Information Technology Manager's Cybersecurity Report to the Board of Directors
August 26, 2026

Events have transpired in recent months involving ransomware and other attacks on water districts, internet service providers, and governmental entities that have spawned a renewed concern and healthy paranoia over cybersecurity matters in our industry.

As a water district providing essential infrastructure services, RMCSD stands as a prime target for foreign and domestic bad actors. Of particular concern is the SCADA (Supervisory Control and Data Acquisition) system that controls the fresh water and wastewater treatment plants. These plants are vulnerable to attacks that could take the plant down or tamper with water quality.

While RMCSD maintains rigorous information technology standards to which it adheres, more can always be done. With limited staffing, it is impossible to do all of the proactive work required to truly stay on top of emerging threats.

RMCSD operates the SCADA environment within its own secured bubble, using VPN (Virtual Private Network) services that segment that network away from other RMCSD networking services. This is standard procedure within the operational technology field but does not represent all that can be done to mitigate the inherent risk.

RMCSD utilizes Microsoft technologies through subscription-based services to provide our computing environment operating system software, applications, email, and server-side file sharing, along with remote, cloud-hosted services. Microsoft offers additional subscription-based services that will enhance our security profile and reduce our attack surface.

We would like to take advantage of the additional security services that are available to us. Enhancements to our security software are available from our managed service provider, ITS, who also provides additional services such as more proactive monitoring and penetration testing.

Quotes for these items are attached. We would like to add the additional services outlined below. This will result in our spending an additional $1,764 per month. I am asking that we consider moving forward with the purchase of these additional services as they will further protect our computing environment and mitigate the risks we face.

Rancho Murieta Community Services District

Security Recommendation and Board Briefing

Prepared by the Security Division of Intelligent Technical Solutions

Premise

The District requested security pricing to support a budget presentation to the Board of Directors. This document provides that, along with the reasoning behind each recommendation in language a board can act on.

The recommendation has two parts. The first is a set of security services that can be turned on immediately and that close specific, identifiable exposures. The second is a virtual Chief Information Security Officer engagement that builds the security program the District does not currently have and satisfies obligations that are already in force.

The two are not sequential. The services reduce risk while the program is being built. The program tells the District what else needs to happen and in what order.

Background: what already happened to this District

Most security presentations open with something that happened to somebody else. This one does not need to.

On Sunday, July 12, 2026, Greenfield Communications was hit with a large scale distributed denial of service attack. Greenfield's CEO told the River Valley Times that network monitoring identified the traffic pattern as a DDoS within minutes of the outage starting, but safely mitigating it and rebuilding the affected infrastructure took until Tuesday afternoon.

District phones and the billing department were unavailable for the duration. The District confirmed publicly on July 14 that internet and phone service had been restored and the billing department had reopened, with staff working through messages received during the outage. Every director with Greenfield service at home experienced the same two and a half days.

Then it happened again. On July 19, Zeta Broadband was hit by the same campaign and restored service in roughly twelve hours after refusing an extortion demand. Zeta's CEO told the same publication he believes several regional providers were targeted in a

coordinated effort, noting both incidents began on a Sunday, involved identical extortion communications, and used large scale volumetric carpet bomb DDoS techniques. Some Rancho Murieta customers who had switched to Zeta following the Greenfield outage were offline again inside of a week.

Three conclusions the Board should draw from its own July.

The District was never the target and it did not matter. Criminals attacked a regional internet provider for extortion money. District phones and billing went down anyway, in front of ratepayers. Being small, local, and uninteresting is not protection. It is a description of what makes a soft target.

A second provider is not a backup plan. Residents who switched from Greenfield to Zeta made a reasonable decision and were offline again seven days later. Real redundancy means a different path and a different technology, not a different logo.

The District has no way to detect the version of this that stays quiet. A denial of service attack is loud, and the District knew within minutes. An attacker who gets into a District account is silent by design, often for weeks. The District currently has nothing installed that would find them.

That third point is what the rest of this document addresses.

