of consumer, business and government environments, the industry's trusted expert for eliminating threats, protecting privacy and data, and enabling cyber resiliency.

End-Point Detection and Response (EDR)

Block threats before they target you. This solution delivers next generation antivirus that stops today's complex attacks. Simplify security investigations with advanced EDR and a broader context on endpoint, web, email, and network data. Achieve up to a 97% reduction in time to respond to and remediate an attack. Automate threat responses with one-click isolation of an infected host.

Coverage Breakdown

Server Monitoring, Alerting and Updates	8
Firmware Update Management (Physical Servers Only) Application	2
Health Check, Service Packs and Roll-Ups	0
End User Company Owned Devices	85
Network Infrastructure Monitoring, Alerting and Updates	8
Configuration Backup w/NetFlow	10
Monitored Network Element	0
External Security Scan & Brief Analysis(up to 50 IP's)	1
DC Hypervisor Monitor, Alerting and Updates	8
DC Network Element	0
UPS coverage	1
Security and Phishing Training Subscription *	25
Email Advanced Threat Protection *	25
Advanced Malware Protection (EDR Solution)*	
Technical Business Reviews	25
-	
Security Analysis and Threat Remediation	
Technical Alignment Management	
Helpdesk Support	
Adv. Engineering Services	
-	
Protected VMs Plan (BaaS | Health Monitoring, Job Management)	
Secure Cloud Backup (Offisite Data Protection| 3-2-1 Compliance)	

*Per User

ON-BOARDING SCHEDULE

ALLCONNECTED WILL DELIVER SERVICES ACCORDING TO THE FOLLOWING SCHEDULE:

	WEEK 01	WEEK 02	WEEK 03
PHASE 01			
PHASE 02			
PHASE 03			
PHASE 04			

**** Standard is based off a normal on-boarding period, any adjustments due to hardware, systems, project delays will be communicated to client***

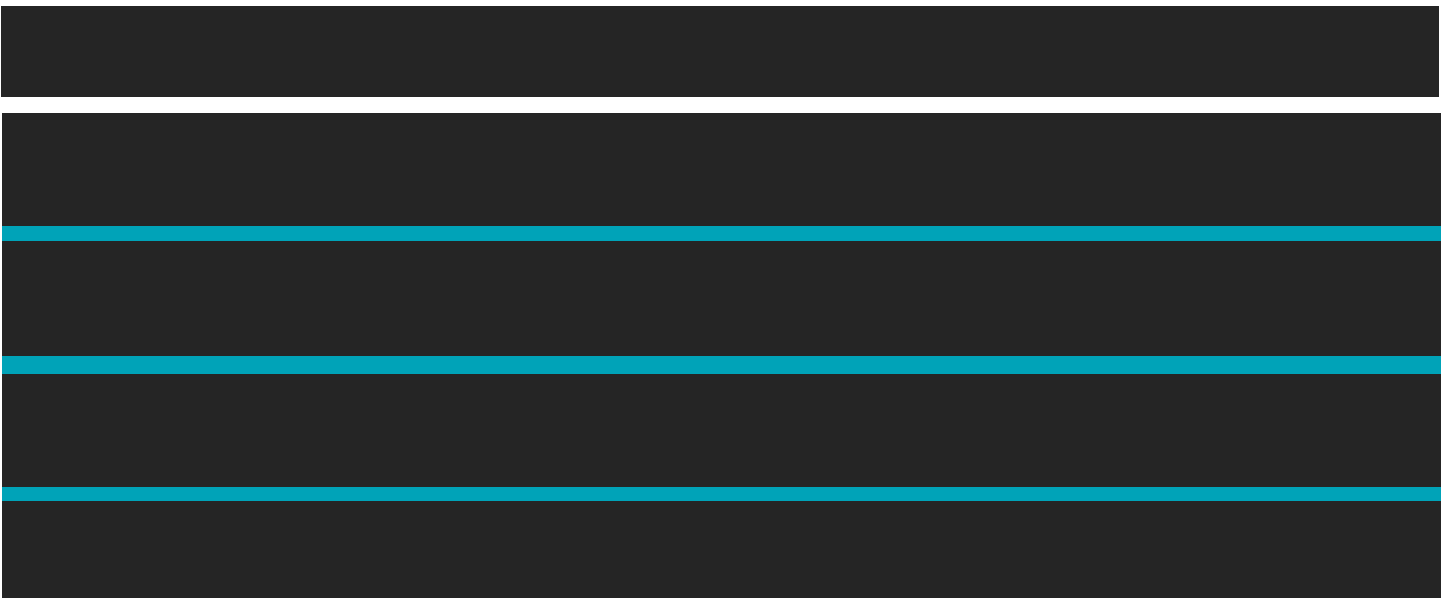
PHASE I STANDARD* DAYS 1 - 14

- Internal kick-off meeting with the deployment team
- Installed probe(s) and ACI managementtools in client environment
- Apply service templates for servers with specific roles and specific hardware
- Create alert flowchart with priority 0
- Pro-rated billing begins

PHASE II STANDARD*: FIRST 30 DAYS

- Collect all third-party vendor informationand add ACI as a contact where applicable
- Confirm asset information and start a complete inventory
- Discuss and set a tentative maintenance window for after hour upgrades
- Schedule any firmware upgrades as needed

WEEK 04 WEEK 08 WEEK 12



PHASE III STANDARD*: FIRST 60 DAYS

- Set and tune alerting thresholds
- Decide on imaging software and set up a standard image
- Confirm that all devices are showing with no errors in Solar Wind's N-Central
- Perform firmware upgrades as necessary

PHASE IV STANDARD*: FIRST 60-90 DAYS

- Complete first draft of network documentation and site topology
- Create and deliver the first TBR report

TERMS & CONDITIONS

PROFESSIONAL SERVICES

Our team will regularly review your environment and make recommendations that help keep your environment performing well, ensure it is secured properly, and can scale. While we do not require that all our best practices be implemented, or that they are implemented all at once, there are some issues that may require high prioritization. Such will be escalated as soon as possible. Our goal is to deliver a cost-effective private cloud, protect our client's networks properly, and offer effective disaster recovery solutions which may incur additional expenditures. we may recommend that a critical item be replaced to mitigate a potentially high-risk vulnerability in your network. If such device is not replaced in a timely manner, remediation of any damage will not be covered within the scope of our agreement.