Background: the water sector in the last thirty days

Beginning the weekend of July 26 and 27, 2026, a coordinated campaign disrupted operational technology at more than thirty municipal water and wastewater utilities in Minnesota. The FBI reports that utilities in at least seven states have reported incidents since July 27, and that some of that activity degraded water operations. The FBI and EPA issued a joint Public Service Announcement warning that malicious cyber actors are attacking operational technology devices, naming specific Rockwell Automation and Allen-Bradley controller models.

The operational detail matters for a treatment plant. Federal advisories describe attackers modifying or deleting controller logic, manipulating what human machine interface and SCADA displays showed operators, and disabling shutdown and alarm functions, allowing equipment to run in unsafe conditions without notifying anyone. Affected utilities issued boil water notices and operated manually for extended periods.

On July 30, 2026, CISA issued an urgent sector wide advisory telling operators to immediately remove internet exposed PLCs and other operational technology from public networks. A July 22 update to CISA Advisory AA26-097A expanded the named device scope

to include Schneider Electric Modicon M340 and Siemens S7-1200 controllers and documented exfiltration of controller project files, indicating targeting beyond the originally named manufacturers.

Those Minnesota systems were not selected for who they are. They were selected because they were reachable.

Where the District stands today

The District already has a security foundation: Secure Essentials, security awareness training, and Microsoft 365 protections, supported by the ITS managed services team. What follows is not a list of failures. It is what sits outside that foundation, established during the August discovery call.

Governance and documentation. One boilerplate information security policy. No incident response plan, disaster recovery plan, or business continuity plan. No risk assessment has ever been performed. Employee policy attestation is available in the HR platform but has nothing current to attest to.

Operational technology. The SCADA system was recently replaced. The firewall and supporting infrastructure sit under integrator control on a segmented VPN. Responsibility for the environment stays with the District regardless of who operates it.

Resilience. A single internet provider, no secondary path, and a demonstrated two and a half day outage.

Identity and credentials. Password management split between LastPass and Bitwarden with inconsistent adoption. Credentials known to exist on paper outside any managed system.

Testing and validation. No penetration testing, no vulnerability assessment, no tabletop exercise.

None of this is unusual for a district of this size. All of it is addressable inside twelve months.

Obligations already in force

AWIA Section 2013. Community water systems serving more than 3,300 people must develop or update risk and resilience assessments and emergency response plans, certify completion to EPA, and recertify every five years. The statute expressly reaches the security

of electronic, computer, and automated systems, not only physical assets. For systems in the 3,301 to 49,999 population tier, the risk and resilience assessment certification deadline in the current cycle was June 30, 2026, and the emergency response plan certification deadline is December 31, 2026. The District should confirm its certification status immediately.

CIRCIA. Once final implementing regulations take effect, expected in September 2026, covered critical infrastructure entities including water and wastewater systems must report substantial cyber incidents to CISA within 72 hours and ransomware payments within 24 hours. A district with no incident response plan cannot meet a 72 hour clock, because the clock starts before anyone has decided who is authorized to make the call.

EPA enforcement posture. EPA continues to press on cybersecurity through guidance, technical assistance, and enforcement of existing authority, and in May 2024 issued an enforcement alert warning it would increase inspections tied to cybersecurity gaps found in drinking water systems.

Insurance. Cyber insurance applications ask directly about patch management, multifactor authentication, backup immutability, incident response planning, and awareness training. Answers that do not match the documented program create a coverage dispute at exactly the wrong moment.

What the District has today, and what we are adding

The recommendation builds on controls the District already runs. Each line below pairs what exists with what it does not yet cover.

Current foundation	Recommended enhancement	Why it matters
Secure Essentials and security awareness training	Secure package upgrade	If something gets past the current controls, who is watching for it? The upgrade adds third party patching, dark web credential monitoring, and detection coverage for District cloud accounts outside Microsoft. The aim is to find an attacker early rather than after the damage is visible.
Existing IT support	vCISO security leadership	Are we prepared before an incident rather than during one? A vCISO identifies gaps, prices risk in dollars, reviews the IT, OT and SCADA environments, builds the incident response plan, and produces a prioritized roadmap the Board can budget against.