HELPDESK SERVICECS

In general, Helpdesk support involves day to day troubleshooting, remediation and related tasks surrounding individual users and their systems. I.E. Password issues, Application Installation/Configuration, New Workstation Deployment, Virtual On-Boarding and Off-Boarding of Employees. This contract does not include unlimited support from our engineers when conducting remediation work. Billable time will be applied to (if available) labor retainer funds, ongoing work may result in the generation of overage invoices. While we use best industry practices and tools we cannot guarantee successful remediation of issues resulting from security denial of service or other Internet based attacks, recovery related issues or remediation of problems caused by updating 3rd party or proprietary software

HOURS OF SERVICE & TARGET SLA(S)

AllConnected reserves the right to schedule maintenance windows from 12am to 5am as needed with prior approval of the client. Standard business hours are 8AM to 5PM PDT Monday through Friday, expect Holidays. Our Service Team can be reached by email, phone and through our website, a customized contact sheet with this information will be provided. Our standard response times and incident handling targets (SLAs) are as follows:

New Tickets: 9x5 Response within 60 minutes which may come in the form of emails, phone calls, etc. Develop a resolution plan within 6 business hours and resolve the issue within 48 hours for standard requests; if more time is required, client will be contacted

High Severity* Issues: Response time is within 60 minutes, develop a resolution plan within 2 hours. Resolve the issue within 4 hours.

*Identified as a serious and/or complete interruption to normal business for entire departments and/orcompany-wide

After Business Hours: After-hours and /or weekend support will be responded to by the following business day [Exception:High Severity issues, SLA response within4 hours & 24hours resolution time] and aresolution planwithin 48 hours.

CUSTOMER RESPONSIBILITIES

Customer is responsible to protect all account passwords and account access whether authorized or not. Customer shall comply with all rules regarding networks that customer accesses via AllConnected's services. Customer acknowledges that information which is confidential should not be transmitted over or reside on any computer connected to the internet. Customer shall not transmit or make available via the Internet any material that is illegal, libelous, or may result in action against AllConnected or any AllConnected customer. Customer shall not use any AllConnected equipment, electronic mail address, or AllConnected service to send or facilitate an unsolicited email, commercial, or otherwise. All emails shall (a) comply with all elements of the federal CANSPAM act of 2008, (b) only be sent to recipients that have voluntarily registered to receive emails from customer, (c) contain Customer's physical mailing address and (d) contain a link or instructions that allow recipients to remove themselves from Customer's email distribution list. Customer shall not use AllConnected service in any way that is unlawful or violates any right of any person or entity. Customer shall not resell the service to any third party, whether in Customer's building or not, without AllConnected's prior written approval.

PAYMENT, CONTRACT PERIOD AND TERMINATION TERMS

The smartConnect setup fee is invoiced within 15 days of the completion of OnBoarding phase I. Unless otherwise agreed, AllConnected bills service charges one month in advance, due Net 30 days. Service charges for an initial partial month will be prorated. Overages will be billed separately and are due within 30 days. Any additional reimbursable expense or charges not included in the fees set forth above are payable upon receipt of invoice by customer. ACI will provide client with materials and service as outlined in this agreement. Client agrees to pay for all Client requirements for all goods and services according to the terms and conditions of this agreement and MSA including increases to materials and/or services. Failure to comply with these payment terms constitutes a breach of this agreement and may cause interruption and/or cancellation of all services provided. Price quotes are based on a 36-month contract term. This agreement is effective on the date of final signature and will continue through June 30th, 2025. Renewal of this agreement beyond the contract term is optional under the condition both client and AllConnected wish to proceed. Upon contract and service termination any unpaid services including any initial implementation costs will be billed and due in full. All VM, application and data protection is terminated. AllConnected reserves the right to terminate the contract and services if client fails to make monthly payments. MSA section 2 covers all other pertinent termination terms.

ESTIMATE & SIGN OFF

NO	OPERATION	COSTS
01	smartConnect	$ 4,432.27
02	recoverConnect	$ 2,636.50

ALLCONNECTED, INC
Alan McDonald, President & CEO

BY: _____
DATE: _____

SUBTOTAL	$ 7,068.77
ACI APPLIANCE	$ 41.67
***BACKUP APPLIANCE**	$ 379.00
MONTHLY TOTAL	$ 7,489.44
ONE TIME ON-BOARDING FEE	$ 15,000.00

CAMROSA WATER DISTRICT

PRINT NAME: _____
BY: _____
DATE: _____

PRINT NAME: _____
BY: _____
DATE: _____

AGREEMENT

Agreement and Notice to Proceed
This addendum and attached MSA supplement each other and should be read together. I agree that I represent the organization listed and am authorized to enter into this agreement.

*Appliance rental and Licensing invoiced through Ingram Micro, Inc.

THANK YOU

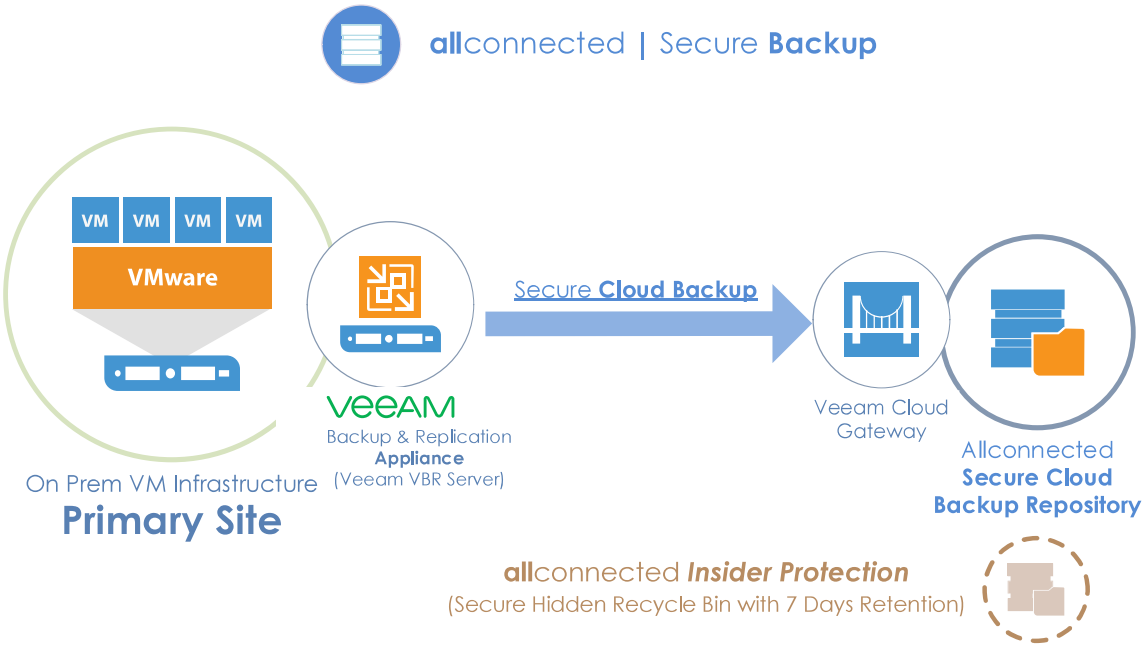
4514 Ish Drive, Simi Valley,
CA, 93063
Phone: +01.805.526.1455
help@allconnected.com
www.allconnected.com