Current foundation	Recommended enhancement	Why it matters
Microsoft 365 security	M365 Monitoring	What if an employee account is compromised? An attacker holding a valid login can reach email, files, and banking, or redirect a vendor payment. Monitoring detects the compromise, establishes what was accessed, and acts before the money moves.

Taken together these add earlier detection, faster response, fewer open vulnerabilities, and a written plan the District can follow under pressure.

Part One: Security Services

The Secure package

The District currently runs a baseline security package. The Secure upgrade adds three capabilities that address how organizations of this size are actually compromised.

Third party patching

What it is. Automated patching for the software that is not made by Microsoft: browsers, PDF readers, remote access tools, Java, conferencing clients, and the utility applications running on District workstations.

Why it matters here. Microsoft patching covers Microsoft. It does not touch the majority of what is installed on a District computer. The most common way into an organization this size is not a sophisticated exploit against Windows. It is an outdated browser or PDF reader on one machine in the business office, reached by an employee clicking a link.

An unpatched application on a single administrative workstation gives an attacker a foothold. From there the question becomes whether the boundary between the business network and the plant network holds, which is not a question the District currently has evidence to answer.

Secondary benefit. Cyber insurance applications ask directly whether the District operates a patch management program covering third party applications. Answering yes with documentation behind it affects both premium and whether a claim is paid.

The ask. Fund automated third party patching so every application on every District computer stays current without depending on staff time that does not exist.

Dark web monitoring

What it is. Continuous monitoring of criminal marketplaces and breach dumps for District email addresses and credentials, with alerting when one appears.

Why it matters here. District employees reuse passwords. Everyone does. When an employee's password is exposed in a breach of an unrelated service, an attacker will try that same password against District systems. This is the most common initial access method in use today and it requires no skill on the attacker's part.

The District has a specific version of this problem. Password management is split between two platforms with inconsistent adoption, and credentials are known to exist on paper outside any managed system. The District does not currently know which passwords are in use, where, or how old they are.

What it buys. This control does not stop an attack. It gives the District the chance to reset a password before it is used, which converts a breach into a nonevent. It is also the least expensive item in this entire recommendation.

The ask. Fund dark web monitoring so exposed District credentials are found by us rather than by an attacker.

Additional XDR for non Microsoft accounts

What it is. Detection and response coverage extended to the District's cloud services and accounts that live outside Microsoft 365: the HR platform, billing and utility applications, banking portals, vendor portals, and any other service holding District data or reachable with a District login.

Why it matters here. Attacks increasingly target the login rather than the computer, because a valid login bypasses every protection installed on the endpoint. The District's tools today watch District computers. If an attacker takes over a District account on a system that is not Microsoft, nothing currently sees it.

Payroll and personnel data in the HR platform, customer billing information, and banking access are all reachable through accounts nobody is monitoring. For a public agency this size, financial loss almost always occurs inside cloud accounts and never touches a District computer at all.

How it pairs with the next section. This covers everything outside Microsoft. Microsoft 365 itself, which is where District identity, email, and files actually live, is covered

separately below. Together they mean coverage follows the account rather than stopping at a vendor boundary.

The ask. Fund additional XDR so District cloud accounts outside Microsoft are monitored rather than assumed safe.

M365 Monitoring

Priced per user per month.

What it is. Continuous monitoring of the District's Microsoft 365 environment for account takeover and email based fraud, with alerts routed to the ITS security operations center.

Why this is the highest financial risk item in the recommendation. The largest cash loss for a public agency the size of this District is not ransomware. It is vendor payment redirection.

It works like this. An attacker gets into a District mailbox using a stolen password. They read a genuine email thread with a contractor or supplier. They wait for an invoice. Then they send banking change instructions from the real District account, in the real thread, in the voice of the person who normally sends it.

Nothing malicious ever touches a computer. No antivirus alert fires, because technically nothing about it is an attack. The money leaves through the accounts payable process working exactly as designed. The District finds out weeks later when the actual vendor asks why they have not been paid.

Endpoint tools cannot see this. Neither can patching or dark web monitoring, because by the time it happens the credential has already been used successfully.