allconnected

smartBackup | Solution Design

Our Managed Backup Technical Solution features the following:

1. **On Prem Data Backups** via our Managed Hardware Appliance
2. **Offsite Data Backups** via our Secure Cloud Backup Repository
3. **Allconnected *Insider Protection*** with the "hidden secure recycle bin" to add a layer of defense against advanced cyber attacks, including ransomware that involve the deletion of On Prem and even Cloud Backup Files



smartBackup | Quote

Service | Description | Quantity and Costs

Cloud Backup

Secure Cloud Backup (Offsite Data Protection | 3-2-1 Compliance)

Secure Cloud Backup | 15 TB Protection Plan w. Insider Protection	$ 1,000.00

- **Secure Offsite Cloud Repository:** Ensure compliance with the 3-2-1 Rule by maintaining Data Backups on prem as well as to Allconnected's Secure Cloud Backup
- **Centralized Backup Management:** A single centralized console provides complete visibility into the backup solution
- **Full Encryption Options:** In addition to data always being encrypted in transit, data encryption can be configured at the source and at rest
- **Item Level Granular Restoration:** Recover VMs, VMDKs or individual files such as SQL databases or mailbox items
- **Office 365 Protection:** Ensure Critical Exchange Online, SharePoint Online OneDrive for Business and Microsoft Teams Data is always protected
- **Cloud Connect Licensing and Cloud Backup Bandwidth:** Included

Recovery Services

Insider Protection

- **Advanced Protection Included: Insider Protection** provides an additional layer of defense against cyber threats such as **ransomware** that involve advanced data destruction attacks targeting the deletion of backup files.
- **Secure Recycle Bin:** Deleted files are auto-moved to a secure location that is not accessible to clients

* Additional charges apply during a data recovery request using Insider Protection
* A GFS Backup Scheme must be configured for Secure Cloud Backup Jobs to ensure data recoverability

Managed Backup

Protected VMs Plan (BaaS | Health Monitoring, Job Management)

"smartBackup 15" Protection Plan | Up to 15 Protected VMs	$ 1,195.00

Managed Backup (BaaS)

- **Allconnected Managed Veeam Backups:** Job Monitoring, Reporting, Health Checks & RPO Managed by our Expert Team (Standard On Prem & Cloud Backup Retention is 30 Days)
- **Appliance Management:** We Monitor, Update & Patch and Provide HW Support
- **Veeam VCSP Backup Licensing:** Included
- **Veeam Updates and Patch Management:** We ensure Version Updates & Hotfixes
- **Veeam Backup Restore Test:** 1 Veeam Backup Restore Test per Year (Basic VM Restore or Item Level)
- **Yearly Backup Health Report:** Data protection findings & recommendations, appliance life cycle planning

Appliance

ACI Backup Appliance

"Seconda" C240 M5	Cisco 8 x 5	20 Cores	64 GB	24 TB Useable (36 mo. RENTAL)	$379/mo

* If selected, rentals are through the Ingram Micro Rental Program and actual monthly invoice may vary slightly from above quote. Taxes additional.

Veeam Licenses

Lic. **Veeam VCSP Microsoft Office 365** Licenses (Per User)	25	$ 2.50	$ 62.50

Onboarding Project

Managed Backup Professional Onboarding (Pri Site)	$5,000

Monthly Costs Total **$ 2,636.50**

Veeam Product Support:

Depending on your licensing model, technical support for your On Premise Veeam product is included in the licensing model that you selected at the time of purchase.*

a. Veeam On-Premise VCSP Subscription Licensing (per VM):
   i. Support is provided by AllConnected as your Service Provider. Escalation to Veeam included as necessary.
   ii. Basic Support is 12x5, Advanced is 24x7 (additional charges apply)
   iii. Support can be reached by contacting: draas.support@allconnected.com | 1-805-526-1455

Support Program	Business Hours
12x5 Support	Mon-Fri, 8am - 8pm PST
24x7 Support	24 x 7 x 365**

* Technical support does not include custom recovery scenarios, advanced consulting, or onsite service.
** Support requiring Systems or networking engineers will be billed as Professional Services

Veeam Cloud Connect Support:

Support is available for AllConnected customers with our Hosted Cloud Connect Replication and Cloud Connect Backup Services for Veeam Cloud Connect product and service related issues. Support can be reached by contacting: draas.support@allconnected.com | 805-526-1455

Support Program	Business Hours
12x5 Support	Mon-Fri, 8am - 8pm PST
24x7 Support	24 x 7 x 365**

Additional AllConnected Professional Services Support:

Disaster Recovery Professional Services are available on a per hour basis.

a. L1 Engineer: $150/hour
b. L2 Engineer: $185/hour
c. L3 Engineer: $225/hour
d. Architect: $255/hour

Service Level Agreement:

1. AllConnected ensures 99.95% uptime for our Veeam Cloud Connect Resources
2. AllConnected DRaaS Essentials Services includes Managed Backup & Replication
3. AllConnected ensures availability of the Veeam Backup Repository per each client's configuration for Cloud Connect Backup Services
4. AllConnected ensures availability of each tenant's Replica Storage and Hardware Plan per each client's configuration for Veeam Cloud Connect Replica/Replication Services.
5. If Service Levels are not maintained by AllConnected, clients may be eligible for a credit towards a portion of the monthly service fees.
6. **Monthly Maintenance:** Downtime incurred for scheduled maintenance windows such as for the purposes of major Veeam Update Deployments are not subject to the uptime metrics. The 1st Sunday of the month is reserved from 10am-6pm PST for maintenance. A 48 hour minimum advance notice would be sent for any maintenance scheduled outside of this window.
7. **Service Credits:** Service Credits are your sole and exclusive remedy for any performance or availability issues for any Service under the Agreement and this SLA. You may not unilaterally offset your Applicable Monthly Service Fees for any performance or availability issues. Service Credits apply only to fees paid for the particular Service for which a Service Level has not been met. The Service Credits awarded in any billing month for a particular Service will not, under any circumstance, exceed your monthly service fees for that Service in the billing month.