What it watches for.

- Sign ins that do not fit the user, including access from unusual locations or from two locations too far apart to be the same person
- Repeated multifactor prompts used to wear a user down into approving one
- Session token theft, where an attacker bypasses multifactor entirely by stealing an already authenticated session
- Mailbox rules created to hide, delete, or forward messages, which is the standard first move after a mailbox is compromised
- Third party application consent grants, where a user is tricked into giving an outside application ongoing access to District data
- Administrative role and permission changes

The ask. Fund Microsoft 365 monitoring so a compromised District account is detected in hours rather than after a payment has gone out the door.

Part Two: vCISO Engagement

What a vCISO is, in board terms

The District does not have, and does not need to hire, a full time Chief Information Security Officer. It does need the function. A vCISO provides that function on a fractional basis: a credentialed security executive who owns the District's security program, reports to the General Manager, briefs the Board, and is accountable for the roadmap.

Tools reduce specific exposures. They do not tell the District what its risks are, what order to fix them in, what to tell an insurer, how to answer a regulator, or what to do at two in the morning when something goes wrong. That is the gap this engagement fills.

Recommended structure: a three year program at a fixed monthly fee, with leadership meetings every month. Year one is $3,000 a month and covers 120 consulting hours, budgeted at 10 hours a month. Every deliverable in the Statement of Work carries a set hour value, and the year one list totals 120 hours. Years two and three are scoped at the same monthly figure and the same cadence, and each is a separate twelve-month term the District renews or does not.

What this means in practice. Hours are assigned to specific deliverables and reserved before work begins, so the District can see at any point what the remaining balance is committed to. If a deliverable runs longer than scoped, that is our cost rather than the District's. An integrator that ignores the first request, or a document that needs three rounds of revision, does not draw down the balance. The monthly amount is the same every month, and at year end the question is which deliverables were produced.

Pacing. No more than 13 hours are drawn in any single month, so the program cannot be front loaded into a position where nothing is left in month ten. The schedule sits under that limit in every month, and unused hours do not expire during the term.

What we would do

The program runs for three years. Year one is funded and scoped here; years two and three are described so the Board can see the whole arc and budget against it. Each year is a separate twelve month term the District renews or does not.

Year one. Find out what is there, and what it is worth protecting.

The District cannot write a rule for a network nobody has mapped. Year one establishes the boundary, measures it against a recognized standard, prices the risk in dollars, and puts an incident response plan in place against the reporting clocks that already apply.

- Confirmation of whether any District control system device is reachable from the public internet, which is the single most urgent question raised by the July advisories
- AWIA Section 2013 certification status confirmed against the December 31, 2026 deadline
- Full boundary and asset inventory covering the business environment, both treatment plants, remote sites and lift stations, and everything connecting them
- Review of every remote access path into the process control environment, including the integrator's path and any cellular connections nobody installed deliberately
- A formal, tracked security posture request issued to the SCADA integrator, and a written matrix setting out who owns which control area across the District, ITS, and the integrator
- Formal gap assessment against NIST CSF 2.0, rating current state across all six functions, with CIS Controls IG1 and NIST SP 800-82 OT guidance mapped alongside
- Written risk assessment rating each finding by likelihood and financial impact in dollars, with information technology and operational technology scenarios assessed separately because the consequences are not the same
- Incident response plan covering business systems and plant operations, including the CIRCIA 72-hour reporting clock and who is authorized to start it, with an annex for loss of SCADA visibility and manual operations fallback
- Backup architecture validated against ransomware, including immutability, offsite copies, and tested restoration of SCADA configuration and controller project files
- Leadership meetings every month throughout the year, plus advisory time held in reserve for issues that arise between them

Deliverables: gap assessment, written risk assessment, incident response plan and OT annex, findings report, remediation plan with owners and dates, a three year roadmap the Board can budget against, and a nontechnical Board briefing package.

One item deserves emphasis. The integrator currently controls the plant firewall and has not answered the District's emails. A vCISO converts an unanswered email into a

documented governance item with an owner, a due date, and an escalation path. That is a different conversation than a District employee asking politely.