Monthly Uptime Percentage	Service Credit
<99.95%	25%
<98.0%	50%
<97.0%	75%
<95.0%	100%

8. **Limitations:** This SLA and any applicable Service Levels do not apply to any performance or availability issues:
   a. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center);
   b. That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;
   c. Caused by your use of a Service after we advised you to modify your use of the Service, if you did not modify your use as advised. Client will be given a minimum of 30 days to comply with the advised modifications;
   d. That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;
   e. That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;
   f. That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);
   g. That result from your attempts to perform operations that exceed prescribed quotas or that resulted from ourthrottling of suspected abusive behavior;
   h. Due to your use of Service features that are outside of associated Support Windows.

Emergency Data Recovery or DR Event Support (DR Failover is only available for ACI managed Replication clients)	
Full Site Failover Event * (per event base charge) 1.Disaster Event Phone, Email and Messaging Support (Up to 20 Support Hours) 2.Veeam Failover Plan execution with pre-configured vm boot up 3.Failover to off-site recovery environment 4.Baseline VM verifications (OS and Network availability) 5.NEA and Public IP verifications 6.After the included 20 hours are exhausted, on Demand Support @ $225/hr is available * Client is responsible for Application Recovery and Verifications. Only available for ACI managed Replication clients.	**$5,000**
Full Site Failback Event * (per event base charge) 1.Disaster Event Phone, Email and Messaging Support (Up to 20 Support Hours) 2.Veeam Failback Plan execution with pre-configured vm boot up 3.Failback to primary site 4.Baseline VM verifications (OS and Network availability) 5.After the included 20 hours are exhausted, on Demand Support @ $225/hr is available * Client is responsible for Provisioning Primary Site Infrastructure and for Application Recovery and Verifications	**$5,000**
Partial Failover Event * (per VM charge) 1.Disaster Event Phone, Email and Messaging Support 2.Veeam Failover of Selected VMs 3.Failover to off site recovery environment 4.Baseline VM verifications (OS and Network availability * Client is responsible for Application Recovery and Verifications. Only available for ACI managed Replication clients.	**$300**
Partial Failback Event * (per VM charge) 1.Disaster Event Phone, Email and Messaging Support 2.Veeam Failback of Selected VMs 3.Baseline VM verifications (OS and Network availability * Client is responsible for Provisioning Primary Site Infrastructure and for Application Recovery and Verifications	**$300**
DR Cloud Activation * (per GB RAM per Hour) Takes affect during a Recovery Event. Failover only available for ACI managed Replication clients. .	**$0.04**
DR Cloud Activation * (per vCPU per Hour) Takes affect during a Recovery Event. Failover only available for ACI managed Replication clients.	**$0.08**
Insider Protection – Data Restore to Client's Veeam Appliance **(per TB Restored)** 1.Restore from Allconnected Secure Recycle Bin to Client's Appliance 2.Requires a secure connection to Client's Veeam Appliance from Allconnected's datacenter	**$250**
Insider Protection – Data Restore to Client Provided USB Drive or Storage Device **(per TB Restored)** 1.Restore from Allconnected Secure Recycle Bin to Client's USB Drive or Storage Device 2.Client must provide an appropriate USB 3.x Drive or Storage Device with sufficient capacity. Shipping costs extra.	**$300**
Insider Protection – Data Restore to Allconnected provided Storage Device **(Subject to availability. Per TB Restored)** 1.Restore from Allconnected Secure Recycle Bin to Allconnected Storage Device 2.Client must return Allconnected's Storage Device within 15 days or be charged MSRP costs. Shipping costs extra.	**$300**
DR Expert Support (per Hour on Demand)	**Cost**
ACI Recovery Services DR Expert Support * (per Hour) * For Professional Services On Demand Support Not Covered under the general Agreement	**$225**
ACI Recovery Services DR Expert Support - 10 Hour Retainer Per Month * For Professional Services On Demand Support Not Covered under the general Agreement	**$2,250**

ASSUMPTIONS, TERMS AND CONDITIONS

Cloud Backup & Replication Billing and Utilization:

1. Client maintains responsibility for the amount of data stored in the AllConnected cloud repositories.
2. Utilization will be monitored and reported on monthly.
3. Adjustments to the Price Plans will be made as needed including adjusting the Plans according to the number of Protected VMs or the required Cloud Backup or Cloud Replication Protection Plans.
4. Any additional on-demand services will be included in the monthly invoices.

Technical Requirements:

1. Clients must meet minimum technical requirements including maintaining the correct VMware ESX versions, Internet Bandwidth capacity, Physical Environment Requirements, SAN Storage Specifications, and approved Network Configurations. Appropriate rack space, network ports, power and cables must be provided by customer for any on premise Backup and Replication Appliances that are to be installed by AllConnected.
2. AllConnected cannot guarantee functionality and support for clients who do not meet the minimum requirements. Supported technologies and configurations are listed in the Veeam Supported Technologies list.
3. In the event that the client managed compute, network, or storage environment is interrupted, degraded or adversely modified or experiences any kind of failure, AllConnected is not responsible for interruptions in data backup or replication jobs.
4. Allconnected's DRaaS Essentials Solution Supports only Virtual Servers that meet the current Veeam Requirements. No Physical Servers are supported for the DRaaS Essentials Solution.

Contract and Service Termination Agreement:

1. Upon contract and service termination any unpaid services including any initial implementation costs will be billed and due in full.
2. Upon contract and service termination, all vm, application and data protection ends.
3. Upon contract and service termination, any data backups or replicas will be removed permanently from Allconnected owned devices, including cloud repositories.
4. Allconnected reserves the right to terminate the contract and services in the event that client fails to make the monthly payments.