Year two. Write the rules and build the controls.

Policies written in year one would be policies written against an undefined boundary, and they would be rewritten in year two once the boundary is known. Year two builds on measured ground.

- Full information security policy set including operational technology rules, built from the current boilerplate, with attestation stood up in the existing HR platform
- Risk register built and maintained, so treatment progress is tracked rather than assumed
- Business impact analysis, disaster recovery and business continuity plans, including manual operations fallback for both plants
- CIS Controls IG1 implementation driven with the ITS managed services team
- Vendor oversight process covering contract language, shared responsibility, and attestation refresh for the integrator and others
- Oversight of the District's existing security awareness program: coverage, completion rates, and phishing results reviewed against the new policy set

Year three. Prove it works, and sustain it.

- Identity and access hardening validated across Microsoft 365, including multifactor coverage, conditional access, and separation of daily accounts from administrative accounts
- Password management consolidated to one platform, and default, shared, and vendor credential cleanup completed in the operational technology environment
- IT to OT segmentation validated, confirming that a compromise of the business network cannot reach the plant network
- Integrator remote access brought under District control: approval, time limits, logging, and revocation on personnel change
- Tabletop exercise facilitated against a ransomware and loss of SCADA visibility scenario, with a written after action report
- Evidence organized in examination ready form for regulators, auditors, insurers, and grant applications, with cyber insurance and grant documentation support

What this engagement will surface

Being direct about something the Board should hear now rather than in month four. The services in Part One address prevention, credential exposure, and cloud detection. They do not provide visibility into network traffic inside the District, which is where ransomware moves between machines before it encrypts anything. That is a real remaining gap.

We are not recommending the District solve it today. We are recommending the year one risk assessment quantify it so the Board can decide with a number in front of it rather than a sales pitch. That is the difference between a vendor and a security program.

The risk we cannot ignore

A cyberattack on a water district is not an IT problem. The chain runs from operational disruption, to loss of access to critical systems, to emergency recovery costs, to impact on public services, to loss of public trust.

The District saw the first two links of that chain in July, without an attacker ever being inside District systems.

The question is not whether the District can prevent every attack. It is how quickly the District would know, how quickly it could contain an attacker, and how prepared it would be to recover. Everything in this recommendation is aimed at those three questions.

> *We are not investing because an attack is certain. We are investing because the cost of being unprepared is far greater than the cost of preparing now.*

The recommendation at a glance

Component	Basis	What it addresses
Secure package upgrade	Package	Third party patching, dark web monitoring, additional XDR for non Microsoft cloud accounts
M365 Monitoring	Per user per month	Account takeover and vendor payment fraud inside Microsoft 365

Component	Basis	What it addresses
vCISO engagement	$3,000 per month; 120 consulting hours for year one of three	Year one: NIST CSF 2.0 gap assessment, risk assessment, incident response, backup validation, AWIA, SCADA integrator governance, Board reporting. Policies and continuity planning follow in year two.
Engagement onboarding and Year End Session	Quoted separately	One time setup of the evidence repository, document library, stakeholder matrix and reporting cadence, and the year end close. Required on every engagement.
ITS Verify Governance Portal (optional)	Platform subscription	Hosts the program evidence set. The gap assessment itself is included in the vCISO engagement, not purchased separately.
Penetration testing and vulnerability assessment	Quoted separately	Scoped when the program reaches that stage

Work inside the SCADA and process control environment is documentation and configuration review based. No active scanning or testing is performed against production control systems without written authorization and a scheduled maintenance window.

Delivery is by the Security Division of Intelligent Technical Solutions, which operates a 24/7 security operations center, a vCISO advisory practice, and a dedicated offensive security team. ITS is the contracting entity.

Important Questions

“Aren't we already paying ITS for security?”

The District pays for managed information technology with baseline protection. This adds detection and governance, which are different functions. Baseline protection tries to stop known bad software on individual computers. It does not see an attacker using a legitimate District password, and it does not tell the District what its risks are or what to do about them.

“Has anything happened to us?”

July happened to us. Beyond that, nothing we know of, and that statement is doing more work than it appears to. The District has limited capability to detect an intrusion that does not announce itself. Absence of a known incident is not evidence of absence.

“We were a bystander in July. Isn't that just bad luck?”

It was position, not luck. The District depends on a single regional provider that criminals identified as a soft extortion target and had no alternate path. That is a decision the District can change, and the same reasoning applies to everything else here.

“Can this wait until next fiscal year?”

The sector threat activity described here is from last month. The AWIA emergency response plan certification deadline is December 31, 2026. Federal incident reporting rules requiring notification within 72 hours are expected to take effect in September 2026. The timeline is set externally.

“What would an incident actually cost us?”

The District can estimate its floor from experience. Two and a half days of lost phones and billing, with no attacker inside District systems and no data at risk, produced measurable operational cost and public visibility. A ransomware event is measured in weeks, plus incident response and legal fees, plus notification costs, plus insurance and rate consequences, plus the reputational cost of a boil water notice in a community this size. Putting a real number on this is a year one deliverable.

“Why do we need the vCISO if we are buying the tools?”

The tools close specific holes. They do not produce the risk assessment, the incident response plan, the AWIA certification, the insurance answers, or the roadmap. If the District buys only tools, it will have better protection and still no answer when EPA, an insurer, or this Board asks what the plan is.

“How do we know we are getting the hours we pay for?”

Each deliverable in the Statement of Work carries a set hour value and is reserved against the balance before work starts. The District receives a written statement every month showing what was completed, what is in progress, and how many hours remain. At year end the Board can check the deliverable list against what was produced.

“What happens if we do not use all 120 hours?”

The schedule is built so the deliverable list consumes the full entitlement, with a small reserve held back for issues that come up between meetings. Hours do not expire during

the term and can be pulled forward. They do not carry past the anniversary, which is why the year is scheduled rather than left open.

“If we can only fund part of this, what comes first?”

The vCISO engagement, because it tells the District what to buy next and satisfies obligations that already have deadlines attached. The Secure package upgrade should go alongside it, because it is inexpensive relative to the exposure it closes and does not need to wait on the assessment.

Recommended next steps

1. Approve the vCISO engagement so discovery begins in September. The NIST CSF 2.0 gap assessment is included in it.
2. Approve the Secure package upgrade and M365 Monitoring in parallel.
3. Confirm AWIA certification status this month. The emergency response plan deadline is December 31, 2026.
4. Inventory internet reachable operational technology, including anything the integrator installed, ahead of formal year one discovery. This is the highest value action available to the District today and it costs nothing.

Sources

- River Valley Times, “Greenfield Outage Disrupts Service More Than Two Days,” July 21, 2026
- River Valley Times, “Greenfield CEO Answers Outage Questions,” July 21, 2026
- River Valley Times, “Zeta Restores Broadband Service, Refuses to Pay Extortion for Cyberattack,” August 4, 2026
- FBI and EPA Public Service Announcement on water sector PLC targeting, August 2026
- CISA Advisory AA26-097A, issued April 7, 2026, updated July 22, 2026
- CISA sector wide alert to the Water and Wastewater Systems Sector, July 30, 2026
- EPA, AWIA Section 2013 and SDWA Section 1433 certification deadlines
- Cyber Incident Reporting for Critical Infrastructure Act of 2022, final implementing regulations expected September 2026

PROPOSAL

3330 W Desert Inn Road, Suite B, Las Vegas, NV 89102

SOW#: AAAQ29413

t. 702-869-3636 f. 702-869-6777

Aug 21, 2026

Expires:Sep 20, 2026

CLIENT: RMCSD

SHIP TO: RMCSD

ITS:

Celeste Catan

Andy Lee
celeste.catan@itsasap.com

Andy Lee

15160 Jackson Road Rancho Murieta, CA 95683-9620
United States

15160 Jackson Road Rancho Murieta, CA 95683-9620
United States

Contract Start Date:

Contract Initial Terms:

This Statement of Work ("SOW") shall be governed by the Terms and Conditions set forth at https://www.itsasap.com/terms-and-conditions (as they may be updated from time-to-time by the Company, the "Terms and Conditions"), which Terms and Conditions are hereby incorporated by reference as if set forth herein.