Support:

1. Certain features, technical functionality and support services may be exclusive to a specific Allconnected Service such as Veeam Failover functionality that is available only to DRaaS Essentials or Tailored DRaaS customers that have signed up for the Allconnected Managed Replication Service.
2. Emergency Data Recovery or Disaster Recovery Professional Services are available on a per hour basis.
3. Support can be reached by contacting: draas.support@allconnected.com | 1-805-526-1455.

QUOTE: ACIQ15443-03 - CWD - AUXILIARY BLOCK FEB-JUNE 2022

allconnected

Prepare IT for Survival

EXECUTIVE SUMMARY

PREPARED FOR: Joe Willingham, Camrosa Water District
7385 Santa Rosa Rd., Camarillo, CA 93012
SHIP TO: 7385 Santa Rosa Rd., Camarillo, CA 93012

PREPARED BY: Alan McDonald, President, 805-526-1455 | alanm@allconnected.com

Auxiliary Support Agreement Term:
2/1/2022 - 6/30/2022
CMAS Contract #3-13-70-1346K
February 5, 2021 through October 11, 2022

DESCRIPTION	TOTAL
Camrosa Water District Auxiliary Support Agreement FY2022	$58,850.00

Services allocated against this agreement of $58,850 will be based on the attached CMAS rate structure. This amount includes:

$ 2,250: DevOps Additional Ramp (RFP p. 13)
$14,100: Engineering Additional Ramp (RFP p.13)
$42,500: Engineering/DevOps Ongoing Support 5 Months (5 x $8500)

- AllConnected's Service Manager and/or TAM will pre-schedule a majority of the remote/onsite labor for this Auxiliary Support Agreement.

-Labor expended within a calendar month will be invoiced against this agreement by the 10th of the following month, with NET30 terms.

- When over 75% of the agreement is utilized, AllConnected will advise Camrosa if approval for additional budget may be required. Reconciliation Reports can be provided upon request.

Per AllConnected's proposal dated 11/3/2021, this Auxiliary Support Agreement will cover technical and engineering resources including, but not limited to the following issues:

- Projects to better align Camrosa with AllConnected's NIST 800-171 based standards, regulatory compliance requirements recommended in our quarterly technology business reviews (cover page)
- Up to 14 hours per week of pre-scheduled onsite engineering support (cover page)
- Emergency work or remediation of security issues
- Engineering issues escalated from HelpDesk, including L1 Systems/Network Engineer, L2 Systems/Network/Data Center Engineer, L3 Systems/Network/Data Center/Security Engineer (item #1 of RFP)
- Supporting Camrosa's existing on-premise Hyper-V based solution to recover based on the 24hr Recovery Time Objective (RTO) and 24hr Recovery Point Objective (RPO). RPOs/RTOs will be validated by testing. (item #2 of RFP)
- Escalation/Management of issues related to existing Carbon Black contract (item #6 of RFP)
- Deploying new PCs (item #7 of RFP)
- Support Non-contracted Printers/Copiers/Scanners/Devices, or other systems on a best-effort basis, including the SuperMicro servers/storage with no service contract (item #10 of RFP)
- Moves/Adds/Changes for changes to the location, configuration of existing equipment or software, and installation of additional equipment or software as needed (item #14 of RFP)
- Support of the IBM Mobile Device Management solution (item #15 of RFP)
- Fortigate Administration
- Programming and Development (Addendum B)

DESCRIPTION	TOTAL
- Other Systems and Network Tasks to be determined (and not covered by our smartConnect agreement)	
Estimated NTE Auxiliary Support	**$58,850.00**

TERMS & CONDITIONS:

Terms are NET30 unless otherwise agreed upon.

In the event of a conflict between the master service agreement ('agreement') and this proposal, the terms of the agreement shall control.

Company: Camrosa Water District

Print Name: _____
By: _____
Date: _____

Print Name: _____
By: _____
Date: _____

AllConnected, Inc.

Print Name: _____
By: _____
Date: _____

allconnected

Network Availability Experts
*Virtualization * Storage * Remote Access * Business Continuity*

Professional Services Rates **(SLED Customers Only)**
CMAS Contract #3-13-70-1346K
February 5, 2021 through October 11, 2022

Thank you for choosing AllConnected, Inc. to assist you with the service, support and maintenance of your company's critical network systems and infrastructure. Our goal is to provide you with timely, professional IT service.

Our standard on-site response time for network consulting is 48 hours, excluding evenings, weekends, and holidays. [1] A two hour minimum is required for on-site consulting services. Phone support is billed in 15 minute increments, with a 15-minute minimum. Please refer to the table below for billing types and rates.

Technician/Engineering Role	*Standard Rate*	*CMAS Rate*
Field Technician (Technology Consultant)	$95	$82
L1 Network/Systems Engineer (Subject Matter Expert VI) [1]	$150	$141
L2 Senior Network/Systems Engineer ((Subject Matter Expert VI) [1]	$185	$174
L3 Expert Network/Systems Engineer (Subject Matter Expert VI) [1]	$225	$215
Expert Architect (Project Manager) [1]	$255	$245
Documentation Specialist/Technical Writer (Junior Technology Consultant)	$145	$136
Senior Project Management (Technology Consultant) [1]	$180	$162
Travel Hourly Rate [3]	½ of Base Rate	
Weekend/Evening or Emergency Rates	150% of base rate	
Holiday Emergency Rate [4]	175% of base rate	
Out of Region Service requests via the TrustXAlliance/IM-Link Network [5]	(varies based on work role, region)	

Network Consulting Rates (continued)

[1] L1 (Level 1) systems engineers hold a Microsoft MCTS or Cisco CCNA certification with 3+ years of experience in the IT industry.
L2 (Level 2) systems and network engineers have 5+ years of experience in the IT industry and hold the same certifications as L1 engineers plus one or more of the following certifications: Microsoft MCITP; Cisco CCNP/CCSP/DCUCD/DCUCI; Citrix CCA/CCEE; Network +, or a Microsoft specialization in key Applications or Security.
L3 (Level 3) expert specialist engineers have 10+ years of experience in the IT industry and focus on the architect and expert engineering role. L3's may also hold specific certifications with either VMware, Microsoft, Enterprise SAN, Cisco CCIE, Citrix CCIA, Security, or other high-end storage solutions.