Line #	ITS SECURE SERVICE PACKAGE		Unit Price	Qty
3	**ITS SECURE v2.5**	**Monthly**	**$3,250.00**	**1**

Quantities will be adjusted based on actual inventory counts at time of billing.

5 (53) ITS Secure per Endpoint | $35/ea

6 (73) ITS Secure per User Mailbox | $15/ea

7 (1) Security Appliance - Medium (25-250U) | $300/ea

8 **SECURE Monthly SubTotal**

$3,250.00

Default payment method is ACH. In the event payment is made through any method other than ACH, a surcharge of 5% will be applied to the total agreement value.

10 *Secure endpoints with standards-aligned configurations that reduce risk and simplify security operations. (Optional)*

Monthly

$3.00 53 *$159.00*

TOTAL: MONTHLY RECURRING CHARGES $3,250.00

EXISTING MONTHLY CHARGES TO BE REPLACED -$

Line #			Unit Price	Qty
	This SOW supercedes and replaces the following existing services and charges:			
15	SEssentials-Cloud-UNLTD	*Monthly*	$10.00	-62
	-$620.00			
16	SEssentials-Endpoint-UNLTD	*Monthly*	$15.00	-53
	-$795.00			
17	Security Awareness Training- Per user License	*Monthly*	$3.00	-62
	-$186.00			
18	Security Awareness Training- Monthly Fee	*Monthly*	$250.00	-1
	-$250.00			

TOTALS	ONE-TIME CHARGES		MONTHLY RECURRING CHARGES	
	Subtotal	$1,399.00	**Subtotal**	$1,399.00
	Tax	$0.00	**Tax**	$0.00
	One-Time Total	**$1,399.00**	**Net Monthly Change**	**$1,399.00**

TOTAL: EXISTING MONTHLY CHARGES REPLACED -$1,851.00

Created on 08/25/26 12:28:02 by Celeste Catan

PROPOSAL

3330 W Desert Inn Road, Suite B, Las Vegas, NV 89102 **SOW#: AAAQ29417**

t. 702-869-3636 f. 702-869-6777 **Aug 21, 2026 Expires:Sep 20, 2026**

CLIENT: RMCSD **SHIP TO:** Andy Lee **ITS:** Celeste Catan

Andy Lee 15160 Jackson Road

Rancho Murieta, CA

95683-9620

United States

celeste.catan@itsasap.com

15160 Jackson Road

Rancho Murieta, CA

95683-9620

United States

This Statement of Work ("SOW") shall be governed by the Terms and Conditions set forth at https://www.itsasap.com/terms-and-conditions (as

they may be updated from time-to-time by the Company, the "Terms and Conditions"), which Terms and Conditions are hereby incorporated by

reference as if set forth herein.

Monthly Recurring Services

2 M365 monitoring *Monthly* $5.00 73 $365.00

Monthly Recurring Subtotal $365.00 Professional Services

Onboarding Fee $500.00 1 $500.00 **Professional Services Subtotal $500.00 Project Workplan**

POC: Andy Lee

Timeline: Standard

Scope of Work:

Initial setup and configuration of Petra

Integration with Microsoft 365 environment

Basic configuration for incident detection and alerting

Setup of reporting features and dashboards

Validation and testing of functionality

TOTALS Monthly Recurring Charges One-Time Charges

Subtotal $365.00 **Subtotal** $500.00

Tax $0.00 **Tax** $0.00

Monthly Total $365.00 Shipping $0.00

One-Time Total $500.00

Deposit Required $500.00

Payment Terms: 100% Deposit due at signing.

The prices listed in this SOW show an ESTIMATED sales tax. However, if state and/or local tax codes require the collection of sales tax, the tax

will be added to invoices and will be calculated based on the applicable tax rate at the time of billing.

Speed up your order processing by entering payment information upfront at https://signnow.com/s/oQhgHXxc