[2] Service block agreements are to be paid in advance and are posted to your account as a block of dollars. Monthly statements will be provided that outline the status of your Service block agreement. Our agreement reconciliations include the date of service, the engineer servicing your account, and a description of the work performed on each visit. Block time does not apply to web development/updates/projects.

[3] Travel is calculated one-way and is billed by calculating the time it takes for our engineers to travel from his prior location to your office. If your location is outside of our 50 mile radius, additional charges apply for the trip back to our office.

[4] Holiday emergency support available only for xConnect customers.

[5] Service tickets are coordinated through AllConnected's Service Coordinator and dispatched to our North American service network. Rates may vary by region and work role.

Last Updated: April 2017

CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

Board Memorandum

January 27, 2022

To: Board of Directors

From: General Manager

Subject: **Closed Session Conference with Legal Counsel – Personnel**

Objective: Confer with and receive advice from counsel regarding personnel matters.

Action Required: No action necessary; for information only.

Discussion: Personnel matters may be discussed in closed session pursuant to Government Code section 54957.

CAMROSA WATER DISTRICT
BUILDING WATER SELF-RELIANCE

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. **Quarterly Investments Report (QE 12/31/21)**
B. **Cash Balances (12/2021)**
C. **Change Order Listing (as of 12/29/21)**
D. **2022 Board Calendar**

CAMROSA WATER DISTRICT
Statement of Investments
FY 21-22
For Quarter Ending: 12/31/21 (01/15/22)

			Date Of Deposit	Call Date	Beginning of Year Investment	Opening Balance	Closing Balance		Value at Maturity
LAIF	N/A	State Treasurer	Daily	Daily	13,774,265	29,080,564 -	$ 26,991,900 -	100.00%	$26,991,900 -
Total Laif					13,774,265	29,080,564	26,991,900	100.00%	26,991,900
				OTHER INVESTMENT TOTALS:	-	-	-	0.00%	-
				TOTAL OF ALL INVESTMENTS:	13,774,265	29,080,564	26,991,900	100.00%	

ACTIVITY FOR THE QUARTER:

LAIF

Transfers of fund to General Operations.	2,105,000
Transfer from Cash Receipts to LAIF	0
Quarterly Interest as of 12/31/21 for Qtr ending 01/15/2022	16,335

LAIF Performance Report

Apportionment Rate	0.23%
Earnings Ratio	0.00000625812849570
Daily	0.22%
Quarter to Date	0.21%

PMIA Average Monthly Effective Yield

Oct 2021	0.203
Nov 2021	0.203
Dec 2021	0.212

TREASURY BILL RATES (12/31/21)

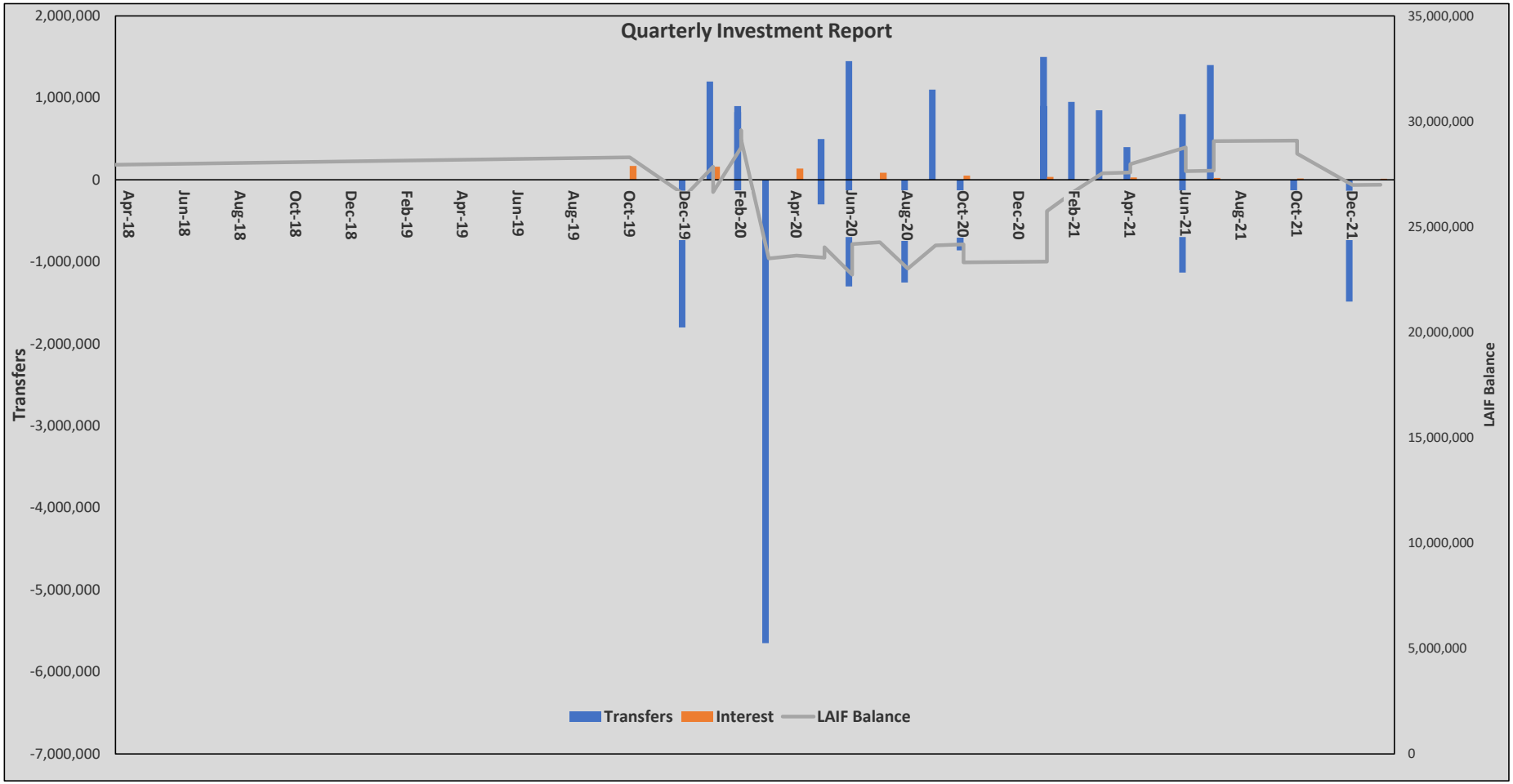
1 Mo	3 Mo	6 Mo	1 Yr	2 Yr	3 Yr	5 Yr	7 Yr	10 Yr	20 Yr	30 Yr
0.06	0.06	0.19	0.39	0.73	0.97	1.26	1.44	1.52	1.94	1.9

BOND RESERVES

	TYPE OF INVESTMENT	INSTITUION	DATE OF DEPOSIT	DATE OF MATURITY		PRINCIPAL INVESTMENT		ACCRUED INCOME	RATE OF RETURN
W & WW Rev Bonds Series 2016	LIQUIDITY FUNDS	BLACKROCK	10/19/2016	N/A		$ 879,529		$ 18.92	0.03%
						$ 879,529		**$ 18.92**	

BOND ACQUISITION FUNDS

	TYPE OF INVESTEMENT	INSTITUTION	DATE OF DEPOSIT	DATE OF MATURITY		PRINCIPAL INVESTEMENT		ACCRUED INCOME	RATE OF RETURN
W&WW Rev Bonds Series 2016	WATER ACQUISITION FUND	BLOCKROCK	10/19/2016	N/A		$ 3,165,723		$ 67.64	0.03%
W&WW Rev Bonds Series 2016	INSURED CASH SHELTER ACCOUNT WASTE WATER	WILMINGTON TRUST	N/A	N/A		$ 13,801			0.10%
						$ 3,179,523		**$ 68**	


Quarterly Investment Report
Transfers
LAIF Balance
2,000,000
1,000,000
0
-1,000,000
-2,000,000
-3,000,000
-4,000,000
-5,000,000
-6,000,000
-7,000,000
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
Apr-18
Jun-18
Aug-18
Oct-18
Dec-18
Feb-19
Apr-19
Jun-19
Aug-19
Oct-19
Dec-19
Feb-20
Apr-20
Jun-20
Aug-20
Oct-20
Dec-20
Feb-21
Apr-21
Jun-21
Aug-21
Oct-21
Dec-21
Transfers
Interest
LAIF Balance

FUNDS FY 21-22

UNRESTRICTED FUNDS	JULY	AUGUST	SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER		JANUARY
LAIF	29,063,071.14	29,063,071.14	29,063,071.14	28,460,564.62	28,460,564.62	26,975,564.62	1,6	
UNION BANK DEPOSIT ACCOUNT	540,806.84	652,148.31	637,269.75	640,504.35	858,977.39	2,061,808.15		
UNION BANK DISBURSEMENTS ACCOUNT	709,022.24	1,191,275.90	493,799.34	693,438.01	377,068.20	496,555.47		
BANK OF AMERICA-RTL ACCOUNT	402,940.55	521,841.75	164,260.51	363,986.18	851,744.00	173,784.83		
TOTAL	$ 30,715,840.77	$ 31,428,337.10	$ 30,358,400.74	$ 30,158,493.16	$ 30,548,354.21	$ 29,707,713.07		$ -
RESTRICTED FUNDS								
PAYMENT FUND 2016	83.30	179.53	271.13	356.63	444.98	848,715.63	2,3,4	
RESERVES 2016	879,528.69	879,528.69	879,528.69	879,528.69	879,528.69	879,528.69	2	
WATER ACQUISITION FUND 2016	3,438,209.23	3,253,934.00	3,253,934.00	3,253,934.00	3,165,722.60	3,165,722.60	3	
INSURED CASH SHELTER ACCOUNT (Wastewate	13,793.94	13,795.70	13,797.40	13,798.57	13,799.70	13,800.87	5	
TOTAL	$ 4,331,615.16	$ 4,147,437.92	$ 4,147,531.22	$ 4,147,617.89	$ 4,059,495.97	$ 4,907,767.79		$ -
GRAND TOTAL	$ 35,047,455.93	$ 35,575,775.02	$ 34,505,931.96	$ 34,306,111.05	$ 34,607,850.18	$ 34,615,480.86		$ -

Series 2016-Reserve Fund

Cusip Number	Financial Institution	Settlement Date	Coupon Rate	Maturity	Amount	Accrued Income
09248u445	Blackrock Liquidity Funds	10/19/2016	0.03%	N/A	879,528.69	18.92

Series 2016-Water Acquisition Fund

Cusip Number	Financial Institution	Settlement Date	Coupon Rate	Maturity	Amount	Accrued Income
09248u445	Blackrock Liquidity Funds	10/19/2016	0.03%	N/A	3,165,722.60	67.64

ANTICIPATED OUTFLOWS	
Water Purchases December 2021	262,803.02
Payroll PR 1-1, 1-2 & ME	300,000.00
AP Check Run 1/5 & 1/19	1,205,000.00
Large CIP Project Payments	-
Bond Payments	-
	$ 1,767,803.02

FINANCE MEETING

DATE **1/20/2022**

Tony Stafford -General Manager

Tamara Sexton-Finance Manager

Sandra Llamas-Senior Accountant

MEETING NOTES:

1. A transfer from LAIF to operations in the amount of $1,485,000 took place on December 15, 2021.
2. The Reserve Fund earned $18.27 in interest in the month of December. The full amount was transferred to the Payment Fund
3. The Water Acquisition Fund earned $66.22 in interest in the month of December. The full amount was transferred to the Payment Fund
4. Camrosa transferred $848,186.16 into the 2016 payment fund for principal and interest payment due on January 15th.
5. The Insured Cash Shelter Account earned $1.17 in interest in the month of December
6. LAIF's average monthly rate of return for the period was 0.212%

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**	**$ 72,952.49**							
											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
	2019-58				Cannon Corporation	12/13/2018	BD		$ 100,705.00	$ 71,765.00	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**	**$ 230,631.11**							
	2017-30				MNS Engineeers, 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	
					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**	**$ 1,985,126.07**							
	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	
600-15-01		**Pressure Zone 2 - 3 Pump Station**	**$ 1,280,000.00**	**$ 61,237.43**							
	2015-55	Engineering Design PZ 2 to 3			Perliter & Ingalsbe	4/23/2015	BD		$ 33,200.00	$ 33,200.00	Award and up to $5,000 out-of scope
						11/19/2015	BD			$ 30,000.00	Additional out-of-scope $30,000 Flo Science
						11/19/2015	BD	CO #1	$ 22,425.00	$ 22,425.00	Surge Analysis
						9/13/2018	BD	CO #2	$ 14,706.00	$ 17,312.00	Additional design and construction services
						3/20/2019	GM	CO #3	$ 2,900.00	$ 2,900.00	Control diagram drawing
						8/8/2019	BD	CO #4	$ 18,526.00	$ 18,526.00	Engineering & construction support
						9/22/2019	GM	CO #5	$ 3,000.00	$ 3,000.00	T&M electrical engineering support & other technical services as needed
						8/23/2021	GM	CO#6	$ 4,200.00	$ 4,301.00	As-Builts
										$ 131,664.00	
	PW19-03				Pacific Hydrotech Corporation	8/8/2019	BD		$ 1,059,401.00	$ 1,059,401.00	Construct pump stations
						5/29/2020	GM	CO #1A	$ 16,953.91	$ 11,953.91	Mismarked waterline rock excavation- Negotiated down from $16,953.91
						5/29/2020	GM	CO #1B	$ 887.95	$ 887.95	Adjustment to Discharge Tie-in Point
						5/11/2021	GM	CO #2	$ 11,500.00	$ 2,415.31	Extra work resulting in replacing of electrical for pump and motor
										$ 1,074,658.17	
650-15-01		**PV Well (Lynwood Well)**	**$ 5,967,000.00**	**$ 61,121.76**							
	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	
600-20-02		**Conejo Wellfield Treatment**	**$ 11,275,000.00**	**$ 1,090,186.45**						**$ 3.00**	
	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	
400-22-01		**District Headquarters Security**	**$**	**300,000.00**	**$**	**69,785.97**						
	2020-75					J. E. Armstrong	2/12/2020	GM		$ 18,900.00	$ 18,900.00	Architect interior remodel
							11/5/2020	GM	CO#1	$ 4,977.50	$ 4,977.50	ADA Compliance additional electrical engineering work
							12/9/2021	BD	CO#2	$ 1,538.76	$ 1,538.76	
											$ 25,416.26	
	FY22-0074					Apex	8/5/2021	BD			$ 208,500.00	
							9/20/2021	GM	CO#1		$ 3,620.00	remove concret & install
							10/18/2021	GM	CO#2		$ -	declined
									CO #3		$ -	declined
							10/18/2021	GM	CO#4		$ 500.00	install tile & stone
							11/9/2021	GM	CO#5		$ 1,955.00	Seal parking lot area
							11/9/2021	GM	CO#6		$ 2,070.00	Install 2 8" pipe ballards
							11/9/2021	GM	CO#7		$ 2,877.00	install concrete pedestrian ramp
							11/19/2021	GM	CO#8		$ (1,273.00)	reduce sow for carpet installation and relocation of toilet partition
							12/10/2021	GM	CO#10		$ 653.00	paint exterior wall
											$ 218,902.00	
900-20-01		**CWRF Emergency Generator Fuel Tank**	**$**	**288,000.00**	**$**	**56,694.29**						
800-20-02		**Pump Station #2 Generator Fuel Tank**	**$**	**363,000.00**	**$**	**56,828.22**						
	2020-80					Cannon	4/9/2020	BD		105,382.00	$ 95,772.00	Engineering design services
							2/11/2021	BD	CO#1	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
											$ 303,372.13	
400-20-02		**Reservoir 1B Comm Facility**	**$**	**670,000.00**	**$**	**47,738.29**						
						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	
800-20-04		**Reservoir 4C Replacement**	**$**	**160,000.00**	**$**	**110,503.00**						
800-20-03		**Reservoir 4C Hydro-pneumatic Pump Station**	**$**	**160,000.00**	**$**	**115,958.58**						
						Cannon	1/14/2021	BD		$ 297,855.00	$ 265,881.00	provide professional engineering services for the Reservoir 4C welded steel tank and hydropneumatic pump station replacements
							4/22/2021	BD	CO# 1	35,840.00	$ 35,840.00	provide additional professional engineering analysis for the Reservoir 4C welded steel tank and hydro-pneumatic pump station
							7/12/2021		CO#2	0.00	0.00	slope stability evaluation
							8/30/2021	GM	CO#3	3,347.00	$ 3,347.00	additional analysis eliminating reservoir storage
											$ 305,068.00	
650-22-02		**Tierra Rejada Well**	**$**	**295,000.00**	**$**	**24,004.52**						
						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 servies/spinner overview
											$ 28,950.00	
						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
											$ 285,864.23	

2022 Camrosa Board Calendar

JANUARY

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

FEBRUARY

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28					

MARCH

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

APRIL

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

MAY

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

JUNE

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

JULY

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

AUGUST

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

SEPTEMBER

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

OCTOBER

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

NOVEMBER

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

DECEMBER

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Camrosa Water District
7385 Santa Rosa Road
Camarillo, CA 93012

Note: Board of Directors meetings are highlighted in RED. Board Meetings are held on the **2nd & 4th Thursday** of each month at 5pm unless indicated.

2022 Holidays

- January 3rd - New Year's Holiday (Observed)
- February 21st - President's Day
- May 30th - Memorial Day
- July 4th - Independence Day
- September 5th - Labor Day
- November 11th - Veteran's Day
- November 24th & 25th - Thanksgiving
- December 23rd & 26th - Christmas
- December 30th - New Year's Eve

2022 Conferences

- CASA Winter Conf. (Palm Springs) - Jan. 19th - 21st
- ACWA Spring Conf. (Sacramento) - May 3rd - 6th
- CASA 67th Annual Conf. (Squaw Creek) - Aug. 10th - 12th
- ACWA Fall Conf. (Indian Wells) - Nov. 29th - Dec. 2nd

2022 AWA Meetings

- *"Water Issues" Third Tuesday (except Apr., Aug., Dec.)*
- Waterwise Breakfast (See yellow on calendar)
- AWA Board Meetings (See orange on calendar)
- ***August - DARK (No Meetings or Events)***
- September 29th - Reagan Library Reception
- ****DATE ?? - Annual Symposium****
- December 8th - Holiday Mixer

2022 VCSDA Meetings

- February 1st - Annual Dinner
- April 5th
- June 7th
- August 2nd
- October 4th
- December 6th

Read File